資料３－２

論点の整理（案）

２０１９年６月２０日
事　　務　　局

１．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

１．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

（１）関係者の共通認識の下での検討

- 本検討に当たって、まずはインターネット上の海賊版による被害状況、海賊版に対処するための出版業界等における取組状況、アクセス抑止方策の実現に向けたユーザの意識や意向、技術的な課題・動向などの現状について、検証可能なデータ・証拠に基づいた関係者の共通の認識の基盤の上で議論を進めることが、アクセス抑止方策を含むインターネット上の海賊版対策についての適切な結論を得るために重要。
  →海賊版サイトによる被害状況や海賊版サイトに対する取組・対策等についての出版業界からのヒアリング、検討の論点に関する意見募集やアクセス抑止方策に関する一般ネットユーザの意識・意向調査、アクセス警告方式の実現に関する技術的な課題とコスト試算について通信事業者団体からのヒアリング等を実施。

（２）あるべきネットワークの姿を踏まえた検討

- インターネットには自律・分散・協調という特徴があること、また、インターネットが新たなサービスやビジネスを創出する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自由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は何かを十分考慮した上で、結論を得ることが重要。

（３）ユーザの意識や意向を踏まえた検討

- 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から、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。
  →検討の論点に関する意見募集やアクセス抑止方策に関する一般ネットユーザの意識・意向調査を実施し、これらを踏まえて議論を実施。

2．アクセス警告方式について

2．アクセス警告方式について

（1）アクセス警告方式の狙いや意義、プロバイダの役割など、実施の前提

- アクセス警告方式は、警告画面を表示することで、ユーザに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）がアクセスすることを自ら思いとどまることを促そうとするもの。

- ユーザの同意を得て実施する点、警告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者はオプトアウトすることにより実施対象としない点等において、いわゆるサイトブロッキングとの違いがある。

- ユーザによる海賊版サイトへのアクセスを減らすことによって、インターネット上のマンガ・アニメなどに対する著作権侵害の被害を防止することが目的。

- このほか、ダウンロード行為が違法となる場合には、警告画面を表示させることはユーザに対して「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、ダウンロード行為が違法でない場合に比べると、ユーザの理解が得られやすい面があるとも考えられる。
  →事業者団体からは、通信事業者がアクセス警告表示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あり。

- ただし、ダウンロード行為の違法性の有無によって、カジュアル・ユーザが必ずしも大きく対応を変化させるとは限らないことから、アクセス警告方式の意義や役割は、ダウンロード行為が違法か違法でないかで大きな違いはないとも考えられる。
  →ユーザアンケート結果：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93.3%、静止画ダウンロード違法化想定の場合95.9%

2．アクセス警告方式について

2．アクセス警告方式について（つづき）

（2）アクセス警告方式の効果・メリット

- 海賊版サイトにアクセスしようとする際に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一定の効果が見込まれる。なお、ダウンロード行為が違法か違法でないかで効果に大きな違いは見られないものと考えられる。
  →ユーザアンケート結果：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93.3%、静止画ダウンロード違法化想定の場合95.9%

- 一方で、ユーザがオプトアウトすれば警告画面が表示されない、ブラウザとウェブサイトの間の通信にSSL（TLS）による暗号化通信（いわゆる"HTTPS"）が用いられる場合には警告画面を表示させることが困難である、警告画面が表示されても「はい」をクリックしてアクセスするユーザは一定程度いると想定される等、海賊版サイト対策としての効果は限定的であるとも考えられる。
  →日本のユーザのHTTPSアクセス割合：73%（2019年4月）

2．アクセス警告方式について

2．アクセス警告方式について（つづき）

（3）アクセス警告方式の実施の前提となる法的整理

- アクセス警告方式を実施するためには、通信事業者がユーザのアクセス先を検知する必要があり、通信の秘密に関してユーザの有効な同意が得られることが不可欠の前提条件。ただし、通信の秘密は、日本国憲法において基本的人権として保障されているものであることから、ユーザによる同意の成否は慎重に判断されるべき。また、通信の秘密の侵害に関して有効な同意といえるのは、個別具体的かつ明確な同意が原則。

