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（第２回）

令和元年６月３日

【濱田座長】　本日は、皆様、お忙しい中、お集まりいただきまして、ありがとうございます。定刻となりましたので、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（第２回会合）を開催させていただきます。

本日は、上沼構成員及び曽我部構成員、オブザーバーのデジタルコミック協議会様、出版広報センター様がご欠席となっております。

それでは、配付資料について事務局から確認をお願いいたします。

【中川消費者行政第二課課長補佐】　配付資料についてご確認させていただきます。本日、メーン資料が２－１、２－２、２－３とございまして、さらに、参考資料の２－１と、席上配付のみでございますがＡ３の参考資料２－２というものがございます。さらにもう一つ、Ａ４の席上配付のみと書いた資料が１枚ございます。過不足等ございましたら、事務局までお申しつけください。

【濱田座長】　資料はよろしいでしょうか。

それでは、議事に入ります。前回会合において、この検討会の「検討の論点」を取りまとめて、４月２４日から５月１４日までの間、提案募集を実施いたしました。これについて、事務局で提出された意見をもとに結果概要資料を作成いただきましたので、その説明をお願いします。

【中川消費者行政第二課課長補佐】　それでは、資料２－１についてご説明いたします。「提案募集の結果概要」と書かれた紙でございます。

１ページ目でございますが、提案募集の概要についてです。

提出された意見は計１２９件。うち法人または団体が１４件、個人の方から１１５件いただいております。

事前に第１回目で、論点１から１５まで論点があるのではないかというふうに構成員の方々からまとめていただきましたので、それについて幅広く意見をいただいたものでございます。

それでは、論点ごとに、大部ですのでかいつまんでご説明させていただきたいと思いま

す。

２ページ目をごらんください。論点１といたしまして、「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？」という論点でございます。

１つ目の分類として、当然、共通認識のもとで議論を進めるべきというものが１９件ございました。特に３ポツ目でございますが、海賊版流通の背景やそれによる影響・被害、また、さまざまな方策とそれにかかる法的課題や技術的問題について、検証可能な証拠・データに基づいた共通の認識の基盤の上で議論を進めるべきという意見がございました。

２つ目の分類でございますが、海賊版サイトの被害・損害について、正しい事実を前提に議論を行うべきという意見も６件ほどいただいております。

その他の意見といたしまして、「共通認識」とは何を指すのかがそもそも不明であるが、一刻も早く実効的な対策を講じることが急務であり、これまで醸成された共通認識のもとで議論を直ちに進めるべきであるというご意見もいただいております。

３ページ目、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？」についてでございます。

１つ目の分類でございますが、インターネットのあるべき姿を踏まえて議論すべきという意見を１７件ほどいただいております。

２つ目の分類といたしまして、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という意見を７件ほどいただいております。

４ページ目に移りまして、論点３「具体的な方策の検討に当たっては、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？」でございます。

１つ目の分類として、幅広いユーザの意見を聞き、ユーザの理解を十分に得て進めるべきという意見を２１件ほどいただいております。

２つ目の分類として、総論としてアクセス警告方式に反対という意見を６４件ほどいただいております。具体的には、例えば２ポツ目でございますが、利用の萎縮を招く可能性が極めて高いというような意見をいただいているところでございます。

５ページ目は、論点３の続きでございますけれども、１つ目の分類として、アクセス警告方式は通信の秘密を侵害する、また、通信の秘密への影響が大きいという意見を４５件ほどいただいております。

１つ目のポツですが、その仕組み上、憲法で保障された通信の秘密を侵すことになるた

め、実施するべきではない。また３ポツ目でございますが、ブロッキング方式の問題点は通信の秘密が守られないところにあるのに、アクセス警告方式も通信の秘密が守られておらず代替案として不適当といったような意見をいただいております。

２つ目の分類として、アクセス警告方式は国家による監視・検閲行為であるという意見も３１件ほどいただいております。

６ページ目も、さらに論点３の続きでございます。上から２番目の分類でございますが、アクセス警告方式の実効性に疑問というご意見も１４件ほどいただいております。

７ページ目になります。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？」でございます。

１つ目の分類として、民間主導で進められるべきというものが８件ほどご意見をいただいております。他方で、民間主導で実施すべきではないという意見も１４件ほどいただいております。例えば１ポツ目では、民間主導を建前としても許されてはならないという意見ですとか、２ポツ目、民主主義の手続きを経て公平・公正に進めるべきであるというようなご意見をいただいたところでございます。

また、３つ目の分類として、通信の秘密に関する法的整理については必要であるという意見も３件ほどいただいたところです。

次のページ、８ページ目でございます。論点５「アクセス警告方式の実施の前提について議論すべきではないか、また、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？」でございます。

１つ目の分類として、ダウンロード違法化が行われることで違いが生じるという意見を４件ほどいただいております。例えば１ポツ目、利用者への説明が容易で理解を得やすいというポイントがあるというようなご意見をいただいております。

２つ目の分類として、他方で、ダウンロード違法化の有無による違いはないという意見を９件ほどいただいております。１ポツ目で、通信の秘密を侵害するということは、ユーザによるダウンロード行為が違法であるか否かによる違いはないというご意見ですとか、２ポツ目のように、違法性の意識の有無によって、ユーザの行為が変化するとは思えないというようなご意見をいただいております。

