児童ポルノのブロッキング に関する法律問題

Internet Week 2009

英知法律事務所

弁護士　森　亮二

違法有害情報に対する自主規制の拡大と児ポのブロッキング

安心ネットづくり促進協議会

- 青少年インターネット利用環境整備法の成立を受けて2009年2月に設立。安全・安心なネットづくりを推進し、インターネット利用環境を整備する。インターネットにかかわるあらゆる当事者の参加を想定。
- 調査企画委員会と普及啓発委員会の2つが活動の柱。前者の中に**「児童ポルノ対策作業部会」**「コミュニティサイト検証作業部会」を設置。

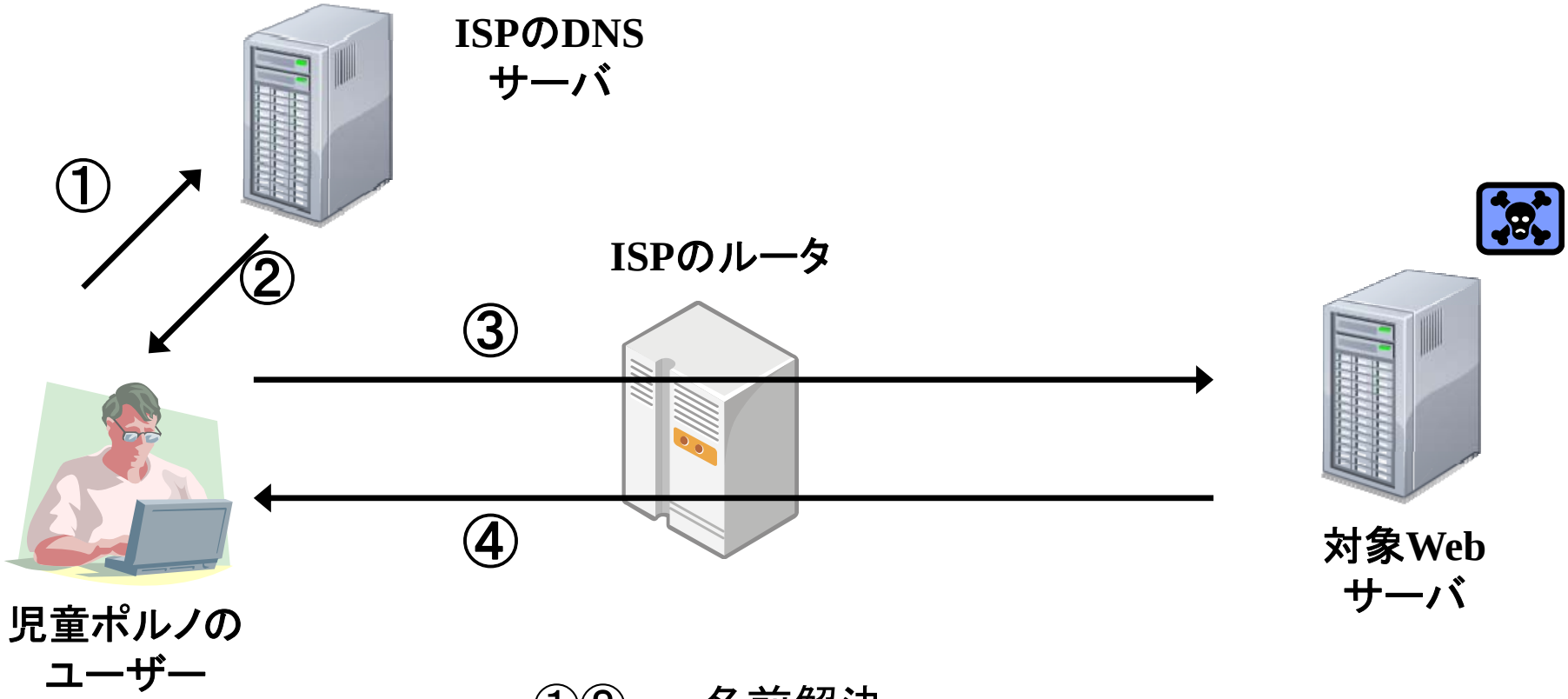
EMA、I-ROI

- サイトの第三者認証。サイトの安全性についてお墨付きを与えるしくみ。

児童ポルノ流通防止協議会

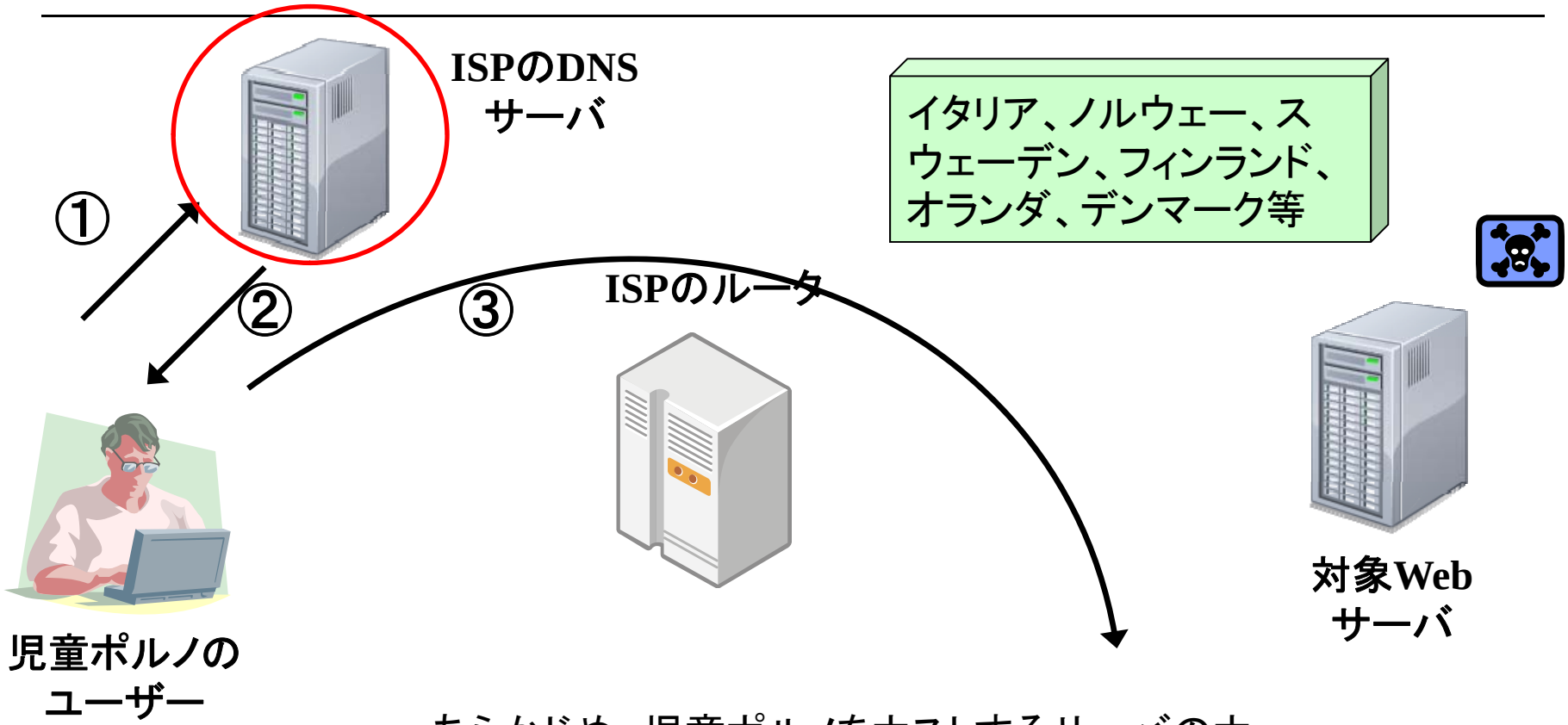
- インターネット上の児童ポルノの流通を防止する対策について検討を行うため、2009年6月に設立。児童ポルノの流通防止対策に関係する事業者、民間団体、学識経験者等が参加。
- 児童ポルノ掲載アドレスリスト作成管理団体の設置に向けた検討と**ブロッキング等の手法に関する検討**を行う。