- アクセス警告方式の実効性・普及率を高めるためには、通信の秘密に関する同意について、通信事業者が提供する通信サービスの約款に記載することにより同意を取得する方法が考えられる。約款による包括同意が有効な同意とみなされるかどうかについて、過去の類似の取組に係る法的整理に照らすと、第一の条件として、「一般的・類型的に見て、通常のユーザであれば許諾することが想定し得ること」が挙げられる。

- なお、上記条件のほか、「ユーザが、一旦契約約款に同意した後も、随時、同意内容を変更（オプトアウト）できること」「同意の有無にかかわらず、その他の提供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（オプトアウト）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」などが挙げられるが、ここでは、まず、第一の条件について検討を行う。
（→次ページへ）

2．アクセス警告方式について

2．アクセス警告方式について（つづき）

（3）アクセス警告方式の実施の前提となる法的整理（つづき）

- 一般的・類型的に見てユーザが許諾することが想定し得ると言えるためには、幅広く、かつ、偏りなくユーザの意向・意識を把握することで、その裏付けを得ることが必要と考えられる。この点、ユーザアンケートにおいて「アクセス警告方式に際して通信事業者がアクセス先をチェックすることについて「許容できる / 気にならない」と回答した人の割合は、５割に満たない結果となっている。
  →ユーザアンケート結果：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%

- また、検討の論点に対する意見募集においては、通信事業者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い。
  →意見募集結果「総論としてアクセス警告方式に反対」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」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」31件

- また、上記のユーザの反応については、静止画ダウンロード違法化の有無による違いは見られない。
  →意見募集結果「ダウンロード違法化が行われることで違いが生じる」４件、「ダウンロード違法化の有無による違いはない」９件
  → ユーザアンケート結果：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）

- 以上を踏まえると、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許諾することが想定し得る」とはいえないと考えられる。したがって、アクセス警告方式の実施に係る同意の取得方法に関して、約款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なる場合であっても同じ整理になるものと考えられる。

- ただし、ユーザから個別具体的かつ明確な同意を得ることにより、アクセス警告表示を実施することは可能。

2．アクセス警告方式について

2．アクセス警告方式について（つづき）

（４）導入及び実施のための技術的な課題・コストについて

- アクセス警告方式の実装方法としては複数の手法が考えられ、例えば、(a)ＤＮＳで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、別のサーバに誘導して警告画面を表示する手法（ＤＮＳ＋プロキシ方式)、(b)新たに用意する特殊なサーバを経由してウェブ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り替え等を行う手法（プロキシ方式）、(c)通信事業者の機器にパケットそのものをすべて点検する機能を持たせる手法（ＤＰＩ方式）などが考えられる。

- それぞれの手法によって課題・コストは異なるが、ＤＮＳ＋プロキシ方式やプロキシ方式では、通信の遅延が生じるおそれがあるほか、ＤＰＩ方式も含めた全般的な技術的課題として、SSL(TLS)を用いたブラウザからウェブ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。また、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あり方などによっても大きな差が生じる。
  →日本のユーザのHTTPSアクセス割合：73％(2019年4月）（再掲）
  →　最もコストが安価であると想定されるDNS＋プロキシ方式の場合、最小構成で初期費用18億+月2千万円、より現実的な構成の場合は初期費用46億円+月１億円（全国の固定系ISPを対象とした試算。全国に1000社と仮定した場合の総額。）

- また、日本には多数の通信事業者が存在し、通信事業者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、通信事業者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。

- 一方で、コスト負担のあり方については、本来は導入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、検討の論点に対する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、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等の意見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。

2．アクセス警告方式について

2．アクセス警告方式について（つづき）

（５）その他

- アクセス警告方式を実施・運営する場合には、対象サイトが合理的かつ必要最小限度の範囲となるよう、対象サイトの基準の公正・中立性が確保されることが必要であるほか、サイトリストの管理・運営等の透明性も確保される必要。誤ってリスト化されたサイトの救済手段についても要検討。

