資料４―１

インターネット上の海賊版サイトへの
アクセス抑止方策に関する検討会
報告書（案）

令和元年８月５日

目次

第１章　インターネット上の海賊版サイトへのアクセス抑止方策の検討の背景並びに基本的な考え方及び進め方について

１．検討の背景等

近年、スマートフォンの普及が進むとともに、多様なコンテンツアプリケーションの登場に伴ってインターネット上のデータ流通量が増加の一途をたどる中で、ネットワークインフラの大容量化・高速化やコンテンツ処理技術・配信技術等の高度化等により、多くのコンテンツやデータがインターネット上で円滑に流通する環境が実現している。他方で、最近では、悪質かつ大規模な海賊版サイト（マンガやアニメなどのコンテンツが権利者の承諾なく違法にアップロードされているサイトをいう。以下同じ。）の登場が、権利者の利益を著しく損なうなどの点で大きな社会問題となっている。

インターネット上の海賊版対策に関しては、2018 年（平成 30 年）６月の「知的財産推進計画 2018」（知的財産戦略本部決定）において、インターネット上で流通する模倣品・海賊版対策について、有識者及び関係府省における検討の場を設けることとされ、知的財産戦略本部の検証・評価・企画委員会の下に「インターネット上の海賊版対策に関する検討会議（タスクフォース）（共同座長：中村伊知哉 慶應義塾大学大学院メディアデザイン研究科教授、村井純 慶応義塾大学大学院政策・メディア研究科委員長）」が設置された。同タスクフォースにおいては、（１）正規版流通の更なる拡大によるコンテンツ視聴環境の整備、（２）現行法令下での既存の海賊版対策の取組状況の検証及び実効性評価、（３）特に悪質な海賊版サイトに対する権利行使を可能とする法制度整備の在り方等が検討事項とされ、同年６月～10 月の間に９回の会合が開催された。この検討の中で、海賊版対策の一つのメニューとして「アクセス警告方式」についても提案がなされた。

同タスクフォースでの検討を踏まえて、2018 年 10 月に開催された「検証・評価・企画委員会コンテンツ分野会合」（第１回）において、同タスクフォースの両座長より、以下（抜粋）のとおり検討状況報告がなされた。

「権利者、インターネットサービス事業者、学識経験者、法律家などの関係者を一堂に集めて、コンテンツの流通の促進、既存の海賊版対策の検証・評価、アクセス遮断の法制度化も含めた総合的対策について、短期間に９回にわたる集中的な議論を行った。

その結果、著作権教育・意識啓発、海賊版対策に資する出版業界・通信業界における環境整備、海賊版サイトに対する広告出稿の自主的な抑制、フィルタリングの

強化等、関係者が民間主導で連携して取り組むべき対策のほか、関係省庁の連携等によるリーチサイト規制の法制化、著作権を侵害する静止画（書籍）のダウンロードの違法化の検討等、様々な側面から直ちに取り掛かることが必要な内容について、共通の認識が得られた。しかし、いわゆるブロッキングに関する法制度整備について、議論をまとめることはできなかった。（中略）

今後、権利者、インターネット関係事業者、関係省庁等が連携して、海賊版の撲滅に向けて取り組んでいくことを心より期待する。」

また、2019 年（平成 31 年）３月に開催された「検証・評価・企画委員会コンテンツ分野会合」（第４回）において、インターネット上の海賊版への総合的な対策メニュー（案）（以下「総合的対策メニュー（案）」という。）[1]が示され、同メニュー（案）中において、「アクセス警告方式」に関して、「法制度の変更を前提とせずにユーザのアクセス抑止効果を最大限高める方式を検討し、海賊版サイトへの対策として実効的な枠組みを提示した上で、速やかに導入する（関係者と協議しながら検討・導入）」旨の記述等が盛り込まれた。

本検討会は、以上の経緯を踏まえて、海賊版サイトへのアクセス抑止に資する方策の導入を支援するため、その実施の前提となる法的整理、導入・実施に当たっての技術的可能性等について、ユーザの通信の秘密の保護やインターネットの自由な利用の確保等にも配慮しつつ検討を行ったほか、併せて、フィルタリングなどの手法を含めた効果的な方策の在り方について検討を行ったものである。

２．検討に当たっての基本的な考え方及び進め方

本検討会においては、インターネット上の海賊版対策を検討するに当たり、以下の基本的な考え方及び進め方の下で行っていくことが必要との認識に立って検討を進めた。

[1] 「インターネット上の海賊版対策に関する検討会議」等の議論を踏まえ、海賊版による被害を効果的に防ぎ、著作権者等の正当な利益を確保するため、以下に掲げる対策を段階的に実施するものとされた。①著作権教育・普及啓発、②正規版の流通促進、③海賊版サイト対策の中心となる組織の設置、④国際連携・国際執行の強化、⑤検索サイト対策、⑥海賊版サイトへの広告出稿の抑制、⑦フィルタリング、⑧アクセス警告方式、⑨リーチサイト対策、⑩著作権を侵害する静止画（書籍）のダウンロード違法化、⑪ブロッキング。このうち、①～⑦及びアクセス警告方式の検討については「できることから直ちに実施」、アクセス警告方式の導入及び⑨～⑩については「導入・法案提出に向けて準備」、⑪については「他の取組の効果や被害状況等を見ながら検討」とされた。

（１）関係者の共通認識の下での検討

アクセス抑止方策を含め、インターネット上の海賊版対策の在り方について適切な結論を得るためには、まずは、インターネット上の海賊版による被害の状況、海賊版に対処するための出版業界等における取組の状況、海賊版サイトへのアクセス抑止方策の導入・利用に係るユーザの意識や意向、アクセス抑止方策の実現に係る技術的な課題・動向などの現状について、関係者の共通認識の下で検討を進めることが重要である。

なお、本検討会においては、こうした観点から、インターネット上の海賊版による被害状況や海賊版サイトに対処するための取組等について出版業界からヒアリングを行い、検討の論点に対する意見募集[2]（以下「意見募集」という。）やアクセス抑止方策に関する一般ネットユーザへのアンケート調査[3]（以下「アンケート調査」という。）を実施してユーザの意識や意向を把握し、アクセス警告方式の実現に係る技術的な課題とコスト試算について電気通信事業者団体からのヒアリングを実施することにより、幅広い関係者の共通認識の下で検討を行うことに留意しつつ、結論を得ることとした。

ア　インターネット上の海賊版サイトによる被害状況

本検討会の第１回会合では、オブザーバの出版広報センターから、インターネット上の出版物海賊版サイトの最新状況についてヒアリングを行った。出版広報センターの調査によると、2019 年４月時点で把握しているアクセス数が多い 10 サイトのうち、６つがリーチサイト型[4]となっており、現在の主流はリーチサイト型であるといえる。

また、出版広報センターの試算によると、最大手リーチサイトを経由してダウンロードされている侵害ファイル数は１ヶ月あたり 260 万件に上る。また、１ファイルにコミックス数巻がまとめられているケースも多いことから、コミックスの数に換算すると 260 万をはるかに超える数がダウンロードされている

[2] 本検討会における「アクセス抑止方策に係る検討の論点」について、議論の透明性を高め、幅広い関係者の声を踏まえた上で議論を進める観点から、提案募集を実施。実施期間は 2019 年4月 24 日から 2019 年（令和元年）5月 14 日。計 129 件（うち法人又は団体 14 件、個人 115 件）の意見が寄せられた。

[3] 実施期間は 2019 年5月 16 日から同月 17 日。調査対象は 15 歳から 69 歳までの男女。（「Macromill 推計インターネット週1以上利用者基幹人口（H29 年版）」の構成比に基づきサンプルサイズを決定した後、無作為抽出）。回答者数は 2067 人。（株式会社マクロミルの提供するインターネットリサーチサービスにより実施。）。

[4] 自身の web サイトにはコンテンツを掲載せず、他の web サイトに蔵置された著作権侵害コンテンツへのリンク情報を提供して、利用者を侵害コンテンツへ誘導することにより、侵害コンテンツへのアクセスを容易にし、著作権侵害を助長しているサイトをいう。

可能性がある。

イ　海賊版サイトに対処するための取組状況

海賊版サイトに対処するための取組状況についても、出版広報センターから同様にヒアリングを行った。出版広報センターによると、出版業界が実施してきた取組は以下のとおりである。

①海賊版サイトへの削除要請・警告書の送付
②国内外のネット接続業者、サーバ、サービスへの削除要請・警告書の送付
③ドメイン登録業者への閉鎖要請
④リーチサイトが使用するサイバーロッカーへの削除要請
⑤裁判所での発信者情報開示請求仮処分手続
⑥Google などへの検索結果からの表示抑制要請及び Google との連携
⑦インターネット広告の海賊版サイトへの出稿停止要請
⑧「FreeBooks」に対する出版社連合による海外サーバに対しての現地での法的アクション
⑨「マンガパンダ」「はるか夢の址」「ネタバレサイト」「漢化組」（中国語の翻訳海賊版組織）に関する警察と連携した摘発[5]
⑩普及啓蒙活動（STOP!海賊版キャンペーンや ABJ マークの策定等）
⑪関係省庁、関連団体との連携・情報共有

これらの対策により、年間 200 もの海賊版サイトを閉鎖に追い込むも、ドメインサーバの移転や新規サイトの誕生により、海賊版サイトの根絶には至っていない状況である[6]。

（２）あるべきネットワークの姿を踏まえた検討

インターネットは、その成り立ちから、システム全体を制御・統治する主体がおらず、自律・分散した各構成要素の協調作業によって全体のシステムを機能させる、いわゆる自立分散協調型のシステムであり、このことがインターネットを拡張性が高い（スケーラブルな）ネットワークたらしめている。また、インター

[5] これ以外にも、多い社では年間に 10 件以上の刑事事件と関わっているとのことである。

[6] 被害額が非常に大きいとされており問題視されていた海賊版サイト「漫画村」(2018 年4月にサイト閉鎖済)に関しては、福岡県警を含む合同捜査本部が著作権法違反の容疑で捜査を行ってきたところ。また、2019 年7月には、同サイトの運営者がフィリピンの入国管理局により拘束され、日本国内においても、その共犯者2名が逮捕されたとの報道があった。