ブロッキングのしくみ　ーWeb閲覧の通常の流れー



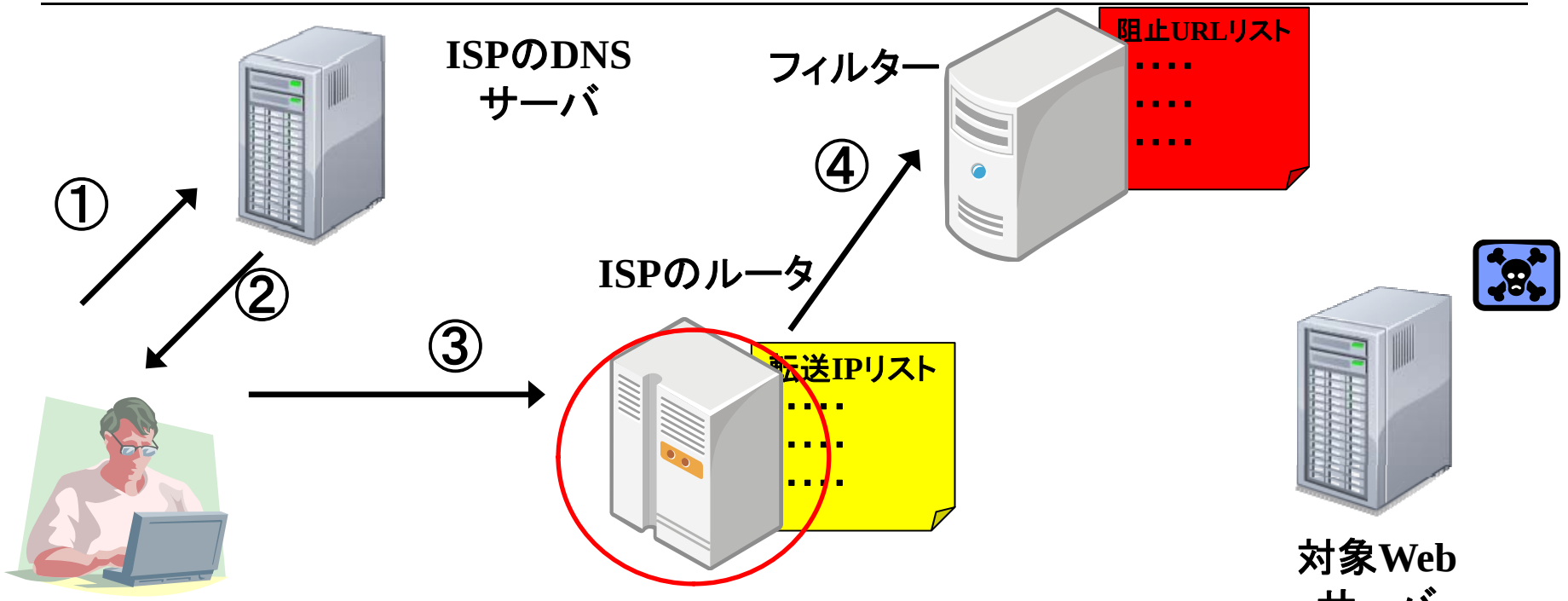
①②:　名前解決
③:　送信要求
④:　受信ー閲覧

ブロッキングのしくみ　ーDNSポイズニングー



- あらかじめ、児童ポルノをホストするサーバのホスト名をDNSサーバに登録する。
- 登録されたホスト名の照会（①）に対してはダミーのIPアドレスを返す（②）。

ブロッキングのしくみ　ーハイブリッド・フィルタリングー



- 児童ポルノをホストするIPアドレスのリストを作成し、リストにあるIPアドレスへの送信要求はフィルターに転送する。
- フィルターではあて先のURLベースでより精密に監視しリストにあるURLへのアクセスについては閲覧を阻止