３つ目の分類として、アクセス警告方式の目的や意味など、実施の前提について議論すべきという意見も８件ほどいただいております。こちらはブロッキングの議論を前提とすべきというような意見を具体的にいただいておるところです。

９ページ目に入ります。論点６として、アクセス警告方式のメリット・効果についてご意見を頂戴したところです。

１つ目の分類、アクセス警告方式にはメリットがあるという意見を４件ほどいただいております。例えば１ポツ目、「違法であることを知らせる」効果があるというような意見がございました。

２つ目の分類として、アクセス警告方式にはメリットはあるが限定的というようなご意見も６件ほどいただいております。例えば２ポツ目でございますが、ほか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というようなご意見をいただいているところです。

１０ページ目に移りまして、論点６の続きでございますが、他方で、アクセス警告方式のメリットはない、あるいはデメリットが大きいという意見を１４件ほどいただいております。

例えば１ポツ目、「警告が出てこないから合法サイトである」というようなミスリードを生むといったご意見ですとか、３ポツ目、国民のネット利用を畏縮させるだけであるというようなご意見が上がったところです。

１１ページ目、論点７に移ります。「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？」という論点でございます。

１つ目の分類として、包括同意ではなく、個別同意が必要であるという意見を７件ほどいただいております。

２つ目の分類として、ユーザが約款に気づかず同意したり、意味を正しく理解せずに同意したりすることになるので不適切、あるいは、通常の利用者であれば承諾するという想定が困難であるというご意見を９件ほどいただいております。具体的には１ポツ目、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。このようなご意見をいただいております。

３つ目の分類として、契約法の原則に照らして無効であるとか不当条項に当たるというような意見も８件ほどいただいたところです。

１２ページ目、論点７の続きでございますが、セキュリティ対策にお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という意見を４件ほど。２つ目の分類として、たとえ同意があっても許されないということを１０件ほどご意見をいただいたところです。

次のページ、さらに論点７の続きは、その他ということで割愛させていただきます。

１４ページ目に移りまして、論点８でございます。「アクセス警告方式に関する技術的な課題はあるか？」という論点でございます。

分類の１つ目ですが、技術的課題を明らかにすべきというご意見を９件いただいております。

２つ目の分類として、暗号化通信の場合に実施が困難であるという意見も１２件ほどいただいたところです。例えば２ポツ目でございますが、ＨＴＴＰＳ通信をはじめとしたエンドツーエンド通信の暗号化による保護技術により技術的に実現できないと考えるといったような個別の意見を頂戴したところです。

１５ページ目、論点８の続きでございます。その他として、例えば２ポツ目でございますが、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といったような意見もいただいております。

１６ページ目に移ります。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？」でございます。

１つ目の分類のご意見として、コスト負担の議論を深めることが必要というものを８件ほどいただいております。例えば１つ目のご意見でございますが、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るといったご意見をいただいております。

２つ目の分類として、コストは受益者負担とすべきというような意見も６件ほどいただいております。

１７ページ目に移ります。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？」でございます。

１つ目の分類として、リスト管理等の実際の運用の在り方について議論が必要であるという意見を２０件ほどいただいております。

２つ目の分類ですが、アクセス警告方式の実効性に疑問という意見を１４件ほどいただいております。

さらに３つ目の分類として、機微情報の取り扱いに関して慎重に議論すべきという意見を８件いただいております。

具体的に機微情報と申しますのは、１ポツ目ですが、例えば利用者が拒否の申出をした事実自体は、利用者の内心にかかわる機微な情報であることで、管理について検討を要す

るというような意見をいただいております。

ここまでがいわゆるアクセス警告方式と呼ばれるネットワーク側での対象についての論点でございます。

１８ページ目からは、その他の方策として、主に端末側での対処についての論点に移りたいと思います。

１８ページ目、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？」という論点でございます。

１つ目の分類として、端末側での対応策には一定のメリットがあるというご意見を１０件ほどいただいております。例えば１ポツ目、通信の秘密に関する問題が回避されるというメリットがある。また、２ポツ目でございますが、ＩＳＰのネットワークに新たな設備を導入する必要がない。また、導入の迅速性の点についてもメリットが大きいというようなご意見があったところです。

２つ目の分類として、端末側での対応策にはメリットがあるが効果は限定的というご意見も４件ほどいただいたところです。

続いて１９ページ目、論点１２でございます。「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？」という論点でございます。

１つ目の分類として、ブラウザでの対応が考えられるというご意見が４件ほど。

２つ目の分類として、既存のフィルタリングサービスが存在するというご意見が４件ほど。

また、その他として、例えば各端末のＯＳベンダーの協力を得ることを検討すべきといったご意見もいただいたところです。

２０ページ目に移ります。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？」という論点でございます。

その他という分類になってしまいますが、１つ目、例えば１ポツ目でございますが、フィルタリングサービスの状況等を参考例として、今後こういった技術について検討していくのがよいというご意見をいただいたところです。

おめくりいただいて、２１ページ目でございます。論点１４として、「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？」という論点でございます。

１つ目の分類として、コストは受益者負担とすべきというご意見を３件ほど。

その他として、例えば３ポツ目ですが、フィルタリングソフトの利用料の負担が問題になるですとか、このコストを誰が負担すべきかは議論のテーマにあるといったご意見をいただいたところです。

２２ページ目に参ります。論点１５でございますが、「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？」という論点でございます。