ネットの普及が進んだ今日においては、インターネットは、新たなサービスやビジネスを創出し、イノベーションを促進するなど、経済成長のエンジンとなっており、さらに、ユーザの表現活動や知る権利を支える重要な基盤としての役割を果たしていることを踏まえて、今後ともこうした特徴や役割を阻害することなく、インターネットがユーザや経済社会にもたらす便益を最大限に引き出すことができるよう、あるべきネットワークの姿とは何かといった点についても十分に考慮した上で、結論を得ることが重要である。

（３）ユーザの意識や意向を踏まえた検討

さらに、具体的な方策の検討に当たっては、これらの方策が海賊版サイトにアクセスするユーザにとどまらず、それ以外の多くのネットユーザにも影響があり得ること、特に、当該施策が、本来海賊版サイトへのアクセスとは無関係なネットユーザー般のインターネット利用を制限することになりかねないことに鑑みれば、ユーザの声に幅広く耳を傾け、ユーザの意識や意向を十分に踏まえた上で、結論を得ることが重要である。

したがって、本検討会において実施した意見募集に寄せられたユーザの意見やアンケート調査の結果を十分に考慮することが重要である。

第２章　ネットワーク側におけるアクセス抑止方策（アクセス警告方式）

１．アクセス警告方式の概要

本報告書において、「アクセス警告方式」とは、ユーザの同意に基づき、インターネット接続サービスを提供する電気通信事業者（以下「ISP」という。）が、ネットワーク上でユーザのアクセス先（海賊版サイト以外のサイトへのアクセスも含む。以下同じ。）をチェックし、ユーザによる海賊版サイトへのアクセスを検知した場合に、「本当に海賊版サイトにアクセスしますか？（はい/いいえ）」等の警告画面を表示させるなどの仕組みをいう。

警告画面を表示することで、ユーザに対して海賊版サイトにアクセスしようとしている旨の注意喚起を行い、主としてカジュアル・ユーザ（当該サイトが海賊版サイトであることの認識が薄いユーザや、海賊版サイトへのアクセス頻度がそれほど高くないユーザなどをいう。以下同じ。）が自らアクセスすることを思いとどまることを促そうとするのが、同方式の狙いである。

警告画面を表示するためには、ISP はユーザのアクセス先をチェックする必要があるが、あらかじめユーザの同意を取得することにより通信の秘密に関する問題を生じさせることなく実施し得る点、また、警告画面の表示やそのために必要なアクセス先のチェックを望まないユーザについては実施対象としない（オプトアウト）など、ユーザの意思を尊重した仕組みである点において、いわゆるサイトブロッキングとの違い[7]がある。

２．アクセス警告方式の意義・役割

アクセス警告方式の目的は、カジュアル・ユーザが警告画面表示を見て、インターネット上のマンガ・アニメなどの海賊版サイトへのアクセスを思いとどまることを促し、これによって海賊版サイトへのアクセス数を減らし、著作権者の被害を最小限にすることである。

また、これに加えて、著作権を侵害するものと知りながら静止画（電子書籍）をダウンロードする行為（以下「ダウンロード行為」という。）が違法とされる場合[8]

---

[7] アクセス警告方式とブロッキングは、いずれも ISP がネットワーク上でユーザのアクセス先をチェックする必要があり、形式上は通信の秘密の侵害に該当するといった問題が生じ得る点が共通する。

[8] 2019 年7月時点における著作権法上、海賊版と知りながら静止画（電子書籍）をダウンロードする行為は違法ではないものの、今後、著作権を侵害する静止画（書籍）のダウンロードの違法化のための法制度整備を

には、ISP が警告画面を表示することは、ユーザに対してダウンロード行為が違法であることを知らせる意味や、ユーザが意図せず海賊版サイトにアクセスして違法行為を行ってしまうことを防ぐ意味があると考えられる。

したがって、ダウンロード行為が違法とされる場合には、そうでない場合に比べて、アクセス警告方式の実施に対するユーザの理解が得られやすくなる面があるとも考えられる[9]。

この点、アンケート調査の結果によると、海賊版サイトにアクセスした際に警告画面が表示された場合、アクセスを思いとどまる人の割合は、現行法の場合（ダウンロード行為が違法ではない場合）で 93.3%、ダウンロード行為が違法化されると想定した場合で 95.9%となっている。これを踏まえれば、ダウンロード行為が違法とされたとしても、実際には、必ずしも多くのユーザが対応を変化させるとは限らず、また、アクセス警告方式の意義や役割に対するユーザの意識や意向も、ダウンロード行為が違法とされるか否かによって大きな違いはないものと考えられる[10]。

３．アクセス警告方式の効果・メリット

アンケート調査の結果によると、海賊版サイトにアクセスした際に警告画面が表示された場合、アクセスを思いとどまる人の割合は、現行法の場合（ダウンロード行為が違法ではない場合）で 93.3%、ダウンロード行為が違法化されると想定した場合で 95.9%となっている（再掲）。この調査結果から、警告画面を表示させることで、多くのユーザが海賊版サイトにアクセスすることを思いとどまるものと見込まれることから、アクセス警告方式には海賊版対策として一定の効果が見込まれると考えることができる。また、警告表示（注意喚起）の効果については、２．で示したとおり、ダウンロード行為が違法とされるか否かによって大きな違いはないものと考えられる。

また、ブロッキングはユーザの意思に反する場合であっても実施するものであるのに対して、アクセス警告方式はユーザの同意を取得することを前提として実施す

速やかに行うこととされている（2019 年3月 29 日 知的財産戦略本部 検証・評価・企画委員会コンテンツ分野会合（第4回）資料参照。）。なお、動画及び音楽については、現行法上、海賊版と知りながらダウンロードする行為は違法とされている。

[9] 意見募集においても、電気通信事業者により構成される団体から、ISP がアクセス警告方式を実施する際のユーザへの説明の局面では、ダウンロード行為が違法である場合の方が、説明が容易で理解を得やすいものと考える旨の意見が提出された。

[10] 意見募集に対する意見：「ダウンロード違法化が行われることで違いが生じる」同旨4件、「ダウンロード違法化の有無による違いはない」同旨9件。

るものであることから（後述）、プライバシーや通信の秘密の保護の観点で、ブロッキングのような様々な課題を生じさせることなく実施することができるという面がある。

なお、意見募集においては、メリットはあるが限定的である旨の意見や、メリットよりもデメリットの方が大きい旨の意見も寄せられている[11]。

４．アクセス警告方式の実施の前提となる法的整理

（１）「通信の秘密」の保護規定の基本的な考え方

日本国憲法第 21 条は、基本的人権の一つとして表現の自由を保障するとともに（第１項）、通信の秘密の保護について規定している（第２項後段）。同条は、表現の自由の保障と通信の秘密の保護を併せて規定している。すなわち、憲法において通信の秘密を保護する意義は、国民のプライバシーの保護にとどまらず、国民の表現の自由や知る権利を保障すること、さらに、国家権力が自ら通信の秘密を侵害しないのみならず、私人による侵害から通信の秘密を保護し、国民が安全・安心に利用できる通信制度を保障することにより、国民の通信の自由を確保することにあると考えられる。

電気通信事業法（昭和 59 年法律第 86 号）においては、通信の秘密の保護に関して、「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。」（第４条第１項）と定めている[12]。同規定は上記憲法上の要請を担保するために法律レベルで具体化したものであると考えることができる。つまり、同法の通信の秘密の保護規定は、これによって電気通信事業者を含めて何人からも通信がみだりに侵害されないよう利用者の通信を保護し、もって利用者が安心して通信を利用できるようにすることで、表現の自由や知る権利を保障するとともに、電気通信ネットワークや通信制度そのものへの利用者の信頼を確保し、多様なサービスやビジネスの実現による電気通信の健全な発展と国民の利便の確保を図ることが、その意義であると考えられる。

---

[11] 意見募集に対する意見：「アクセス警告方式にはメリットがある」同旨4件、「アクセス警告方式にはメリットはあるが限定的（具体的には、「他の国々がアクセス警告方式に類似した措置を実施したが、大きな成果は得られなかった」など）」6件、「アクセス警告方式のメリットはない・デメリットが大きい（具体的には、「ISP がアクセス警告方式を実施するためにユーザのアクセス先をチェックする行為は、表現の自由や通信の秘密などの国民の基本的な権利の制限に直結する」「ユーザのネット利用を畏縮させるおそれがある」「海賊版サイトに警告表示がされない場合などには『このサイトには警告が出てこないから合法サイトである』という誤解を生むおそれがある」など）」14 件。

[12] 後述のように、通信の秘密を侵した者に対しては刑事罰が設けられている（第 179 条）。

こうした趣旨に鑑み、従来から、「通信の秘密」の範囲には、個別の通信に係る通信内容のほか、個別の通信に係る通信の日時、場所、通信当事者の氏名、住所・居所、電話番号などの当事者の識別符号、通信回数等これらの事項を知られることによって通信の意味内容を推知されるような事項全てが含まれると整理がなされている。

また、通信の秘密を侵害する行為としては、「知得」（積極的に通信の秘密を知ろうとする意思の下で知ろうとする行為）、「窃用」（発信者又は受信者の意思に反して利用すること）、「漏えい」（他人が知り得る状態に置くこと）の３類型がある。通信の秘密を侵害した者に対しては、処罰規定が設けられており（電気通信事業法第 179 条第１項）、特に、電気通信事業者には通信の秘密の厳格な保護が求められており、通信の秘密の侵害罪について電気通信事業に従事する者にはより重い法定刑が規定され（同法第 179 条第２項）、こうした規定によって、電気通信事業者による通信の秘密の厳格な保護の確保が図られている。