イギリス、オーストラリア

法的問題1　通信の秘密

憲法第21条2項

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4条1項

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。

もしも、法改正で単純所持が犯罪化されれば、
正当防衛として違法阻却されることも・・

- 誰と通信をしようとしているかということは当然通信の秘密に含まれる。

＋

- 機械的に誰と通信をしようとしているか監視することも通信の秘密の侵害にあたる。

⇩

- もちろん、通常の通信でもルーティングに際してあて先を機械的にチェックしているがこれは、通信を成立させるための**正当業務行為**として違法行為が阻却される。

⇩

- 同意なく、リストの該当性を探る行為「このあて先は児ポのホスト（IP）では？」は通信の秘密の侵害にあたる可能性あり。

法的問題2　オーバーブロッキング

- DNSポイズニングのオーバーブロッキング

DNSポイズニングについては、ホスト名の照会に対して、偽のIPアドレスを返すため、そのホスト名全体について閲覧することができなくなる。

適法なコンテンツまでブロッキングの対象とすることに･･･

- そもそも児ポのみをブロッキングすることは困難

① URLの中身が変わることもある。

＋

② 児ポの該当性判断は場合により難しい※

不必要なブロッキングのおそれ

※

Q1：18歳未満のアイドルの水着姿の写真は児童ポルノ？
Q2：裸の乳幼児のオムツのコマーシャルは児童ポルノ？

A1、A2：
具体的な写真等を見ない限り結論が出せません。
「よくわかる改正児童買春・児童ポルノ禁止法」（ぎょうせい）

児童ポルノの規制に関する議論の整理

実はほとんど
対立点なし

児童虐待情報はインターネットから締め出さなければ！

それは仕方ないかな‥

いやそこまではいわないよ･･･

アイドルの水着や親が撮った子供の映像もだめなの！？

他の違法情報のことなんて知らないよ

他の違法情報にもブロッキングなんてやりすぎだ！

定義の不明確さ

児童性愛者の問題

規　制　派

表現の自由派

ブロッキングの法的問題点と今後

- 法的には問題が残っており費用もかかるが、海外では自主的取組としてかなり広く行われている。
- 児童ポルノの流通抑止については、反論が少なく、放置していると強力な法規制がなされるおそれがある。そのリスクを考慮すべき。
- “NO TORELANCE”は児童ポルノのキャッチフレーズ。ブロッキングのような強力で広汎な制限を他の違法・有害情報に流用することは問題。

資料　ブロッキングについての説明①

インターネット上の違法・有害情報への対応に関する検討会　最終取りまとめ

(a) DNSポイズニング方式

ユーザーがウェブページにアクセスしようとする場合、まず、DNSのキャッシュサーバーに目的のウェブページのドメイン名に対応するIPアドレスを問い合わせ、当該キャッシュサーバから返ってきたIPアドレスによって目的のウェブページにアクセスすることになる（この仕組みを「名前解決」という。）。一般個人ユーザとしてのISPの利用者や、無線LANなどのモバイルISPの利用者は、自身でDNSのキャッシュサーバを用意せずISPの提供するDNSのキャッシュサーバーを利用することが多く、個人向けISPやモバイルISPのサービスもそれを前提とした接続情報を提供している。DNSポイズニングとは、この名前解決の仕組みを利用して、ユーザーが名前解決のためにDNSのキャッシュサーバーにIPアドレスを問い合わせてきた際に、DNSのキャッシュサーバにおいて当該ホスト名とDNSキャッシュサーバに設定された閲覧規制リストとを照合し、閲覧規制リストにあるホスト名については、正しいIPアドレスを返さず、ダミーのIPアドレスを返すことにより、閲覧規制リストにあるウェブページへのアクセスを阻止する手法である106。ブロッキングとしては一般的な手法であり、スウェーデンをはじめ北欧諸国において民間の自主的取組として導入されている。この手法の利点は、閲覧規制リストに載せれば国内外のコンテンツを問わずアクセスを遮断できること、名前解決はユーザーとDNSのキャッシュサーバーとの通信当事者間の通信と解しうるため、通信の秘密との関係の整理が比較的しやすく、ユーザー側の設定や同意がなくても、ISP側の設定変更のみで実施可能と解する余地があることなどである。また、後出のハイブリッドフィルタリング方式と比較して設備投資等のコスト負担が少なくてすむとの指摘もある。

資料　ブロッキングについての説明②

インターネット上の違法・有害情報への対応に関する検討会　最終取りまとめ

(a) DNSポイズニング方式　（続き）

他方、ホスト名という粗い単位でアクセスを遮断するため、同じホスト名の中に遮断すべき児童ポルノコンテンツとその他の問題のないコンテンツとが混在している場合にも一律に遮断せざるを得ず、結果的に問題のないコンテンツまでブロックされてしまうという、いわゆるオーバーブロッキングという問題が生じる。本手法を採用している諸外国でもこの点が問題点として指摘されることがある。また、DNSのキャッシュサーバーで名前解決する際にブロックするものであるため、ユーザーが直にIPアドレスを入力したり、ISPではない外部のDNSのキャッシュサーバーで名前解決したりして107、ISPのDNSのキャッシュサーバーを利用することなく児童ポルノサイトにアクセスすればブロッキングを回避でき、仕組みとして脆弱な面がある。さらに、DNSのキャッシュサーバーの設定を操作することから、DNSのセキュリティを向上させるための仕組みであるDNSSECの導入等、今後のDNS技術の高度化を阻害するおそれも指摘されている。