ここも分類としてはその他ということになりますが、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、別途課題になるというご意見ですとか、４ポツ目でございますが、ユーザが所有する端末は、当然ながらユーザの財産でありプライバシーの塊であることを留意すべきといった意見ですとか、５ポツ目として、幅広い国民に対して利用を促すのであれば、その正当性を十分に確保して、維持することが必要といったご意見をいただいております。

ここまでが第１回目でご議論をいただいた１５の論点にかかるご意見でございます。

２３ページ目以降は、その他の意見ということで、論点外ではございますが、他の海賊版対策とアクセス抑止方策との比較を含む、海賊版対策全般への評価についても多くご意見をいただいたので、別途まとめているところでございます。

１つ目の分類として、海賊版サイト運営者の取締・執行強化が必要であるという意見を３９件、いただいております。例えば１ポツ目でございますが、アップロードによる著作権侵害に対する民事・刑事の権利行使においてどこにボトルネックがあるのかを明らかにした上で、そのボトルネックを解消するための地道な取り組みのみに注力するべきであるというご意見ですとか、３ポツ目でございますが、実施すべきはアップロード者の取り締まりであって、国境を越えて取り締まれるための海外の連携などについて考えることが必要であるというご意見をいただいております。

２つ目の分類として、民事上の法的訴求に資する取り組みや制度改正が必要というご意見を１２件ほどいただいております。

３つ目の分類は、広告対策が必要というご意見を１４件ほどいただいたところです。

２４ページ目はその他の意見の続きでございます。

正規版流通強化が必要というご意見を９件ほどいただいております。例えば１ポツ目でございますが、「正規コンテンツ」が買われていれば、「海賊版コンテンツ」は使われないので、「正規版コンテンツ」が買われるような施策を明確にすることが必要だというご

意見があったところです。

２５ページ目もまだ続きですが、著作権教育・啓発が必要というご意見を５件ほど、ブロッキングが必要であるというご意見を４件ほどいただいております。他方で、ブロッキングに反対というご意見を１３件ほど、フィルタリングが必要であるということを５件ほどいただいております。

最後のページは、その他の意見となっております。

駆け足ですが、意見募集の結果の概要については以上でございます。

【濱田座長】　どうもありがとうございました。いろいろご質問やご意見あるかと思いますが、一わたり報告を伺って、その後で委員の皆様からご議論をいただければと思っております。

それでは、引き続いて、議題の２番目になりますが、事務局で５月１６日から１７日までの間、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して調査をいただきました。調査結果資料を作成いただいておりますので、その説明をお願いいたします。

【中川消費者行政第二課課長補佐】　それでは、資料２－２についてご説明いたします。こちらは、前回、第１回目のご議論で、ユーザの声、意向を聞くことが重要ではないか。特に正式なダウンロード違法化がなされた場合、なされない場合、その場合分けをして、ユーザの意向というのをよく確認したほうがいいのではないかというようなご意見を構成員の方々からいただいたこともございまして、アンケート調査を行いました。その結果の報告でございます。

１ページ目でございますが、調査の概要です。

調査の手法としては、まずウェブアンケートという手法で、調査対象は、１５歳から６９歳までの男女。

対象としては、インターネットを週１回以上使う方々の構成比に基づいて、無作為抽出でアンケートをとったところです。

回答者の数は、約２，０００名となっております。

おめくりいただきまして、２ページ目が調査の概要といたしまして、この導入の説明を実際のアンケートの際にも、回答していただいた方に示して回答を募ったところです。海賊版サイトの説明ですとか現状、また、その侵害状況、被害状況。また、著作権法上、ダウンロードする行為や閲覧する行為がどう評価されるのかという前提をしっかり説明した上で、回答していただくようにしております。

３ページ目に移りまして、最初は幾つか答えていただいたユーザの属性に関する結果でございます。属性の１つ目といたしまして、回答していただいたユーザがどれほどインターネットサイトにアクセスしているかの属性でございます。結果を見ますと、インターネットによくアクセスしている方というのは、２０代が最も多く、年代が上がっていくにつれて減少傾向にあるという結果が出ております。

４ページ目に移りまして、属性の２つ目でございますが、インターネット上で漫画が掲載されたサイトにアクセスして、漫画を閲覧したことがあるかという結果を聞いております。ここでは、正規版サイト、海賊版を問わず、インターネット上で漫画を読んだ、その割合について聞いているところでございます。

結果は、インターネット上で漫画を読んだことがあるのは、１０代が最も多く、年代が上がっていくにつれて減少傾向にあります。特に６０代に至っては、１割を切る結果になっております。

５ページ目でございますが、先ほどの属性２で、インターネットで漫画を読んだことがあると答えた者のうち、そのうち、特に海賊版サイトにアクセスしたことがありますかという割合を聞いたものでございます。こちらも２０代をピークにしておりまして、年代が進むごとに減少傾向にあるところです。２０代の方だと、ネットで漫画を読んだことがあると答えた者のうち、約６割が海賊版にアクセスしたことがあるという結果が出ております。

ここまでが今回、回答いただいた方の属性でございまして、６ページ目以降がそれらのユーザの受容性の結果になっており、アクセス警告表示に対する受容性の結果になっております。

