意見書

2019 年 5 月 14 日

総務省総合通信基盤局
　電気通信事業部消費者行政第二課　御中

所属	一般社団法人日本インターネットプロバイダー協会
氏名	会長　会田 容弘
住所	東京都渋谷区代々木 1-36-1 オダカビル 6F
連絡先	連絡担当者氏名　：事務局長　亀田　武嗣 電話：03-5304-7511 e-mail：info@jaipa.or.jp

「アクセス抑止方策に係る検討の論点」に関し、別紙のとおり意見を提出します。

別紙

検討・実施に当たっての基本的な考え方及び進め方について	
論点１： アクセス抑止方策の検討に際しては、インターネット上の海賊版の現状について関係者の共通認識のもとで議論を進めるべきではないか。	論点案の通り、関係者の共通認識のもとでの丁寧な議論が必要と考えます。
論点２： インターネットの特徴や役割を踏まえて、あるべきネットワークの姿は何かを考慮しつつ議論を進めるべきではないか。	インターネットは民間主導のもと、その時々の技術進歩を踏まえ、さまざまな形で発展してきました。基本的には自律分散の構成であるため、ISP によりそのネットワーク構成は多種多様です。アクセス抑止方策の検討にあたっては、そのような多様性や技術の進歩を阻害することが無いよう検討を行うことが必要と考えます。 また、インターネットは日本だけで成り立つものではなく、海外の電気通信事業者との相互接続が広く行われています。日常的に使われるブラウザなども海外で開発されて世界中で使われているものが多いため、関係する当事者が広い範囲に及ぶことにも留意する必要があります。 よって論点案のとおり、インターネットの特徴やあるべきネットワークの姿を考慮しつつ、丁寧に議論を進めていただきたいと考えます。
論点３：具体的な方策の検討に当たっては、海賊版サイトにアクセスするユーザにとどまらず、多くのネットユーザにも影響があり得ることから、幅広いユーザの声に耳を傾け、 ユーザの理解を十分に得て進めることが必要ではないか。	利用者の積極的な意思で行うフィルタリングと異なり、ブロッキングやアクセス抑止方策は、論点案の通り海賊版サイトへのアクセスの有無にかかわらず、一度すべての利用者の通信内容をチェックする点で、通信の秘密への影響が極めて大きい手法です。 また、アクセス抑止策に用いられる装置や技術は、広くインターネット上の検閲やブロッキングなどにも転用可能です。

	現在、極めて悪質な児童ポルノに限定して行われているブロッキングは、「これ以外に広げることはない」という官民の約束の上で、2011 年から電気通信事業者の自主的な取り組みとして、利用者の皆さまの理解を得ながら行ってきました。そのような中で 2018 年に政府が海賊版サイトへのブロッキングを「要請」し、その議論が混迷を極めたことは、一度このようなしくみを導入してしまった後で、その範囲が広がらないように厳格に守ることの難しさを示しています。 国民の重要な権利である通信の秘密や表現の自由への干渉につながる手法を検討するにあたっては、最大の利害関係者であるインターネットユーザ（国民）を抜きに進めることは考えられません。 よって論点案のとおり、幅広いユーザの声に耳を傾け、丁寧な合意形成のプロセスを行っていくことが必要です。
論点４：アクセス抑止方策の実際の導入に向けた詳細調整・実施は、民間部門において主体的・主導的に進められるべきではないか。	インターネットは民間主導のもとに発展してきました。もしアクセス抑止方策を導入するのであれば、論点案のとおり、その調整・実施は民間部門を抜きにしては考えられないと思います。 また、ネットワーク上でアクセス抑止方策を導入する場合、法的な問題をクリアするためには運用の正当性も不可欠になります。児童ポルノのブロッキングの例にならい、対象サイトのリストの作成、管理を透明かつ中立的に行う必要があります。これを政府やその関連組織が行うとなれば、それは検閲に他ならないため、政府から十分独立した民間部門において行うことが必要です。
アクセス警告方式の実現に向けた検討課題	