ただし、利用者の同意がある場合には、通信の秘密の侵害に当たらないほか、通信の秘密を侵害した場合であっても、正当行為（刑法（明治 40 年法律第 45 号）第 35 条）、正当防衛（同法第 36 条）、緊急避難（同法第 37 条）に当たる場合等違法性阻却事由がある場合には、例外的に通信の秘密を侵すことが許容される、と解されている。

なお、意見募集においては、通信の秘密のほか、検閲の規定との関係における懸念や課題を提起する意見が複数寄せられた。アクセス警告方式と検閲の関係を考える場合、検閲は通信の秘密の侵害を前提とする形で行われるのが通常であると考えられることから、ここではまず通信の秘密との関係について整理を行うこととする。

（２）ユーザの有効な同意の考え方について

アクセス警告方式を実施するためには、ISP がユーザのアクセス先を検知する必要があり、また、ユーザが海賊版サイトへアクセスしようとする場合にアクセス先に接続する際に警告画面を表示することとなるが、ISP がユーザの通信の秘密を違法に侵害することなくこれらを実施するためには、あらかじめユーザの有効な同意を取得することが不可欠の前提条件である。すなわち、アクセス警告方式は、ユーザの有効な同意を取得することによって、ユーザの通信の秘密を違法に侵害することなく、海賊版サイトへのアクセスを抑止することを可能とするも

のである。

そこで、アクセス警告方式において、どのような形での同意があれば、有効な同意があると考えることができるかについて検討する[13]。

この点、有効な同意があるといえるのは、ユーザに通信の秘密を侵すことに対する認識・認容がある場合をいい、外形的に見ても明確な同意を取得することが要求されることから、通常は、契約約款等に基づく事前の包括的な同意（以下、単に「包括同意」ということがある。）のみでは有効な同意とは解されず、原則として個別具体的かつ明確な同意（以下、単に「個別同意」ということがある。）[14]が必要とされている。その理由は、契約約款は当事者の同意が推定可能な事項を定める性質のものであり、①通信の秘密の利益を放棄させる内容は、通常その性質になじまないこと、②事前の包括同意は将来の事実に対する予測に基づいて行われることからその対象、範囲が不明確となることにある。

もっとも、上記①・②のような理由が当てはまらない例外的な場合には、契約約款等による事前の包括同意であっても有効な同意といえる。すなわち、①’ ISPにおいて通信の秘密を侵すことについて、一般的・類型的に見て、通常のユーザであれば承諾すると想定し得るため、契約約款等による同意になじまないとはいえない場合であって、②’ ユーザに将来不測の不利益が生じるおそれがない場合がこれに当たる。

このうち②’の「ユーザに将来不測の不利益が生じるおそれがない」といえるか否かを判断するに当たっては、

・ユーザが、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）できる契約内容であること
・同意（及びその変更）の有無にかかわらずその他の条件が同一であるなど、同意しないユーザの利益が侵害されないようにすること
・当該契約約款等の内容や、事後的に同意内容を変更（設定変更）できること及びその変更方法についてユーザに相応の周知や説明がされていること

といった点を考慮する必要があるが、まずはアクセス警告方式において、上記①’の条件、すなわち、ISP が海賊版サイトへのアクセスを警告することを目的として、ユーザのアクセス先を検知し、警告画面を表示することについて、「一般的・

[13] なお、上記(1)のとおり、違法性阻却事由がある場合には、例外的に通信の秘密を侵すことが許容されると解されているが、アクセス警告方式とはユーザの同意を取得して実施することが前提とされていることから、アクセス警告方式に係る違法性阻却事由については検討を行わない。

[14] 具体的には、通信の秘密の取扱いについての同意であることを本人が認識した上で行う「個別」の同意であり、かつ、画面上での操作や文書による同意など外部的に同意の事実が「明確」な同意を意味している。

類型的に見て、通常のユーザであれば承諾すると想定し得る」か否かが問題となる。

アクセス警告方式を実施するに当たっては、ISP が個々のユーザに対して意向を確認し、個別具体的かつ明確な同意を取得することは負担になり得ることから、包括同意によって通信の秘密に関する有効な同意が得られると考えることができるかどうかについて検討する。

（３）有効な同意についてのユーザの意識・意向について

ISP がアクセス警告方式を実施するに当たり、包括同意によって通信の秘密に関する有効な同意を取得することができるか、あるいは、個々のユーザに対して個別同意を取得する必要があるかについて、上記（２）を踏まえて検討する。この点、本検討会においては、「一般的・類型的に見て、通常のユーザであれば承諾すると想定し得る」か否かの判断に当たっては、専門家による規範的な判断のみならず、幅広く、かつ、偏りなく現実のユーザの意向・意識を把握した上で結論を得ることが必要との観点から、アンケート調査を実施したほか、意見募集を実施した。

このアンケート調査においては、アクセス警告方式の実施に際して ISP がアクセス先をチェックすることについて「一定の場合は許容できる」又は「全く気にならない」と回答した人の割合は、現行法の場合 44.7%、ダウンロード行為が違法化されると想定した場合 46.8%であり、いずれも５割にも満たない結果となっている。

また、意見募集においては、ISP がアクセス警告方式を実施することに対して、通信の秘密や検閲といった観点から慎重又は否定的な意見が多く提出された[15]ほか、包括同意を有効な同意と整理することに対する意見として、「運用によっては国民の基本的な権利に抵触しかねないことから、個別の同意を取得すべき」「『通信の秘密』を侵しうる重要な事項がこのような気づきにくい方法で同意を求めることは極めて不適切」といった旨の意見も見られた[16]。

---

[15] 意見募集に対する意見:「総論としてアクセス警告方式に反対」同旨 64 件、「アクセス警告方式は通信の秘密を侵害する・通信の秘密への影響が大きい」同旨 45 件、「アクセス警告方式は国家による監視・検閲行為である」同旨 31 件。

[16] 意見募集に対する意見:「包括同意ではなく、個別同意が必要」同旨7件、「ユーザが約款に気づかずに同意したり意味を正しく理解せずに同意することになるので不適切・通常の利用者であれば承諾するという想定が困難」同旨9件、「契約法の原則に照らして無効・不当条項にあたる」同旨8件、「セキュリティ対策にお

なお、ダウンロード行為が違法とされる場合か否かで、これらのユーザの意識・意向に大きな違いは見られなかった[17]。

（４）法的整理についてのまとめ

上記（３）のとおり、現時点でのユーザの意識・意向を踏まえると、アクセス警告方式の実施について、「一般的・類型的に見て、通常のユーザであれば承諾すると想定し得る」とはいえないと考えられる。したがって、ISP は、ユーザから個別具体的かつ明確な同意を取得する場合にはアクセス警告方式を実施することは可能であるが、現状では、契約約款等による包括同意を有効な同意とみることは困難と考えられる。

また、この点は、ダウンロード行為が違法とされる場合であっても同様に考えられる。

５．アクセス警告方式の導入及び実施のための技術的な課題及びコスト

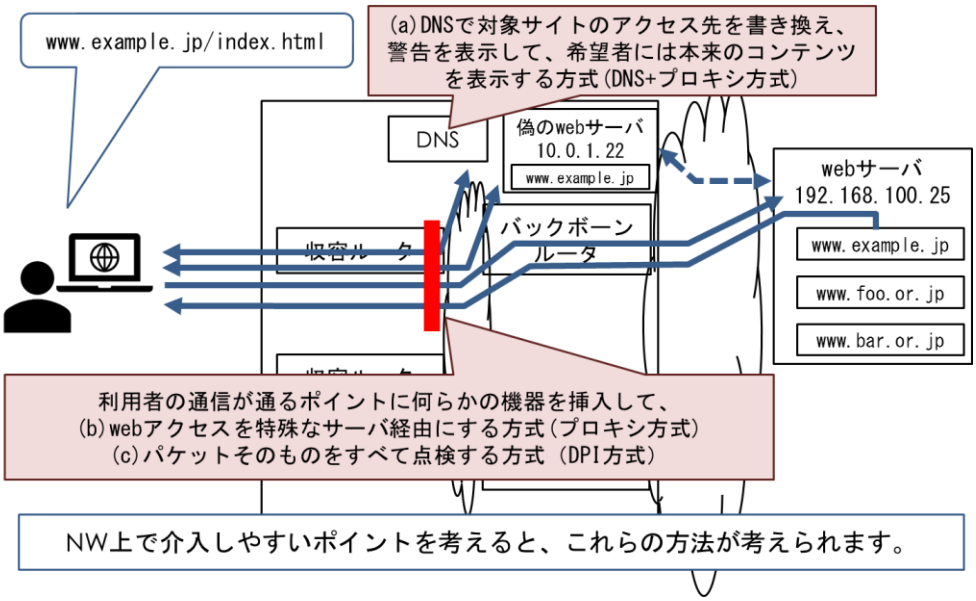
（１）アクセス警告方式の実装方法及びコストについて

アクセス警告方式の導入及び実施に当たっては、いかなる技術的な課題があるかについても検討が必要との観点から、本検討会では技術的な課題について電気通信事業者団体からのヒアリング等を通じて検討を深めた。

ISP による実装方法として、現在の技術レベルやネットワークに対する考え方を前提とすると、具体的には、主に以下の手法（図１中の(a)～(c)）が考えられる。

ける包括同意の考え方を著作権侵害対策に転用すべきではない」同旨4件、「たとえ同意があっても許されない」同旨 10 件。

[17] 意見募集に対する意見:「ダウンロード違法化が行われることで違いが生じる」同旨4件、「ダウンロード違法化の有無による違いはない」同旨9件。
アンケート結果:アクセス警告方式に際して通信事業者にアクセス先をチェックされることについて「許容できる / 気にならない」と回答した人の割合は、現行法の場合 44.7%、静止画ダウンロード違法化想定の場合 46.8%(再掲)。



【図1　アクセス警告方式の実装方法】[18]

(a)DNS＋プロキシ方式

DNS＋プロキシ方式とは、ユーザが海賊版サイトにアクセスしようとした場合に DNS サーバ上で当該アクセスを検知し、アクセス先を海賊版サイトから警告画面を表示するサイトに書き換え、別のサーバ（プロキシサーバ）に誘導して警告画面を表示する手法である。