まず６ページ目でございますが、アクセス警告表示に対する反応を、現行法を想定して聞いたものです。図の左側にあります警告画面のように、あなたが海賊版サイトにアクセスしようとしているときに「本当にアクセスしますか？」という問いとともに、「はい」、「いいえ」を選択するような警告が出た場合に、「はい」を押して、それでも海賊版サイトにアクセスする人の割合を聞いたのが右のグラフでございます。結果を申し上げますと、「アクセスしないと思う」、すなわち思いとどまると考える方の割合が全体の９３．３％と高い数値になっております。

７ページ目に移りまして、前ページで警告画面を表示させる際には、通信事業者がユーザのアクセス先をチェックする必要があるという前提を事実と説明した上で、そのアクセ

ス先をチェックされることについて許容できますか、許容できませんかと聞いた結果になっております。

「許容できる／気にならない」と回答した者は、全体の４４．７％。他方で、「許容できない」と回答した者は、全体の３５．３％という結果になっております。また、「わからない」と答えた者も２０％という回答結果になっております。

おめくりいただきまして、８ページ目、９ページ目ですが、紙の資料をお持ちの方は、見開きで６ページ目、７ページ目と比較する形で見ていただくとわかりやすいかと思います。

８ページ目は、６ページ目の警告表示で、それでもアクセスする人かどうかという結果と比較して、静止画ダウンロードが違法化されたという想定をしたときに反応がどう変わるかというものを聞いたものでございます。結果としては、静止画ダウンロードが違法化された場合、警告画面の表示に対して、それでも「はい」を押して、海賊版サイトにアクセスすると答えた人の割合でございますが、「アクセスしない」と答えた人が９５．９％。現行法に比べて２．６％ほど増加しているという結果が出ております。

９ページ目に移りまして、またこれも静止画ダウンロードが違法化されたという想定でございますが、その警告表示に当たって、アクセス先をチェックされることについての許容度について聞いたものでございます。こちらは、静止画ダウンロードが違法化された前提での許容度でございますが、「許容できる／気にならない」と答えた者が４６．８％、現行法想定時回覧２．１％微増しております。他方で、「許容できない」と回答した者は、全体の３４．７％でございまして、現行法想定から０．６ポイントの微減となっております。

１０ページ目以降が、今お話しした受容性についての回答と属性とのクロス分析となっております。１０ページ目は現行法想定でございますが、どんな属性で、警告表示に対する受容性が変わるかというグラフでございます。ボックスのまとめの中の１ポツ目でございますが、非ネットユーザ、つまり、ふだんあまりインターネットサイトにアクセスしないような属性の人は、アクセス先をチェックされることについて、「わからない」と回答した割合が高くなっておりまして、さらに、警告画面を表示させることについても許容度が低いという結果が出ております。

ボックスの２つ目でございますが、今度は海賊版サイトにどれほどアクセスしたことがあるかという属性とのクロス分析の結果でございますが、海賊版サイトにアクセスしたことについて認識がない。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で

すとか、あるいは海賊版サイトにアクセスしたことがない、経験がないと答えた人ほど、警告画面を表示させることについては許容度が高いという傾向が見られました。

ただ、３ポツ目でございますが、どの属性においても、およそ３０％以上が「許容できない」という回答が得られておりまして、ここは一定数「許容できない」と回答する者がどの属性でも見られたという結果になっております。

１１ページ目が、１０ページ目と同じ質問を、静止画ダウンロードが違法化されたという想定で聞いたグラフになっております。グラフの形を見比べていただければわかると思いますが、いずれの傾向も現行法想定時と静止画ダウンロード想定時と大きな差異は見られないというのが特徴になっております。ボックスの中の４ポツ目でございますが、大きな差異は見られないというのが前回の傾向として出ております。

続きまして、１２ページ目でございます。さらに、この現行法想定時と静止画ダウンロードが違法化されたという想定で、どのような回答の違いが生じるのかというのを、縦軸、横軸で調べてみたものでございます。

赤い枠が５つございますが、要するに、現行法想定であっても、ダウンロードが違法化されたという想定であっても、おおむねアクセス警告表示の受容性に対する傾向に変化はない。同じ回答を維持するという割合が非常に高いという結果が示されております。

ここまでがアクセス警告表示に関する受容性の調査でございます。

１３ページ目以降は、そのアクセス警告方式以外の受容性についても幾つかアンケート結果が出ておりまして、その分析でございます。

１３ページ目は、フィルタリングソフトによる対策についての受容性でございます。まず導入として、現在は、主に１８歳未満の青少年向けにフィルタリングソフトというサービスが提供されておりますが、このフィルタリングソフトは、大人向けのサービスというのもございまして、例えば薬物の売買ですとか、フィッシングサイト、銀行等のなりすましのサイトなどの有害なサイトにアクセスしないよう、大人向けにもインストールできるようなサービスが提供されております。ここではそのフィルタリングサービスに海賊版サイトへのアクセスもフィルターされるような機能というのが付加されておりますので、そのようなフィルタリングソフトの受容性について回答を得たものでございます。

結果としては、「インストールしたい／してもよい」と答えた者は、若い年代ほど高い。他方で、年代が上がっていくとどんどん受容性の割合が低くなっていくという結果になっております。

おめくりいただきまして、先ほどの問いについて、フィルタリングソフトを「インストールしたくない」、あるいは「一定の場合」には「インストールしてもよい」と答えていただいた方の理由を複数回答で聞いたものでございます。フィルタリングソフトを「インストールしたくない」と答えた理由のうち、一番多かったのは、左側のグラフの下から２番目でございますが、「どれが安全なフィルタリングソフトかの判別が難しそうだから」というものが３５．３％で最も高かったものでございます。