論点５：アクセス警告方式を何のために行うのか、どのような意味を持つのか等、実施の前提について議論すべきではないか。ユーザによる海賊版コンテンツのダウンロード行為が違法か違法でないかによって、違いがあるか。	違法でないコンテンツに対してアクセス抑止を行うことは合理的でないばかりでなく、法的にも問題があります。論点案にあるように、ダウンロード行為が違法であるか否かは重要な違いと考えます。 もっとも、ダウンロードが違法であることの一点をもって、ユーザが違法な行為を行わないために他の利用者を含めた通信の秘密の侵害となるおそれのある手法をとることが許されるかについては、別途十分な検討が必要と考えます。
論点６：アクセス警告方式にはどのようなメリット・効果があると考えられるか。	利用者の同意を適切に取得することを前提に、ブロッキングに比べて利用者の権利を侵害する度合いが低い手段であるとは考えられます。
論点７：アクセス警告方式の実施の前提としての法的整理に関し、個別の同意が必要か、あるいは、包括同意で足りると整理することが可能か。	法的な検討は構成員の先生方に委ねますが、通信の秘密は基本的人権の中でもきわめて重要な表現の自由と密接に関連すること、本件における検討の結果は将来、他の類型のアクセス制限等が検討されるときにも少なからぬ影響を与えることを考えると、慎重な議論を要するところであると考えています。 少なくとも、利用者の知らないうちに同意したことになっているような制度は、通信の秘密を守るべき通信手段に適用されることは好ましくありませんし、拒否の意思表示をすることに萎縮が生じるような場合は、利用者の真摯な同意とはいえません。また、利用者が拒否の申出をした事実自体は通信の秘密とはいえないものの、利用者の内心にかかわる機微な情報であるということもできるため、その管理についても、検討を要すると考えます。
論点８：アクセス警告方式に関する技術的な課題はあるか。	十分な実効性を伴うアクセス警告方式をネットワーク側に実装する場合、現在 ISP

	で採用しているネットワーク機器だけではできず、新たな設備を数多く導入する必要が出てきます。 　これまでわが国では、政府の指示や要請を受けた ISP による検閲のようなことが行われてこなかったため、ISP にもこのような運用のノウハウは蓄積されていません。 　ネットワークの安定運用の点からも、ルーティングに起因する事故は少なからず発生しており、ネットワークに不安定な要素を持ち込むことになるという懸念もあります。 　ネットワークの基幹で設備工事を行う場合、利用者への影響が生じないよう、深夜に通信経路を切り替えながら行うことが一般的です。一度に多くの設備で切り替えを行うことは難しく、工期のかかる作業になることが予想されます。 　ネットワーク構成は ISP によって大きく異なるため、実装のポイントも異なることとなり、それぞれ技術的な課題が生じることにもなります。 　通信方式との関係においても、現在急速に進展している常時 SSL 化（ブラウザとサーバの間で常に暗号化通信をすること）、DNS の不正な乗っ取りを防止するための DNSSEC の普及などは、利用者の安全な通信を実現するためのものである一方、ISP によるアクセス制限やアクセス警告の実施を困難にする要素となります。
論点９：アクセス警告方式の導入及び実施のためのコストについて、どのように考えるか。	わが国には多数の ISP が存在し、規模もネットワーク構成もさまざまです。このため、コストについても各事業者によって大きく異なると考えられますが、高速化・大容量化する通信の中から対象の通信を的確に見分けてアクセス警告をするためには、