(b)プロキシ方式

プロキシ方式とは、ISP において新たに用意するプロキシサーバを経由してユーザによる web サイトへのアクセスを提供し、同サーバにおいて警告画面の表示や本来のコンテンツの表示の切替え等を行う手法である。

(c)DPI 方式

DPI 方式とは、ISP の管理するネットワークにパケットの中身を解析する機能（DPI 装置）を実装する手法である。基本的にはユーザの通信の全てを検知・制御することが可能である点が特徴として挙げられる。

（２）技術的課題とコスト負担の在り方

ア　各手法における課題とコスト

(a)DNS＋プロキシ方式

[18] 本検討会資料2－3「アクセス警告方式を ISP 事業者が行う場合の技術的な検討と課題」（一般社団法人日本インターネットプロバイダー協会）8頁。

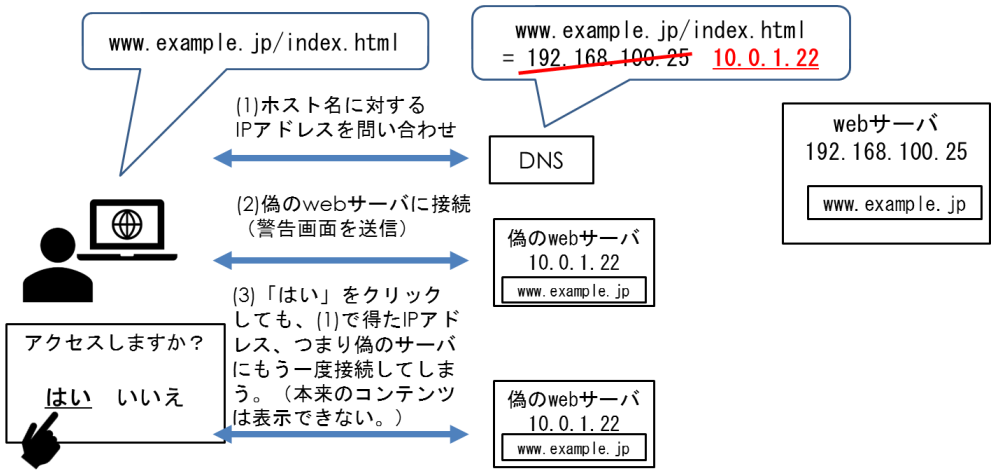
DNS＋プロキシ方式では、海賊版サイトへのアクセスを検知した場合に、DNSサーバで警告表示用の偽のサーバにアクセスさせても、警告画面上で「はい」を押した場合、DNS サーバを介して警告画面用サーバに再びアクセスしてしまうため、本来の海賊版サイトへアクセスさせることができない（図２参照）。そのため、cookie 等の仕組みにより、警告画面用サーバに２度目にアクセスした場合には、警告画面用サーバがプロキシとして機能し、本来の海賊版サイトからコンテンツを代理取得する方法が考えられる（図３参照）。これらの仕組みは、商用ネットワークでの実績が少なく、また、簡易な方法のため、本来遮断すべきでない通信を止めてしまう可能性があるという課題がある[19]。その他、プロキシサーバでの処理が介在することから、DNS サーバで選別した対象となる通信に関して遅延が発生する可能性がある。

コストについては、プロキシサーバ（１社当たり１台～２台と仮定）、オプトアウト用の DNS サーバ（１社当たり２台～４台と仮定）に加え、事業者によっては、対象ホスト名のリストと DNS の連携機能や、オプトアウト用 DNS サーバの指定を顧客 DB と連携する機能の追加が必要となることが想定される。[20]

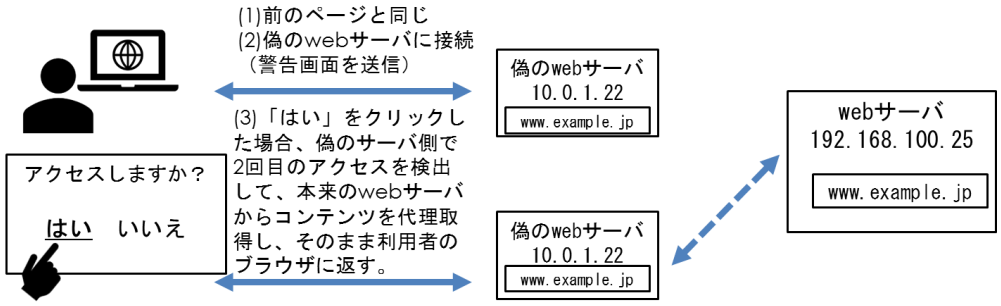
---

[19] 具体的には、アクセス警告方式の対象となる海賊版サイトの web サーバと同じホスト名で運用されているメールサーバ宛ての通信等が遮断される可能性があると考えられる。

[20] ３つの方式のうち、最もコストが安価であると想定される(a)DNS＋プロキシ方式について、最小構成の場合、初期費用 18 億＋2 千万円/月、より現実的な構成の場合は初期費用 46 億円＋1億円/月（全国の固定系 ISP を対象とした試算。固定系ISPが全国に 1000 社あると仮定し、その全ての社がアクセス警告方式を導入する場合の総額。）という試算が通信事業者により構成される団体から示された。最小構成の場合、1社当たりの導入費として、プロキシサーバ 30 万円、設定・導入に 50 万円、運用マニュアル・教育費に 100 万円、運用費としてプロキシサーバ1台当たり2万円/月と想定。この仕様の場合、オプトアウトができない、サーバ故障時は対象サイトへのアクセスがしばらく停止するおそれがある、対象リストの更新は手動という前提。より現実的な構成の場合、1社当たりの導入費として、プロキシサーバ 30 万円×2台、設定・導入に 200 万円、運用マニュアル・教育費に 100 万円、オプトアウト用 DNS サーバに 50 万円×2台、運用費としてプロキシサーバ2万円/月×2台、DNS サーバ3万円/月×2台と想定。この仕様の場合、ISP のサービスの範囲内でオプトアウトが可能（各自 DNS の設定を変更）、プロキシサーバを冗長化、リスト更新は自動（ただし、リスト作成管理団体が自動処理に対応する必要）という前提。ユーザごとにアクセス警告方式を実施するかしないかについて管理するためのシステム構築（顧客管理系システムとの連携）にも、会社の規模によっても異なるものの、相当のコストがかかる可能性がある。また、いずれの構成であっても、プロキシサーバ及び DNS サーバはISPが自らのサービスの責任範囲内で設置することを前提としている。これらの試算の前提として、ネットワークの構成・運用は事業者によって大きく異なり、実際に導入する場合には、どのようなグレードのシステムを導入するかによって金額は大きく変わりうることに留意が必要である（本検討会資料２－３「アクセス警告方式を ISP 事業者が行う場合の技術的な検討と課題」（一般社団法人日本インターネットプロバイダー協会）13-15 頁）。



【図2 DNS＋プロキシ方式①】[21]



【図3 DNS＋プロキシ方式②】[22]

(b) プロキシ方式

プロキシ方式では、(a) の DNS＋プロキシ方式と異なり、ユーザのすべての web 通信をプロキシサーバ経由にして処理を行う必要が生じると考えられることから、全ての通信で遅延が生じる可能性があるほか、現在の関連機器・システムのコスト水準を前提とすると、同サーバの設置・運営・管理費用が膨らみ、上記(a)に比べて多額のコストが生じるものと見込まれる。

(C) DPI 方式

DPI 方式におけるコストについては、DPI 装置は一般的に高価であることに加え、ユーザの通信に含まれる個々のパケットレベルで処理を行うため、DPI 装

[21] 本検討会資料2-3「アクセス警告方式を ISP 事業者が行う場合の技術的な検討と課題」(一般社団法人日本インターネットプロバイダー協会) 10 頁。

[22] 本検討会資料2-3「アクセス警告方式を ISP 事業者が行う場合の技術的な検討と課題」(一般社団法人日本インターネットプロバイダー協会) 11 頁。

置をネットワークの中でも個々のユーザ側に近い箇所に設置し、全てのトラヒックに対応する台数が必要となる。このため、現在の関連機器・システムのコスト水準を前提とすると、上記(a)に比べて非常に多額のコストが見込まれる[23]。

イ　暗号化通信における課題

上記(a)～(c)の方式に共通する全般的な技術的課題として、SSL（TLS）を用いたブラウザからwebサイトへの暗号化通信（いわゆる“HTTPS”）の場合には警告画面の表示が極めて困難であるという点が挙げられる。

インターネットの技術的動向として、通信はエンド(ユーザ)からエンド(webサーバ)まで、内容を変えずにそのまま届けることが本来のネットワークの在り方であるという、いわゆる「End to Endの原則」の考えの下で、セキュアな通信を確保し、盗聴、改ざん、なりすましへの対策として、通信を常時暗号化する動きが進んでいる[24]。SSL（TLS）は、通信の前に宛先となるサーバの電子証明書を検証し、本物のサーバであることが確認できれば通信を継続する仕組みである。

海賊版サイトが暗号化通信に対応している場合、ブラウザは海賊版サイトが保有している電子証明書を検証することとなる。その際、ISPがアクセス警告方式を導入していずれかの方式で警告画面を表示させる場合、警告画面用のサーバは本来の通信の宛先である海賊版サイトの電子証明書を保有していないため、ブラウザは電子証明書の検証に失敗し、エラー画面が表示されてしまい、警告画面を表示できない[25] [26]。

このような証明書エラーの問題を回避し、警告画面を表示させるためには、ISPが保有する警告画面表示用のサーバの証明書を「信頼できるルート証明書」

---

[23] わが国のダウンロードトラヒックは、固定系だけで1日平均で約 11Tbps(「我が国のインターネットにおけるトラヒックの集計結果（2018 年 11 月分）」2019 年3月5日総務省報道発表資料 http://www.soumu.go.jp/menu_news/s-news/01kiban04_02000148.html 参照)であり、ピークは2倍～3倍と考えると、少なくとも33Tbpsのトラヒックに対応するDPI装置が必要となる。また、10Gbps用の装置の価格は1台2000万円～5000万円とされる。