「一定の場合」にはフィルタリングソフトを「インストールしてもよい」と答えていただいたうち、多かった理由としては、上から２番目と３番目でございますが、「手続きが簡単であればインストールしたい」あるいは「使いやすいソフトであればインストールしたい」、この２つが５割弱ということで、最も多かった理由になっております。

最後、１５ページ目でございますが、セキュリティ対策ソフトによる対策の需要についても問いをつくっております。現在のセキュリティソフトですとか端末のセキュリティ対策機能については、ウイルスに感染する可能性のある危険なサイトに対して、警告表示ですとか、アクセスを遮断する機能がございますが、それらのソフトなどについて、海賊版サイトへのアクセスに対して警告表示をしたり、遮断を行う機能について追加したりすることについてどう思うかという問いでございます。

結果といたしましては、「機能を追加してほしい」と回答した者が全体の７８．４％と、比較的高い割合となっております。

資料２－２についての説明は以上でございます。

【濱田座長】　どうもありがとうございました。

それでは、続いてになりますが、議題の３のところで、一般社団法人日本インターネットプロバイダー協会より、「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」について、日本インターネットプロバイダー協会の野口様からご発表をいただくことになっております。野口様、よろしくお願いいたします。

【日本インターネットプロバイダー協会（野口氏）】（スライド p1）　ただいまご紹介をいただきました日本インターネットプロバイダー協会、略してＪＡＩＰＡの野口と申します。今日は発表の機会をいただきまして、ありがとうございます。

ＪＡＩＰＡからは、アクセス警告方式をＩＳＰ事業者が行うとしたらというテーマで、技術的な検討をしたものを発表させていただきたいと思います。

（スライドp2）

まず最初に「おことわり」です。時間の関係で、技術的な説明は大分簡略化をしていますのでご了承ください。また、事務局からは、ネットワーク上でのアクセス警告方式について頼まれているので、端末でのフィルタリングや発信者の検挙などについては、今回は検討をしていません。

（スライドp3）

今回の目次です。これの順序で、おおむね２５分から３０分程度になるでしょうか。説明させていただこうと思います。

（スライドp4）

ここからしばらくは前提になってしまうと思いますが、そもそも何でウェブがつながるのかというお話からさせていただこうと思います。

（スライドp5）

ウェブサイトが表示される仕組みを一度振り返ってみたいと思います。途中のルータという機械はＩＰアドレスしか扱えないものなので、プロバイダのＤＮＳという装置で、ホスト名をＩＰアドレスに変換して、その上でルータにパケットを委ねるような仕組みになっています。このようなネットのつながる仕組みを考えれば、ネットワーク上でアクセスを成立させないということを考えるのであれば、このプロセスのどこかを妨げればいいということになるとは思います。

（スライドp6）

後で詳しく説明させていただくんですが、最近は通信のエンドからエンドまでを暗号化する仕組みというのが一般的になっていまして、これによりプロバイダでも途中で関与するのが難しくなっている点があるということについて、一応気にとめておいていただけたらと思います。

（スライドp7）

参考までに、今、児童ポルノのブロッキングがどんなふうに行われているのかを説明しておきたいと思います。簡単に言うと、プロバイダのＤＮＳサーバが、うそのＩＰアドレスを回答しまして、本来のサーバに行くはずの通信を別のサーバに着信させまして、そこで児童ポルノへのアクセスは禁止ですという画面を表示させています。

（スライドp8）

そうしますと、アクセス警告をネットワーク上でやろうとしたら、ブロッキングと同じようにＤＮＳのところで一度介入するか、またはルータのところでパケットを全部解析す

るＤＰＩという機械を入れるか、この２つが主に考えられると思います。全部プロキシ経由にするという方法もあるとは思うのですが、ちょっと時代に合っていないので、検討から外しています。

（スライドp9）

ここから２つ、方式をそれぞれ検討してみたいと思います。

（スライドp10）

まず、ＤＮＳとプロキシを使った方式を説明します。こちらが簡易だったので、先に説明いたします。これは途中までブロッキングと同じやり方をしている、すなわちＤＮＳを書きかえているわけなので、警告画面を出そうとすると、それでもアクセスしますかという問いに対して、「はい」をクリックしても、結局また同じところにつながってしまって、本物のウェブサーバにつなぐということはできなくなってしまいます。ブロッキングだけでしたらＤＮＳだけでもよいのですが、本来の通信先に戻せないという点が今のブロッキングの問題になります。

（スライドp11）

技術的な検討を頼まれていますので、だめな理由ばかり考えても仕方がないわけで、可能な方法が少しでもないかと思って考えていました。先ほどの警告画面を表示するサーバにプログラムでしかけをつくって、それが１回目のアクセスなのか、２回目のアクセスなのかというのを検出すればいいわけです。２回目以降はプロキシとして振る舞うようにして、本来のウェブサーバのほうからコンテンツを中継する仕組みにしてしまえば、一応不可能ではないというか、可能だとは思います。ただ、このような仕組みが実際に商用のネットワークで大々的に使われているようなことはないと思いますし、ほんとうに実施するということになれば、十分実験をしてからでないと厳しいと思います。

あとは技術的に言うと、ソフトウェアで全部処理をするので、ハードウェアでやるよりは大分遅いんじゃないかなという気がします。ＤＮＳで前さばきして，対象になったものが遅くなるということです。