	それなりに高額なコストがかかります。 海賊版サイトへのアクセス抑止のために新規の設備を導入する場合、そのコストを誰が負担するかは大きな議論のテーマになります。仮に ISP 事業者が負担することとなれば、それは結局毎月の通信料金に転嫁されることとなり、国民の家計にも影響が生じることとなるため、この点でも国民の理解を得ていく必要があります。
論点 10： その他、導入に当たって、法的・技術的課題以外に検討すべき事項はあるか。	アクセス警告方式で警告の対象となるサイトのリストの作成、管理のための透明かつ中立的観点からのルール作り、運営主体やオペレーション、コストについても検討を行う必要があると考えます。
その他アクセスを効果的に抑制するための方策に係る検討	
論点 11：端末側での対応策にはどのようなメリッ ト・効果があると考えられるか。	端末側においてアクセス警告を実施することは、少なくとも電気通信事業法との関係では通信の秘密との問題が生じないことから、法的な問題は少ないと考えます。 また、ISP のネットワークに新たな設備を導入する必要がないことは、ISP 事業者が直接大きな投資をする必要がないことに加え、導入の迅速性の点でもメリットが大きいと考えます。
論点 12： フィルタリング等の端末側での対応策はどのような方法が考えられるか。	フィルタリングのサービスは既に相当程度普及しているため、フィルタリングソフトの開発元の協力を得て、リストに追加することになると考えられます。 電気通信事業者各社では、インターネット接続サービスの利用者に対し、未成年（青少年）の方が利用する場合にはフィルタリングを利用していただくよう働きかけを行っていますが、当協会としてもフィルタリングの普及啓発に引き続き取り組んでいきます。 また、ブラウザのプラグインやアドオン

	などの機能拡張で実装することができれば、それも選択肢のひとつになります。
論点 13： 端末側での対応策はどのような技術的課題があるか。	既存のフィルタリングは、主に青少年を対象に、不適切なサイトへのアクセスを遮断する機能であるため、成人に対して警告を表示したうえでアクセスの判断を委ねるような機能は実装されていない場合があります。 既存のフィルタリングをベースにしてこれを実装する場合、アプリケーションの開発などが必要となり、開発元をまじえた議論が必要となるでしょう。 ブラウザの機能拡張で実施する場合、標準機能として実装してもらうのであれば、日本国内の事情を開発元にどの程度理解してもらえるかが問題となりますし、プラグインで実装する場合、比較的自由に開発はできる一方で、プラグインを利用者にインストールしてもらう方法が課題となります。いずれであっても、アクセス抑止方策の対象となるサイトのリストの管理を誰がどのように行うかは、別途課題になります。
論点 14： 端末側での対応策の導入及び実施のためのコストについて、どのように考える か。	既存のフィルタリングをベースに考える場合、端末側アプリケーションの開発コストのほかに、フィルタリングソフトの利用料の負担が問題となります。多くのフィルタリングソフトは、ウイルス対策ソフトと同様に年間契約のサービスとして提供されており、ISP 事業者がフィルタリングを提供する場合、ソフトの開発元と包括契約を行い、ユーザ数に応じたライセンス料を支払っているのが一般的です。 ライセンス料はフィルタリングサービスが必要な利用者に転嫁する場合と、青少年の利用者を増やす営業政策の見地から事業者が負担する場合がありますが、成人を含

	めたすべての利用者に対象が広がる場合、スケールメリットは相当生じるものの、ISP事業者だけで負担しきれない金額になることが予想されます。 海賊版サイトへのアクセス警告のために導入する場合、このコストを誰が負担すべきかは議論のテーマであると考えますし、ISP 事業者が負担するとなれば結局利用者の通信料金に転嫁されることになります。
論点 15： その他、端末側での対応策の導入に当たって、法的・技術的課題以外に検討すべき事項はあるか。	端末側でのアクセス警告方式についても、仮に利用の対象を青少年以外に広げ、幅広い国民に対して利用を促すのであれば、その正当性を十分確保し、維持することが重要になります。 具体的には、警告の対象となるサイトのリストの作成、管理のための透明かつ中立的観点からのルール作り、運営主体やオペレーション、コストについても十分な検討を行う必要があると考えます。

以上