[24] 日本のユーザのHTTPSアクセス割合:73%(2019年4月)(本検討会資料2－3「アクセス警告方式をISP事業者が行う場合の技術的な検討と課題」(一般社団法人日本インターネットプロバイダー協会)36頁)。

[25] 電子証明書の検証に失敗した場合の処理はブラウザの実装や設定によって異なるが、基本的にはエラー画面が表示されることが通常である。

[26] その他、サイトブロッキングを実施する場合にも、ユーザに対してブロッキングを実施していることについての説明責任が必要であると考えられるところ、暗号化通信の場合にはブロッキングを実施している旨の説明画面表示を行うことができないという課題があるとの指摘が構成員等から示された。

としてユーザのブラウザに追加してもらう方法が考えられるが、そのような方法はセキュリティリテラシーの観点から適切ではなく、現実的な対応策ではないと考えられる[27]。

ウ　その他コストに対する考え方

アクセス警告方式を導入するためのコストについては、各手法によって大きく異なると考えられるほか、プロバイダの規模・バックアップ等の設備投資の在り方などによっても大きな差が生じる。また、我が国には多数の ISP が存在し、ISP ごとにそのネットワーク構成・設備構成は多種多様であることから、ISP ごとに追加的な技術的課題やコストの問題が生じ得るおそれもある。

なお、コスト負担の在り方については、関係する民間事業者間において協議・検討されるべきものであるが、意見募集においては、例えば、実施のためのコストは原則として受益者負担とすべき旨の意見、通信事業者が負担することとなればユーザに転嫁されることも踏まえユーザの理解を得ていく必要がある旨の意見等が寄せられたことを踏まえて、慎重かつ丁寧な協議・検討が必要と考えられる[28]。

（３）アクセス警告方式の技術的な課題及びコストのまとめ

前述のとおり、ISP がアクセス警告方式を実装する方法としては、現在の技術レベルやネットワークに対する考え方を前提とすると、主に(a)DNS＋プロキシ方式、(b)プロキシ方式、(c)DPI 方式が考えられる。(a)の簡易な方法を採る場合にはコスト面が相対的に安価であるものの、本来遮断すべきでない通信を止めてしまう可能性や、通信の遅延が発生する可能性があるといった技術的課題がある。(b)及び(c)の方式は、全国の ISP で導入することを想定した場合には多額なコストが見込まれるといった課題がある。また、(a)～(c)の方式に共通する全般的な技術的課題として、海賊版サイトが暗号化通信（“HTTPS”）に対応している場合には、警告画面の表示が極めて困難であるという点が挙げられる。

以上のとおり、アクセス警告方式には、技術面でもコスト面でも、現状では、

[27] その他、CDN(コンテンツデリバリーネットワーク)サービスで使われる仕組みやリダイレクトの仕組み等を利用して、暗号化通信の場合であっても警告画面を表示させることは技術上可能だが、これらの場合、本来の通信の宛先であるサイトの管理者と契約関係にある者が正当なサーバの電子証明書を入手することが前提となっており、海賊版サイトの管理者から ISP が電子証明書を入手することは考えづらいことから、やはり現実的な対応策ではないと考えられる。

[28] 意見募集に対する意見:「コスト負担の議論を深めることが必要」同旨8件、「コストは受益者負担とすべき」同旨6件。

様々な課題がある。しかしながら、例えば、既に関連機器やシステムを保有しているISPなどもあることから、個別同意を前提としたアクセス警告方式の試行的実施などの技術検証を進めていくほか、インターネットを取り巻く技術の進展は目まぐるしく、また、それに伴って、関連機器・システムのコストも将来的に低下していくことも考えられることから、引き続き技術動向・コスト動向などアクセス警告方式をめぐる状況把握に努めていくことが適当である。

６．アクセス警告方式に関するその他の課題や留意点

（１）実施・運営に当たっての留意点

ISPがアクセス警告方式を実施・運営する場合には、対象となるサイトがむやみに広がればユーザの表現活動に対する萎縮効果を与えることとなり、また、ユーザの知る権利に対する大きな制約にもなり得ることから、対象となるサイトが合理的であり、かつ、必要最小限度の範囲となるよう、対象となるサイトの範囲の選定に当たって留意することが必要であるとともに、海賊版サイトによる著作権者の被害拡大を速やかに防ぐ観点からは、対象となるサイトが迅速にリスト化され、反映されることが重要である。

（２）アクセス警告方式に係る個人情報等の取扱いに係る留意点

ISPがアクセス警告方式を実施する場合には、個々のユーザがオプトアウトをしているか否かに関する情報を取得する必要がある。個々のユーザがオプトアウトをしているか否かに関する情報自体は通信の秘密とはいえないものの、当該ユーザ個人を識別可能とする情報であるため、少なくとも個人情報に該当すると考えられること、また、ユーザの内心に関わる機微な情報ともいえることから、ISPは当該情報について慎重に取り扱うことが必要である。

一方、海賊版サイトにアクセスしようとしたユーザに対して警告画面を表示した際の当該ユーザによるアクセスに係る履歴（ログ）、さらに、当該警告画面の表示にもかかわらず当該ユーザが海賊版サイトにアクセスした際の当該アクセスに係る履歴（ログ）は、ISPにとって通信の秘密に属する情報であることから、ISPはこれらの情報については厳格な取扱いが求められる。

７．アクセス警告方式に係る今後の検討課題

以上の検討を踏まえると、アクセス警告方式は、警告画面を表示させることで、多くのユーザが海賊版サイトにアクセスすることを思いとどまるものと見込まれることから、海賊版対策として一定の効果があると考えられるものの、アクセス警告方式の実施に係る法的整理に関しては、現時点でのユーザの意識や意向を前提とすると、ユーザから個別具体的かつ明確な同意を取得すればアクセス警告方式を実施することは可能である。しかし、現状では、契約約款等による包括同意によってユーザの有効な同意があるとの法的整理を行うことは困難である。また、ダウンロード行為が違法とされたと想定した場合についても、ユーザの意識や意向に大きな違いは見られないことから、同様の整理になるものと考えられる。

また、アクセス警告方式を実現するための技術的な仕組みや関連機器・システムのコストの面でも、現状では、様々な課題があることが示された。しかしながら、例えば、既に関連機器やシステムを保有している ISP などもあることから、個別同意を前提としたアクセス警告方式の試行的実施などの技術検証を進めていくほか、インターネットを取り巻く技術の進展は目まぐるしく、また、それに伴って、関連機器・システムのコストも将来的に低下していくことも考えられることから、今後とも海賊版の被害状況や総合的対策メニュー（案）に示された各施策の取組状況も踏まえつつ、引き続きユーザの意識や意向、技術動向・コスト動向などアクセス警告方式をめぐる状況把握に努めていくことが適当である。

なお、前述のとおり、アクセス警告方式には海賊版対策として一定の効果が見込まれると考えられるところ、カジュアル・ユーザによる海賊版サイトへのアクセスを防ぐことによって著作権者の被害拡大を防止する仕組みは、ネットワーク側におけるアクセス抑止方策であるアクセス警告方式に限られず、端末側においてアクセス警告方式類似の対策の実装を図ることも可能である。したがって、アクセス警告方式に関する課題については、上記のとおり、引き続き技術検証や状況把握等に努めていく一方で、現状では、後述のとおり端末側でアクセス警告方式類似の方策をすでに実施しており、ネットワーク側ではなく、端末側においてアクセス警告方式類似の対策の実装を図ることがより即時性が高い方策であると考えられることから、上記ネットワーク側におけるアクセス抑止方策への対応と併せて、端末側におけるアクセス抑止方策を着実に促進していくことが適当である。

意見募集においても、ネットワーク側よりも、端末側において実装を図る方が効

率的又は本来のネットワークのあるべき姿に相応しい等の意見も多く寄せられた[29]ところであり、こうした声も踏まえて、次章では、端末側におけるアクセス抑止方策について検討を行う。

[29] 意見募集に対する意見:「インターネットのエンドツーエンド原則に着目して議論すべき」同旨7件。

第３章　端末側におけるアクセス抑止方策

１．端末側におけるアクセス抑止方策に関する効果・メリット、具体的な対応策

端末側におけるアクセス抑止方策には、インターネットの「End to End の原則」に則した対応策の実施が可能であること、通信の秘密に関する法的問題を生じさせることなく実施可能であること、青少年向けフィルタリングサービスやセキュリティ対策ソフトなど端末で利用可能な手段が既に存在しており、迅速に対応が可能であること、多くのフィルタリングソフトやセキュリティ対策ソフトにおいて、既に一定数の海賊版サイトへのアクセス制限が実現済みであること、ネットワーク側での対応と比較してコストも低廉であること等のメリットがあると考えられる[30]。

ただし、端末側におけるアクセス抑止方策にはこうしたメリットはあるものの、青少年が安全に安心してインターネットを利用できる環境の整備等に関する法律（平成 20 年法律第 79 号）（以下「青少年インターネット利用環境整備法」という。）に基づく青少年を対象とするフィルタリングサービスは保護者が不要の申出をした場合には利用しなくてよいことや、同法に基づくフィルタリングサービス以外の端末側におけるアクセス抑止方策全般の場合には利用に際してユーザが自ら申し出る必要があること等のため、主として普及率の観点から、海賊版対策としての効果は限定的との意見もある[31]。したがって、端末側におけるアクセス抑止方策に関しては、その普及方法についても検討が求められる。

２．具体的な対応策

端末側での具体的な対応策としては、既存の青少年向けのフィルタリングサービス、セキュリティ対策ソフトへのフィルタリング機能の組込み、ブラウザソフトにおける拡張機能での警告表示又は閲覧防止機能の追加などが考えられる。その中でも、有力な手段として、以下、青少年向けフィルタリングサービス及びセキュリティ対策ソフトへのフィルタリング機能の組込みについて述べる。