（スライドp12）

次に、コストや導入規模の話をするのですが、一度前さばきをＤＮＳで実施しているので、このプロキシを通るトラヒックは多くないと信じたいところです。ここがあふれるようですと、これは社会的にすごい大問題なのではないか、と思います。とりあえずどれぐらいのものを考えるかという点なんですが、自社で、各社が実験のレベルでプログラムを

書いてみて、とりあえず試験運用に持ち込むことができればよい、というレベルを考えてみたいんですが、(スライド p13)ここですみません、ちょっと細かい「おことわり」になります。この手の見積もりはどうしても幅が出てしまうという点が１点と、運用の人件費ですとか、既存のサーバの一部の機能を流用するとかそういったことについて、今申したような費用がただということになってしまうと話がすごくおかしくなるので、その点についてはご留意をいただけたらと思います。

(スライドp14)

また、これはひとり歩きすると困る数字なんですけれども、こんなものをほんとうに商用のネットワークに入れるのかと言われそうなスペックなので、ほんとうに最低限か最低限以下と思っていただいていいと思います。そうすると、資料にある程度の金額になるかとは思います。大手さんの場合だと、どうしても設備が多いのでもっとかかるかもしれませんけども、初期がこれぐらい、運用がこれぐらいという感じだと思います。

これは上の部分というのは１社の金額を出しているので、全部じゃないですね。日本はどうしてもプロバイダがいっぱいあるので、競争が多くなって、値段が下がるというメリットはあるのですが、どこか１カ所で通信をコントロールするですとか、そういったことにはとても不向きな構造です。

(スライドp15)

先ほどのものですと、法的にはおそらく必須と言えるはずのオプトアウト等も全然実現していないので、様々直そうとすると、お示ししているように、大分上がっちゃうと思います。初期がこれぐらい、運用がこれぐらいという感じだと思うのですが、これも上のほうの緑色の枠は１社の金額なので、大手だともっとかかるだろうとは思います。あとは、被害額が３，０００億円というような大手の海賊版サイトができてしまうと、本当にトラヒックも半端ではなくなってしまうため、こういったプロキシもとんでもない数を導入しないといけなくなってしまい、費用もやはりその分膨らむということはあるだろうとは思います。

(スライドp16)

盛り過ぎだとか、アクセス警告方式を導入されないために不誠実な見積もりを出しているんだといったことは全然心外なので、最低限で今、金額をはじいてみました。ただ、そうは言っても、実運用されていないものをいきなりネットワークに入れるのかという話にもなってしまいますし、技術的にもどうしても詰めが甘いものなんですね。ストリーミン

グが通らないとか、違法でもないとしてもストリーミングが通らないという問題も結構あると思いますし、一番の問題というのはおそらく、後で説明しますけども、暗号化通信のＨＴＴＰＳが通らないというところ、これが一番大きいのではないかと思います。

（スライドp17）

続きまして、こちらは、もう少し実績があるものです。先ほどの方式は実績がないと言いましたが、こちらは、実績があるにはあると思うため、その点で考えますとＤＰＩ方式のほうが設備としては、検討されるものだと思います。ただ、これは全部のパケットを見ないといけないが、そうすると、オプトアウトの実装という話になってくるため、どうしても利用者の回線に近いルータのほうに設置しなくてはならなくなってくるので、どうしても台数が膨らんでしまうんです。

（スライドp18）

技術的なメリットとしては、漏れが少ないということだと思います。何しろ全てのパケットを監視するわけですから。但しそうはいっても限度はあるのですが。

（スライドp19）

この導入のスケールなんですが、全国、何しろルータがある場所、たくさんにつけないといけないので、先ほどとちょっと何桁も違う規模になっちゃうんですね。例えばＮＴＴ東西のフレッツ。シェアが一番高いフレッツとプロバイダをつなぐ接続点のルータなのですが、これは公表されている資料で、１Ｇｂｐｓの装置が１万１，０００台あるというふうに書いてあります。そうすると設備の台数で見積もるのも結構難しいのですが、あとはトラヒックからも推計してみる。そんな感じになってしまうと思います。

（スライドp20）

次、お願いします。総務省の推計から、ダウンロードのトラヒックを調べてみると、１日平均で１１Ｔｂｐｓというふうになっていました。そうすると、ピークの時間帯というのは平均の３倍というふうに仮に見たとすると、単純計算で、１０Ｇｂｐｓの装置が３，３００台というふうに出てしまいました。これはトラヒックに比例なので、日本全体でどれぐらいかかるのかと試算していくんですけども、ＤＰＩの装置というのは非常に値段が高くて、１０ギガが通るものというのは大体２，０００万円から５，０００万円ぐらいだそうです。電気も非常に食うし、保守費も高いという代物で、仮にこれ、１台３，０００万円の装置を３，３００台となると、初期だけで１，０００億ということになってしまいます。しかも、これは皆さんに本当に同情してほしいのですが、トラヒックというのは今すごい

増え続けていまして、５年で３倍に膨れ上がっているんです。売り上げが５年で３倍になってくれればいいのですが、人口が減る中で固定系の売り上げは増えるはずがないというのが実はありまして、そこもネックになると思います。