- 通信事業者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、ユーザの内心にかかわる機微な情報とも言えることから、通信事業者は当該情報について慎重に取り扱うことが必要。

- 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情報（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情報（ログ）は、通信の秘密に該当することから、通信事業者はこれらの情報については厳格な取扱いが求められる。

（６）まとめ

- 上記のとおり、ユーザから個別具体的かつ明確な同意を得れば、アクセス警告方式を実施すること自体は可能であるが、約款による包括同意をもって有効な同意があると考えることは困難。

- 技術的な課題やコストにかんがみれば、ユーザからの個別具体的かつ明確な同意に基づく警告表示やアクセス制限等の対応策については、ネットワーク側ではなく、端末側において実装を図ることも可能であり、また、むしろその方が効率的、あるいは、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ことから、以下、端末側での対応策について検討を行う。
  →End to Endの原則。ネットワーク上の通信経路に介入せず、発信側のエンド（削除、検挙など）または受信側のエンド（フィルタリングなど）での対策を行うべき。

３．その他のアクセス抑止方策について

３．その他のアクセス抑止方策について

（１）端末側での対応策に関する効果・メリット、具体的な対応策

- 端末側での対応策には、インターネットのEnd to End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が生じ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においては、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比較的低廉であること等のメリットがあると考えられる。
  →意見募集結果「端末側での対応策には一定のメリットがある」10件
- ただし、検討の論点に対する意見募集においては、端末側での対応策にはこうしたメリットはあるものの、法律で義務づけのある青少年フィルタリング以外の端末側での対応策については、利用に際してユーザが自ら申し出る必要があるため、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。

（２）具体的な対応策

- 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組み込み、ブラウザでの対応などが考えられる。
- １つ目に、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が、海賊版サイトへのアクセス抑止に資すると考えられる。
  →ユーザアンケート結果：「（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：42%　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%、15-19歳：57.5%
- 一方、フィルタリングソフトの利用にあたってのユーザ利便の向上、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。
  →ユーザアンケート結果：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%
- ２つ目に、セキュリティ対策ソフトへの組み込みによる対応策が考えられる。若年層以外におけるフィルタリングサービスの導入意向は必ずしも高くない一方、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する遮断・警告表示機能の追加に対する受容性は比較的高い。
  →ユーザアンケート結果：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%
  → ユーザアンケート結果：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%

３．その他のアクセス抑止方策について

３．その他のアクセス抑止方策について（つづき）

（３）その他

- ブラウザやＯＳなどの端末側ソフトウェアによる対応策を効率的に実施するには、ＯＳベンダーなどとの連携・協力をいかに得るかが課題。
- コスト負担のあり方について、端末側での対応策に要するコストはネットワーク側での対応策に比べれば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の負担のあり方については、慎重かつ丁寧な協議・検討が必要。
- アクセス警告方式の課題と同様に、フィルタリング等の対象となる海賊版サイトが合理的となるよう、サイトリストの管理・運営等の透明性も確保される必要がある。

（４）まとめ

- 青少年向けのフィルタリングサービスについては、フィルタリングソフトの利用にあたってのユーザ利便の向上、周知の強化等により、その普及を図っていくとともに、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。
- セキュリティ対策ソフト等への組み込みについて（P）

４．その他

４．その他

- アクセス警告方式については、ユーザの同意に基づいて実施されるものであるとしても、通信の秘密の保護や検閲の禁止などの法律上の要請にも関わりがあるものとして、意見募集においても多くの者から指摘や懸念が示されたことに留意し、ネットワーク側ではなく端末側での施策を促進することを中心に、海賊版対策のパッケージの一つとして取り組むことが肝要。

- 本施策は海賊版対策のパッケージの一つであることから、政府内で取り組むこととされている、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他の施策と組み合わせつつ、総合的に推進していくことが重要。