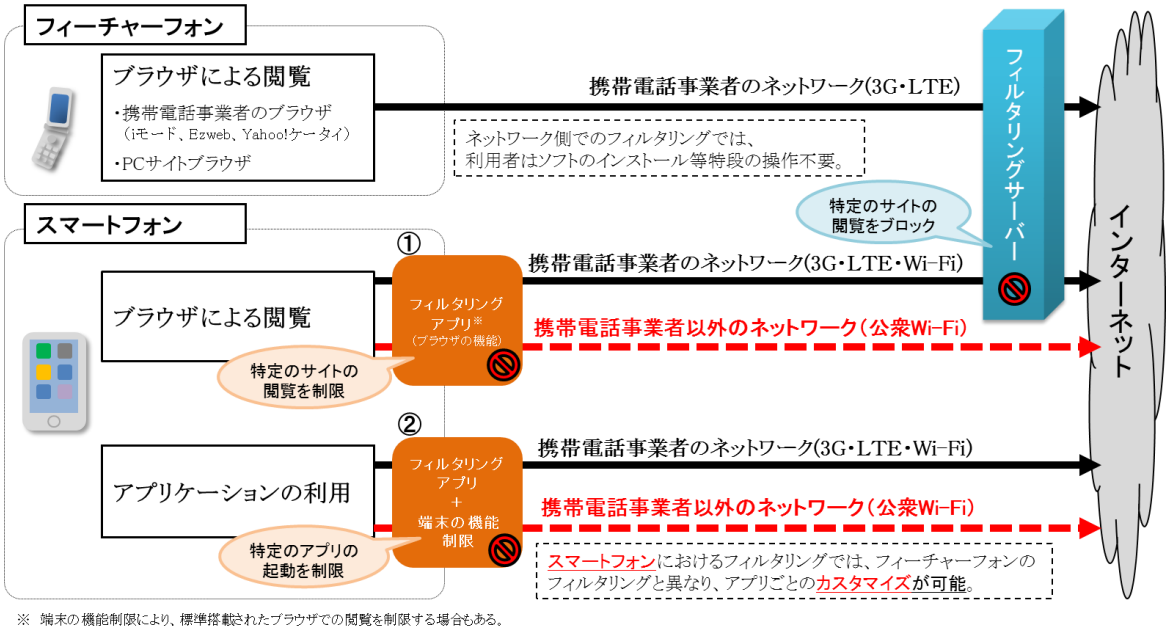
（１）青少年向けフィルタリングサービス

一つ目の対応策として、青少年向けフィルタリングサービスが考えられる。青少年向けフィルタリングサービスとは、青少年にとって有害な情報を閲覧するこ

[30] 意見募集に対する意見：「端末側での対応策には一定のメリットがある」同旨 10 件。

[31] 意見募集に対する意見：「端末側での対応策にはメリットがあるが効果は限定的」同旨4件。

とを防ぐ目的で青少年がアクセスできるサイトやアプリを閲覧制限するサービスをいう。青少年インターネット利用環境整備法により、原則として、18 歳未満の青少年が使用する目的でスマートフォンや携帯電話を契約する際には、フィルタリングサービスの提供が義務付けられている（保護者が利用しない旨を申し出た場合を除く。）。青少年向けフィルタリングサービスには様々な方式があるが、近年では、携帯電話事業者が提供するフィルタリングアプリをスマートフォンにインストールして使用する方式が多く見受けられる。当該アプリはブラウザアプリとして機能し、特定サイトの閲覧防止機能や特定アプリの起動制限処理機能が付加されている[32]。



【図4　スマートフォンにおけるフィルタリング】[33]

現在、青少年向けフィルタリングサービスにおいては、基本的に海賊版サイトは閲覧制限サイトの対象として含まれており、権利者側からフィルタリング事業者に対する海賊版サイトのリストの提供も行われていることから、青少年向けフィルタリングサービスを引き続き普及させることで、海賊版サイトへのアクセス抑止につながるものと考えられる。

---

[32] iOS の場合は、アプリによる対策はできないが、端末の機能により、サイトの閲覧防止やアプリの起動制限を行う場合もある。

[33] 本検討会資料1－2「検討の背景」（事務局）9頁。

また、アンケート調査結果[34]によると、若年層の海賊版サイトへのアクセス経験が多いことから、青少年向けフィルタリングサービスの普及を推進することで、効率的に海賊版サイトへのアクセスを抑止することが可能になると考えられる。さらに、若年層ほど海賊版サイトへ意図せずアクセスすることを防ぐ目的でのフィルタリングサービスの受容度が高い[35]ことから、青少年向けフィルタリングサービスの普及促進により、対象となる青少年が大人になってからも自らの意思により海賊版サイトを含む有害サイトについてアクセスをしないための自衛意識を高めるような啓発を行うことが可能と考えられる。

一方で、このような方法においては、フィルタリングソフトの利用に当たってのユーザ利便の向上[36]や、海賊版サイトリストのフィルタリングソフト事業者への迅速な提供等を促進することが課題となると考えられる。

（２）セキュリティ対策ソフトへのフィルタリング機能の組込み

二つ目の対応策として、セキュリティ対策ソフトへのフィルタリング機能の組込みによる対応策が考えられる。

ア　セキュリティ対策ソフトの現状

セキュリティ対策ソフトの中には、端末にインストールしたセキュリティ対策ソフトの機能として、セキュリティ上危険と判断されるサイトへのアクセスを検知した場合に、警告表示又は閲覧防止措置を行う機能を持つものがある。本検討会においてヒアリングを実施したセキュリティ対策ソフト事業者によると、同社が提供するセキュリティ対策ソフトでは、不正プログラムが隠されている web ページや、正規の web サイトを偽造して情報を盗み取るフィッシン

---

[34] アンケート調査結果:「(正規版・海賊版を問わず)電子コミックを閲覧もしくはダウンロードしたことがある」と答えた人の割合は、全体:41.9%の一方、15-19 歳:66.7%。これらの電子コミック閲覧・DL経験者のうち、「海賊版サイトにアクセスしたことがある / もしかしたらアクセスしたことがあるかもしれない」と答えた人の割合は、全体:47.5%の一方、15-19 歳:57.5%。

[35] アンケート調査結果:海賊版サイトへ意図せずアクセスしてしまうことを防ぐために、フィルタリングソフト(大人向けのサービスも含む)をインストールすることについて、「インストールしたい / してもよい」と答えた人の割合は、全体:59.2% 15-19 歳:71.7% 20 代:69.1% 30 代:63.6% 40 代:57.8% 50 代:53.4% 60 代:44.5%。

[36] アンケート調査結果:フィルタリングソフトを「一定の場合にはインストールしてもよい」と答えた人のうち、インストールするための条件として求める要素の上位2つは「使いやすいソフト」であること 47.4%、「手続きが簡単」であること 46.0%。

グ詐欺の兆候を示すwebページへのアクセスを防止するセキュリティ目的での閲覧防止機能を備えており、同機能はデフォルトオンで提供されている。

上記の機能に加え、同社の製品では、ペアレンタルコントロール機能として、管理者（親）が利用者（子供）に閲覧させたくないwebページの閲覧を防止するフィルタリング機能が備えられている。同機能はPC向け製品及びモバイル向け製品の両方で提供されているが、同機能はデフォルトオフで提供されているため、設定のために別途操作が必要となる。PC向け製品とモバイル向け製品で閲覧防止機能作動時の挙動は若干異なる[37]ものの、いずれも暗号化通信（“HTTPS”）の場合であっても閲覧防止機能は作動する。同フィルタリング機能の対象には海賊版サイトも含まれており[38]、知的財産を保護する団体（権利者団体）等からのリスト提供を受けることにより、フィルタリングの対象となる海賊版サイトが選定されている。

このとおり、現状では、同社の製品では、海賊版サイトへの対策はデフォルトオフのため別途設定が必要なフィルタリング機能によって実施されているものの、海賊版サイトがセキュリティ対策上危険と判断される場合には、デフォルトオンで提供されているセキュリティ目的での閲覧防止機能において別途設定を必要とせずブロックされる可能性がある[39]。

また、アンケート調査結果によると、セキュリティ対策ソフトへのフィルタリング機能の組込みについては需要が高く、通常のフィルタリングサービスへの受容度と比較しても高い数値となっている[40]。このことから、セキュリティ

---

37 本検討会においてヒアリングを実施したセキュリティ対策ソフト事業者からのヒアリングによると、PC向け製品の場合、フィルタリング機能が作動した場合、「いまだけみられるようにする」「これからみられるようにする」といった、保護者がパスワードを入力すると、当該サイトにアクセス可能となるボタンが表示される。他方、モバイル向け製品の場合、スマートフォンの性質に鑑みて、保護者にアクセス解除を求めるようなボタンは表示されず、単なる遮断となる。

38 本検討会においてヒアリングを実施したセキュリティ対策ソフト事業者からのヒアリングによると、フィルタリングのレベルは「高」・「中」・「低」の3段階から選択可能であるところ、最もレベルが低い（フィルタリングの対象が最も少ない）「低」を選んでも海賊版サイトはフィルタリングの対象となるカテゴリに分類されているとのことであった。

39 出版広報センターによると、海賊版サイトの中には、無料でコンテンツをダウンロードできるとうたいつつ会員登録やクレジットカード番号の登録を求め、登録された情報を基に不正請求を行うサイトや、不正な広告を表示させるアドウェアが仕込まれているサイトがあるとのことである。なお、本検討会においてヒアリングを実施したセキュリティ対策ソフト事業者によると、これらのような海賊版サイトがセキュリティ目的での閲覧防止機能やその他の機能においてブロックされるかどうかは個別の事案によって異なるとのことである。

40 アンケート調査結果:フィルタリングソフトを「インストールしたい / してもよい」と答えた人の割合は、全体:59.2% 15-19歳:71.7% 20代:69.1% 30代:63.6% 40代:57.8% 50代:53.4% 60代:44.5%。（再掲）。