（スライドp21）

ＤＰＩの問題点なんですけども、暗号化されてなければ何でも読めてしまうため、心理的な抵抗がすごい多いということと、思想的な問題はともかく、海賊版対策でこの設備を入れてくれと言われてしまうと、やはりちょっと過剰設備もいいとこですし、この設備にかかる費用をプロバイダが負担してくださいと言われましても、そんなお金を持っているところというのは多分ないと思います。こんなこと、最後に言うなと言われるかもしれないのですが、この方式であってもＨＴＴＰＳ、暗号化通信に対応するというものは、少なくとも商用のＩＳＰでは難しいと思います。

そして

（スライドp22）

方式の比較を並べてみました。このためにＤＰＩを入れてくれと言われてしまうと、多分タスクフォースの比ではなく紛糾する気がするため、どれを選ぶかという話になってくると、「ＤＮＳ＋Ｐｒｏｘｙ方式」なのではないかと思います。ただ、結局どの方法をとっても、暗号化通信、ＨＴＴＰＳへの対応が難しいという点がネックになるだろうと思います。

(スライドp23)

ここからちょっと雰囲気が変わります。アクセス警告方式と技術的に安全なインターネットというところの関係を見ていこうと思います。

(スライドp24)

先ほどから、ＨＴＴＰＳの対応が難しいということを何度もお伝えしてきたのですけれども、これは簡単に言いますと、ＳＳＬ、ＴＬＳとも言うんですけど、これを使ったサイトへの通信というのがブラウザからウェブサーバまでの間が全部暗号化されちゃっているため、ネットワークの途中で手を加えることができないということなのです。ブラウザのアドレスバーのところに南京錠のマークが出ているのが目印なのですが、これはすごく多いと思います。

(スライドp25)

そもそもなぜこのようになっているのかといいますと、インターネットに限らず電話も

そうだと思うのですが、通信というものは、エンドからエンドまで、内容を変えずにそのまま届けられるということが本来でありまして、これをＥ２Ｅの原則というふうによく言っています。通信の途中でその内容を見られたりですとか、書きかえられたりですとかしてしまうと、ちょっと俗っぽい話なのですが、産業機密も流せなくなってしまいますので、非常にビジネスでも困ってしまうことになります。ですので、おそらく違法情報とか有害情報も基本的にはどっちかの端っこ、エンドで対応してもらいたいということになるのだと思います。

（スライドp26）

もう一つは、２０１１年のブロッキングが始まったときから、今年の２０１９年までの間に大きな変化があったと言えると思います。スノーデンさんの告発が機になるのですけれども、主なウェブサイトがみんな暗号化通信を行うようになってしまったんです。昔は個人情報を送る場合ですとかそういうシーンに暗号化を実施していたのですけれども、今ではもう会社のトップページからみんな暗号化通信を使っています。これを常時ＳＳＬ化とか、常時ＴＬＳ化という言い方をしているのですが、暗号化の仕組みについて少しだけ、ここからお話をいたします。

（スライドp27）

うそ、大げさ、紛らわしいというわけではないんですけれども、ネットで技術的にあっては困ることというのが、代表例としては、「盗聴・改ざん・なりすまし」という、このあたりになってくると思います。

（スライドp28）

これに対抗する手段としては、結局、エンドツーエンドの暗号化というのが今の一応の答えになっていまして、インターネットというものがどうしてもＷｉ－Ｆｉだったり、マルウェアのような、途中で通信を横取りしてしまうポイント、横取りできてしまうポイントが少なくないので、結局これに尽きるというふうに思うのです。

（スライドp29）

エンドツーエンドの暗号化というのは、どうやっているのかという話なのですが、暗号と、もう一つ、電子証明書の技術を使っています。この暗号と証明書の技術を使って、「盗聴・改ざん・なりすまし」、この３つを一気に防いでいるのがＴＬＳという技術です。もともとＳＳＬと呼ばれていたのですけれども、同じものと思っていただいて、とりあえずここでは大丈夫です。ＳＳＬとかＴＬＳを使ったウェブのアクセスというのがＨＴＴＰ

Ｓということになります。

（スライドp30）

有名なサイトに幾つかアクセスしてみたんですけども、どれもおなじみの南京錠のマークがついています。

（スライドp31）

これはさっきの画像を拡大したものです。一番下のものは、最近はやりのＥＶ ＳＳＬといって、発行者の登記簿まで確認するタイプの証明書です。

（スライドp32）

繰り返しになってしまうのですが、南京錠のマークがついていることで、盗聴できないこと、中で内容を見られないということと、途中で改ざんされてしまったら、それが検出できて、エラーになるということと、もう一つ大事なんですけど、接続先が確かにそのサイトで、この図で行けば、確かにこれがグーグルのサイトなのかということ。それが、これがついていると保証されますよ、確認できますよという意味になります。

（スライドp33）

なりすましの防止のところ、これは結構大事なんですけど、わかりにくいため、説明させていただきたいと思います。ＴＬＳは、暗号の通信を始める前に、相手のサーバの証明書が正しいものなのかどうかを検証します。相手が持っている証明書が不適切であったり、本物と確認できない場合はエラーにしてしまって、通信そのものを成立させない仕組みをとっています。

（スライドp34）

にせもののウェブサーバが横行してしまうと、それこそ電子商取引、ネット通販とかの基盤まで一気に崩壊してしまうので、電子証明書の発行プロセスは国際的に決まっていまして、それに準拠した証明書でなければ、ブラウザがそれを信用せず、エラーを出してしまうということになっています。