(b) ハイブリッドフィルタリング方式

ハイブリッドフィルタリング方式とは、2段階の仕組みでブロックする方式をいう。まず、第一段階（パケットフィルタリング）では、ISPにおいて、アクセスの宛先のIPアドレスを監視し、閲覧規制リストにあるIPアドレスと一致したものについては、第2段階のフィルターに送り込み、それ以外のものについては通常どおりにアクセスさせる。第2段階のフィルター（ウェブフィルタリング）では、宛先のURLベースでより精密に監視し、閲覧規制リストにあるURLへのアクセスについては、ページが存在しないというメッセージをユーザーに返すなどして閲覧を阻止する。

資料　ブロッキングについての説明③

インターネット上の違法・有害情報への対応に関する検討会　最終取りまとめ

(b) ハイブリッドフィルタリング方式（続き）

まずIPアドレスで大づかみに問題のあるサイトとそうでないサイトとを選別し、IPアドレスベースで問題のあるものについて、さらにURLベースでフィルターするという仕組みになっている。この手法は、イギリスにおいて民間の自主的取組として採用されている。

この方式の利点は、2段階のフィルターをかけるため、DNS方式と比較して精度が高く、オーバーブロッキングの危険を減少させることができる点にある。また、IPアドレスとURLベースでフィルターしているため、ユーザーがIPアドレスを直接入力したり、ISP以外のキャッシュサーバーで名前解決したりしても、フィルターをくぐり抜けることが難しく、脆弱性も改善される。閲覧規制リストに載せれば国内外のコンテンツを問わずアクセスを遮断することもできる。

他方、DNSポイズニング方式に比べて中継するISPの通信設備への負荷が大きく、通信速度の低下やシステムの障害を生ずる危険性が高まり、これを避けようとすれば相応の設備投資を要することになるため、実施にあたっての負担が大きくなる。また、この方式では、中継するISPが、通信の宛先のIPアドレスやURLを監視することになるので、フィルタリングと同様、通信の秘密との抵触が問題となり、ユーザーの同意なく実施することは困難である。加えて、ハイブリッドフィルタリング方式では、ユーザー側においてパケット情報を調査するなどの方法により、第1 段階から第2 段階に回されたのか、第1 段階で閲覧リスト対象外とされてそのまま通常通り通信しているのかを判定できる場合がある。この場合、第１段階から第２段階に回されたIPアドレスを集めて、そのIPアドレスからホスト名を検索していけば、児童ポルノ情報が含まれるサイトの一覧表が作成できてしまうという問題も指摘されている。

資料　ブロッキングについての説明④

インターネット上の違法・有害情報への対応に関する検討会　最終取りまとめ

(b) ハイブリッドフィルタリング方式（続き）

DNSポイズニング方式、ハイブリッドフィルタリング方式のいずれも、今後の児童ポルノ情報の閲覧防止策として期待の持てる手法といえるが、どちらの方式にも一長一短あり、それぞれに解決すべき課題を抱えている。それらの課題の具体的な解決策については、今後の議論を待つ必要があるが、DNSポイズニング方式におけるオーバーブロッキングの点は、例えば特に悪質な児童ポルノ関係サイトに限定してブロックするなど、運用上の工夫によりある程度回避することが可能ではないかと考えられる。又ハイブリッドフィルタリング方式については、現状では通信の秘密との関係の整理は容易ではないが、児童ポルノの単純所持が違法化される

法改正の動向によっては、整理できる可能性もある。

なお、別の視点として、適法なサイトやファイルが誤ってブロッキングの対象となってしまった場合の扱いについても併せて考えておく必要がある。現行法の「児童ポルノ」の定義については、個別の事例において該当するか否かの判断が難しいという指摘がなされている。「児童ポルノ」の定義については立法措置等により可能な限り明確化・客観化が図られることが望ましいが、児童ポルノか否か判然としないコンテンツの出現は不可避であり、誤って適法な情報がブロッキングの対象となる事態は起こりうる。しかも、ブロッキングの対象とされた場合でも、自分のサイトがブロッキング対象となっているかどうかは、当然に知りうるわけではない。そのため、自分のサイト等がブロッキングされているかどうかを知りうる手段を用意するとともに、ユーザーからの反論を受け付け、必要に応じて規制対象リストから除外できるようにする仕組みが必要になると考えられる。

ご清聴ありがとうございました