対策ソフト自体の導入に関して普及を促進するとともに、同ソフト等で提供されるフィルタリング機能の導入に関しても同様に普及を促進することで、海賊版サイトへのアクセスの抑止に一定の効果があるものと考えられる。

イ　セキュリティ対策ソフトにおける海賊版サイト対策の課題

セキュリティ対策ソフトにおける海賊版サイト対策の課題として、第一に、セキュリティ対策ソフトにおけるフィルタリング機能の利用率向上が挙げられる。まず、フィルタリング機能の利用率向上のための前提となるセキュリティ対策ソフト自体の普及率に関して、PC 向けセキュリティ対策ソフトは業界全体で高い普及率を誇るものの、他方で、モバイル向けセキュリティ対策ソフトの普及率は、PC 向け製品と比較するとそれほど高くはない[41]。さらに、セキュリティ対策ソフトを導入しているユーザのうちフィルタリング機能を設定しているユーザの割合は、同社の PC 向け製品においても少ないとのことである。

第二の課題として、フィルタリング機能の対象となる海賊版サイトリストの強化が挙げられる。本検討会においてヒアリングを実施したセキュリティ対策ソフト事業者によると、同社におけるセキュリティ対策ソフトのフィルタリング機能において、権利者団体等からの海賊版サイトのリスト提供頻度はそれほど高くないとのことであった[42]。

したがって、セキュリティ対策ソフトにおける海賊版サイト対策に関しては、海賊版サイトリストのセキュリティ対策ソフト事業者への迅速な提供に加え、セキュリティ対策ソフト自体の導入の促進や、セキュリティ対策ソフトにおけるフィルタリング機能の導入及び利用者による設定を促進することが課題となると考えられる。

なお、これらの課題に関して、同社の製品等においてペアレンタルコントロールの観点から主に青少年向けに提供されているフィルタリング機能を大人向けにも活用していくことを促進していくことや、セキュリティ目的での閲覧

一方、セキュリティ対策ソフト等に海賊版サイトへのアクセスに対しても警告表示や遮断を行う機能を「機能を追加してほしい / どちらかといえば機能を追加してほしい」と答えた人の割合は 78.4%。

41 本検討会においてヒアリングを実施したセキュリティ対策ソフト事業者の独自試算。数値は非公開。

42 2019 年6月時点では、権利者団体等から海賊版サイトのリスト提供は、直近では同年3月に実施されたとのことであった。

防止機能と同様にデフォルトオンでの提供を推奨していくという方向性[43]も選択肢の一つとして考えられる。

３．端末側におけるアクセス抑止方策に関するその他の課題や留意点

（１）セキュリティ対策ソフト事業者やブラウザ提供事業者や OS ベンダ等との連携

端末側での対応は、PC 及びスマートフォンのブラウザソフトやスマートフォンの OS などの端末側ソフトウェアにフィルタリングやウイルス対策等の機能を追加すること等により対策を講じる必要があることから、こうした対応策を効率的に実施するには、セキュリティ対策ソフト事業者やブラウザ提供事業者や OS ベンダ等との連携・協力が課題である[44]。

（２）コスト負担の在り方

端末側におけるアクセス抑止方策に要するコストは、ネットワーク側でアクセス警告方式を実装しようとする場合に比べると低廉であるとはいえ、ソフト開発・実施運営等で発生するコスト負担の在り方については、慎重かつ丁寧な協議・検討が必要である[45]。

---

[43] この点について、同社へのヒアリングにおいては、現在同社が提供している製品はあくまでセキュリティ対策用ソフトであり、マルウェアに感染したり、フィッシング詐欺のサイトにアクセスして被害を受けたりすることを防止するという位置付けの製品であることから、海賊版サイトのような違法なコンテンツを標準でブロックするような機能がセキュリティ対策ソフトという位置付けの中で真に求められるものなのかどうかという点については議論が必要との見解が述べられた。

[44] この点について、意見募集に対する意見として、「端末フィルタリングによるアクセス抑止方策の検討にあたっては、むしろ各端末の OS ベンダからの協力を得ることを検討すべき」「既存のフィルタリングをベースにして実装する場合、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」「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るし、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」等の意見が寄せられた。

また、青少年向けフィルタリングに関しても、iOS の機能制限を利用することでフィルタリングを実施する場合、年齢制限等のレーティングについては Apple が独自に判断していることから、迅速な海賊版サイトのリスト反映に関しては OS ベンダの協力が必要と考えられる。

[45] 意見募集に対する意見：「コストは受益者負担とすべき」同旨3件。また、この点について、「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る。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。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るが、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る。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

（３）実施・運営に当たっての留意点

フィルタリング等の対象となるサイトが合理的となるよう、対象サイトの範囲の選定に当たって留意することが必要であるとともに、アクセス警告方式の課題と同様に、対象サイトが迅速にリスト化され、反映されることが重要である。

４．端末側におけるアクセス抑止方策に係る今後の検討課題

端末側の対応策は、前述のとおり、通信の秘密に関する法的問題を生じさせることなく実施可能であること、青少年向けフィルタリングサービスやセキュリティ対策ソフトなどが既に存在しており、迅速に対応が可能であること等のメリットがあると考えられることから、その利便性を向上させ、普及を図っていくことが適当である。

具体的には、青少年向けフィルタリングサービスにおける対策については、電気通信事業者や OS 事業者によるフィルタリングソフトの利用に当たってのユーザ利便の向上や、フィルタリングサービスに関する周知の強化等[46]を推進することにより、その普及を図っていくとともに、OS 事業者との連携も考慮しつつ、海賊版サイトリストのフィルタリングソフト事業者への迅速な提供等を促進することが望ましい。なお、これらの青少年向けフィルタリングサービスに対する今後の対応については、総務省「ICT サービス安心・安全研究会 青少年の安心・安全なインターネット利用環境整備に関するタスクフォース」においてこれまで検討していることから、同タスクフォースにおいて一定の結論を得ることが望ましい。

セキュリティ対策ソフトにおける対策については、権利者側とセキュリティ対策ソフト事業者側の協力体制の構築を支援することにより、海賊版サイトリストをセキュリティ対策ソフト事業者へ迅速かつ定期的に提供する枠組みを整備することに加え、セキュリティ対策ソフト自体の導入の促進や、セキュリティ対策ソフトにおけるフィルタリング機能の導入及び利用者による設定を促進することが望ましい。また、ペアレンタルコントロールの観点から主に青少年向けに提供されているフィルタリング機能を大人向けにも活用していくことを促進していくことや、フィルタリング機能をデフォルトオンで提供することを推奨していくという方向性も

担すべきかは議論のテーマである。」といった意見が寄せられた。

46 検討会における議論では、構成員から「フィルタリング促進のための動機付けについて、例えば正規版のサイトが何時間か見られる等のユーザインセンティブを与えることも考えられる」という意見も述べられた。

選択肢の一つとして考えられるが、この点については、セキュリティ対策ソフトに求められる役割等について、セキュリティ対策ソフト事業者やユーザ等の幅広い関係者の意見を踏まえつつ、さらなる議論が求められる。

上記のとおり、端末側での具体的な対応策としては、既存の青少年向けのフィルタリングサービス、セキュリティ対策ソフトへのフィルタリング機能の組込みのほか、ブラウザソフトにおける拡張機能での警告表示又は閲覧防止機能の追加など、様々な手段が考えられるが、端末側におけるアクセス抑止方策に関して共通することとして、ユーザの意思で自らのアクセス先をコントロールできる仕組みの有用性をユーザに周知啓発していくことにより実効性を高めていくことが非常に重要である。自らのアクセス先をコントロールできることは、青少年向けフィルタリングサービスを中心としたこれまでの取組に加えて、現在のシニア世代を中心とした自らが望まないサイトへアクセスしてしまうことによるフィッシング詐欺等の消費者被害に対しても有効であり、これらを踏まえ、海賊版サイトの性質や問題も含めたインターネットアクセス全般に関する情報リテラシーの普及啓発を幅広い世代に向けて進めていくことが適当である。また、こうした情報リテラシーの普及啓発を進めると同時に、自らのアクセス先をコントロールできる仕組みとして、青少年に限らず幅広い年代のユーザが自らの意思でフィルタリングサービスを活用[47]することの促進や、上述のセキュリティ対策ソフトにおけるフィルタリング機能の組込みを始めとする取組も併せて進めることで高い効果につながっていくものと考えられる。

[47] 青少年に限らず、大人向けのフィルター設定を行うことができるフィルタリングソフトが存在する。

第４章　最後に

１．アクセス抑止方策に関する検討の方向性

本検討会においては、総合的対策メニュー（案）において対策の１つとして挙げられているアクセス警告方式を中心に、アクセス抑止方策に関する検討を行った。アクセス警告方式は、ISP がユーザのアクセス先を検知することが実施に当たって必要不可欠であることから、通信の秘密の規定との関係を始めとする法的整理を中心に検討・議論を行うとともに、導入・実施に当たっての技術的可能性等について、ユーザの通信の秘密の保護やインターネットの自由な利用の確保等にも配慮しつつ検討を行ったほか、併せて、フィルタリングなどの手法を含めた効果的な方策の在り方について検討を行った。

検討・議論を行うに当たっては、関係者の共通認識の下で検討を行うこと、あるべきネットワークの姿を踏まえた検討を行うこと、ユーザの意識や意向を踏まえた検討を行うことを基本的な考え方として進め、その一環として、海賊版による被害状況や海賊版サイトに対処するための取組の現状、アクセス警告方式の実現に係る技術的な課題とコスト試算についてヒアリングを実施したほか、意見募集やアンケート調査を実施し、ユーザの意識や意向をできるだけ正確に把握し、それを尊重して結論を得ることに努めた。検討の結果、各論点について、以下の方向性を示した。

○　アクセス警告方式は、警告画面を表示させることで、多くのユーザが海賊版サイトにアクセスすることを思いとどまるものと見込まれることから、海賊版対策として一定の効果があると考えられるものの、アクセス警告方式の実施に係る法的整理に関しては、現時点でのユーザの意識や意向を前提とすると、ユーザから個別具体的かつ明確な同意を取得してアクセス警告方式を実施することは可能であるが、現状では、契約約款等による包括同意によってユーザの有効な同意があると考えることは困難である。

○　ダウンロード行為が違法とされたと想定した場合においても、ユーザの意識や意向に大きな違いは見られないことから、同様の整理になると考えられる。

○　アクセス警告方式の実施に係る技術的課題について、同方式を実現するための技術的な仕組みや関連機器・システムのコストの面でも、現状では様々な課題がある。

○　しかしながら、例えば、既に関連機器やシステムを保有している ISP などもあ

ることから、個別同意の取得を前提としたアクセス警告方式の試行的実施などの技術検証を進めていくほか、インターネットを取り巻く技術の進展は目まぐるしく、それに伴って、関連機器・システムのコストも将来的に低下していくことも考えられることから、総務省において、今後とも海賊版の被害状況や総合的対策メニュー（案）に示された各施策の取組状況も踏まえつつ、引き続きユーザの意識や意向、技術動向・コスト動向などアクセス警告方式をめぐる状況把握に努めていくことが適当である。

○　その上で、現状では、ネットワーク側ではなく、端末側においてアクセス警告方式類似の対策の実装を図ることがより即時性が高い方策であると考えられることから、上記ネットワーク側におけるアクセス抑止方策への対応と併せて、端末側における対応策を着実に促進していくことが適当である。

○　端末側の対応策については、通信の秘密に関する法的問題を生じさせることなく実施可能であること、青少年向けフィルタリングサービスやセキュリティ対策ソフトなどが既に存在しており、迅速な対応が可能であること等のメリットがあると考えられることから、その利便性を向上させ、普及を図っていくことが適当である。

○　端末側における具体的な対応策としては、第一に、青少年向けフィルタリングサービスがあり、総務省において、電気通信事業者や OS 事業者によるフィルタリングソフトの利用に当たってのユーザ利便の向上や、フィルタリングサービスに関する周知の強化等により、その普及を図っていくとともに、OS 事業者との連携も考慮しつつ、海賊版サイトリストのフィルタリングソフト事業者への迅速な提供等を促進することが望ましい。

○　第二に、セキュリティ対策ソフト等における対策があり、総務省において、権利者側とセキュリティ対策ソフト事業者側の協力体制の構築を支援することにより、海賊版サイトリストをセキュリティ対策ソフト事業者へ迅速かつ定期的に提供する枠組みを整備することとし、その具体的な枠組みの在り方については、現在進みつつある通信業界・出版業界の民間協力の状況も踏まえつつ、本年秋頃を目途に結論を得ることが望ましい。このほか、総務省において、セキュリティ対策ソフト自体の導入の促進や、セキュリティ対策ソフトにおけるフィルタリング機能の導入及び利用者による設定を促進することによりセキュリティ対策ソフトへの当該機能の組込みを推進するとともに、その普及を図っていくことが望

ましい。

○　端末側におけるアクセス抑止方策に関して共通することとして、ユーザの意思で自らのアクセス先をコントロールできる仕組みの有用性をユーザに周知啓発していくことにより実効性を高めていくことが非常に重要である。したがって、総務省において、海賊版サイトの性質や問題も含めたインターネットアクセス全般に関する情報リテラシーの普及啓発を幅広い世代に向けて進めていくと同時に、自らのアクセス先をコントロールできる仕組みとして、青少年に限らず幅広い年代のユーザが自らの意思でフィルタリングサービスを活用することの促進や、上述のセキュリティ対策ソフトにおけるフィルタリング機能の組込みを始めとする取組も併せて進めることが望ましい。

２．今後の取組に当たっての留意点

今後、アクセス抑止方策に係る取組を進めるに当たっては、まず、本検討会における検討を行うに当たっての基本的な考え方を踏襲すること、すなわち、関係者の共通認識の下での取組を進めること、あるべきネットワークの姿を踏まえて取組を進めること、ユーザの意識や意向を踏まえ、ユーザの理解を得て取組を進めることが重要である。

このうち、関係者の共通認識の下での取組が重要であるとの観点から、現在、出版業界と通信業界の間で海賊版対策のための協力の在り方について検討・意見交換を行う場が既に民間主導で進められつつある[48]。今後アクセス抑止方策に係る取組を行っていく際には、総務省においても、これらの民間主導の枠組みを尊重しつつ、国として必要な支援を行っていくことが適当である。

また、ユーザの意識や意向を踏まえ、ユーザの理解を得て取組を進めることが重要であるとの観点から、これらの取組を進めるに当たっては、ユーザの意識動向調査を定期的に実施するなど、各種施策の効果検証を継続的に実施していくことが適当である。

次に、インターネット上の海賊版サイトへのアクセス抑止方策は、総合的対策メニュー（案）に示された様々な海賊版対策のうちの一部の施策であり、海賊版サイ

[48]「総務省さんがおっしゃった信頼醸成の一環ということなのかもしれませんけれども、昨年の様々な経験を踏まえて、通信業界、出版社などの実務有志で声を掛け合って、定期的に現行法のもとで可能な海賊版対策を協議する連絡会議というものを立ち上げております。（中略）特に、両業界のトップレベルが集まった APL の村井純代表とも密に連絡は取り合っております。」（知財本部検証・評価・企画委員会（平成31年3月29日）議事録より、福井構成員発言（抜粋））

トを撲滅するためには、同メニュー（案）において示された他の施策、例えば、著作権教育・意識啓発、正規版の流通促進、国際連携・国際執行の強化、海賊版サイトへの広告出稿の抑制といった施策とも組み合わせつつ、同メニュー（案）を総合的に推進していくことが重要である。

なお、本検討会は、インターネット上の海賊版対策のうち、アクセス抑止方策に関して検討を行うために設置されたものであるが、会合における意見交換においては、また、意見募集において提出されたユーザの意見においても、アクセス抑止方策に限らず、その他の施策に関して多様な意見やコメントが示された。このこと自体が、インターネット上の海賊版対策において、総合的に施策を講じていくことの必要性を示唆するものであるが、これら他の施策に関しても留意すべき意見・コメントがあったことから、参考として以下において記述する。

３．その他の施策についての意見・コメント（参考）

（１）他の海賊版対策に係る施策への全般的意見

本検討会において実施したアクセス抑止方策に係る検討の論点に関する意見募集においては、他の海賊版対策についても多くの意見が寄せられた。具体的には、「海賊版サイト運営者の取締・執行強化が必要」同旨 39 件、「民事上の法的訴求に資する取組や制度改正が必要」同旨 12 件、「広告対策が必要」同旨 14 件、「正規版流通強化が必要」同旨９件、「著作権教育・啓発が必要」同旨５件、「ブロッキングが必要」同旨４件、「ブロッキングに反対」同 13 件という結果となっている。

（２）他の施策に関する主な意見・コメント

上記意見募集のほか、会合における意見交換においても、構成員から、他の施策に関する多様な意見・コメントがあった。これら他の施策に関して、会合における構成員等からの主な意見・コメントは以下のとおり。

① 情報リテラシー（著作権教育・啓発）

本検討会の会合における議論の中で、構成員等から「ユーザの意思で自らのアクセス先をコントロールできるようになるようにするための情報リテラシーの向上について、そのようなコントロールの仕組みと併せて進めていくことが大事」といった意見が述べられた。

②ネットワークの両端（特に発信者側）での取組

第３章においては、インターネットの「End to End の原則」に則した対応策の実施が可能であること等の理由から、端末側における対応策について検討を行ったが、意見募集においても、海賊版コンテンツをアップロードした者に対する取締りの強化など、発信者側（海賊版サイト側）のエンドでの取組の重要性について多数の意見が寄せられた[49]ほか、本検討会の会合における議論でも構成員等から「海賊版サイト対策としては、犯人の検挙やフィルタリングといったエンド側での対応が強調されるべきだということがこの検討会の一つの成果ではないか」といった意見が述べられた。

③ CDN 事業者への対応

発信者側のエンドでの取組に関連して、特に CDN 事業者への対応に関して、本検討会の会合における構成員等からの意見として、例えば、「CDN 事業者に関する取組については、通信関係者側から協力できる、海賊版サイトに対する有効な対策ではないか」といったコメントがあった。

④ 国際連携・国際協調

上記②で述べたネットワークの両端（特に発信者側）での取組に関連して、意見募集において、国境を越えた取締り等を適切に行うための国際連携強化の必要性に関する意見が寄せられたほか、インターネット上のデータ流通に係るルール作りに向けた国際連携・国際協調の観点から、本検討会の会合における構成員等からの意見として、「日本として Data Free Flow with Trust という戦略を打ち出しており、これをグローバルなデータ流通に係るルール作りの基本的なコンセプトとしてコンセンサスを得て進めていこうとしていること、また、GDPR の十分性認定の場面においても、我が国の法制度における特徴として通信の秘密の規定が高く評価されていること、さらに、意見募集の結果からも、通信の秘匿性は我が国の国家戦略として今後さらに重要になっていく」といったコメントがあった。

⑤ サイトブロッキング

サイトブロッキングに関しては、本検討会会合における構成員等からの意見

[49] 意見募集に対する意見:「海賊版サイト運営者の取締・執行強化が必要」同旨39件、「民事上の法的訴求に資する取組や制度改正が必要」同旨 12 件(再掲)。

として、例えば、「提案募集の結果を見ると、通信の秘密の侵害に対して強い懸念が持たれているということを非常に強く感じる。ブロッキングを可能にする法律を作るにせよ、アクセス警告方式を可能にする包括同意の整理をするにせよ、いずれにしても、簡単にできることではないという指摘が多かったので、これらの点を今後の海賊版サイト対策全体を考える上でも心掛けるべき」、「意見募集において、海賊版対策パッケージ全体として、通信の秘密を侵害する形で進めるべきではないという意見がはっきりと出てきており、アクセス警告方式のみならず、ブロッキングについても反対の意見が多いことに留意すべき」といったコメントがあった。