（スライドp35）

ブラウザの開発元としても、安全な通信というのは利用者を守るためにとても必要なこと、大事なことだと思っていますので、今、ブラウザによっては、暗号化未対応のサイトについては、ここまで言われてしまいます。これはどこかの中央省庁のウェブサイトから持ってきたんですけど、「Not secure」と、すごい言われようだと思うのですが、いいんでしょうか。

（スライドp36）

このような状況ですから、ウェブサイトのアクセスで、暗号化通信が使われる割合というのは急上昇しています。もう暗号化通信に対応していないと、ブラウザに「Not secure」とか言われたりですとか、グーグルですと、ＨＴＴＰＳ、暗号化に対応していないサイトの検索順位が下がったりですとかしております。そうすると商売をやっている方でしたら間違いなく対応すると思われますので、このような結果になると思います。

日本は少し、この緑の一番下の線であり、ちょっと導入が遅れているのですが、２０１６年１１月に４分の１だったところが、逆に２０１９年の４月には４分の３まで増えましたので、一気に逆転と言っていいと思います。

（スライドp37）

ウェブの閲覧だけではなく、おなじみのスマホアプリですとかゲームですとか、これはほとんどＴＬＳを裏で使っていると思います。ゲームというのは、実は利用者自身にも通信を読み取られたくないものでございます。なぜかというと、チートされてしまうからです。

（スライドp38）

法的な話は一旦専門の先生に委ねるとしまして、純粋に技術的に言うと、アクセス警告方式というものは、利用者のアクセス先がどこであるかを確認して、警告サーバが正規、要するに、本来のアクセス先のかわりに、本来のコンテンツを警告画面に差しかえる形で表示するという性質のものになるのですけれども、

（スライドp39）

これは技術的に言うと、盗聴して、なりすまして改ざんしようという話なので、どれもセキュリティで防御しようとする保護の対象と申しますか、脅威そのものということになるわけです。

（スライドp40）

そうしますと、変な言い方ではございますが、本物の海賊版サイトが暗号化に対応してしまった場合、している場合につきましては、本物のサイトは正しい証明書を持っているため、そこに対しては通信が成立するのですが、警告画面を表示するサーバをプロバイダがつくったとしても、そこは本物の証明書を持っているはずがないので、ブラウザとしては、これはＤＰＩでも同じなのですけれども、証明書の検証が失敗ということで、通信が成立しません。

（スライドp41）

そうすると、警告画面はやはり表示できず、ＴＬＳの通信そのものが成立しないため、ブラウザがはじくことになります。したがって、アクセス警告方式はやはり使うのが難しいということになってしまうものと思います。

（スライドp42）

先ほど申し上げたように、ウェブのアクセスであれば、７３％が暗号化通信を使っているというお話をしましたが、そんな中で、「盗聴・改ざん・なりすまし」と、技術的には同じことをしようとしているということをご理解いただいておいて、損はないかなと思います。

海賊版対策を「盗聴・改ざん・なりすまし」と言うと、何か人聞きが悪いと怒られるかと思うのですけが、目的が正当ならいいんじゃないかというのは、それは結構、法律家の価値判断でございまして、これに対して技術者の答えは逆に一つなのです。「盗聴・改ざん・なりすまし」は技術でもって排除いたします。この一言です。

（スライドp43）

これは常時ＴＬＳ化、暗号化で、多くのサイトが暗号化対応になってくれること自体は、改ざんですとか、なりすまし防止の観点から、とてもいいことだと思います。イデオロギーですとか、そういったもの以前に実際に安全な通信になりますし、この流れ自体はもう止めようがありません。そうしますと、アクセスプロバイダに対して、こういったことを対応してくださいという期待をされるお気持ちはわかるのですけれども、我々もネットワークで通信をコントロールすることがだんだん不可能になっていて、もはやコントロールを失っていると言ってもいい状態だと思います。

（スライドp44）

先ほどのグラフをもう一回振り返って見てみたいんですけども、結局、どんな方式をとったとしても、アクセス警告方式が適用できそうなのは、これはブロッキングもそうなのかもしれないんですけど、今の時点で２７％ぐらいということになってしまいますので、主要な海賊版サイトが暗号化通信に対応してしまった場合には、残念ながら今までやってきたことも、終わってしまいます。

（スライドp45）

この点について、海賊版サイトがＨＴＴＰＳ、暗号化通信対応になるの？　という話を結構聞かれることがあるので、質問形式でお答えしておきます。暗号化通信に対応させる

ことですが、これは簡単です。証明書は、実は今、１５分ぐらいで取得でき、お金もそんなにかかりません。ただし、本物のウェブサイトの管理人であることは、これはしっかりと確認されているので、それ以外の人が取得するということはできないようにちゃんと設計されています。

（スライドp46）

質問コーナーの感じでもう一個行ってみます。スライドをごらんください。ＤＰＩ装置でＨＴＴＰＳをやっているところはございます。確かにあるのですが、ただ、それは利用者が特定の人に限られた特殊な環境であればできると思うという話です。会社の社内ＬＡＮ等であればできるかもしれません。

（スライドp47）

先ほどの前提なのですけれど、にせものの電子証明書しか持っていない場合には、これは本物である、とブラウザに信じてもらえれば実行可能であると思います。

（スライドp48）

これを、どうやっているかという話なんですけども、途中で暗号化の通信を一度ほどいて、内容を差しかえて、もう一回暗号化することができれば、アクセス警告などを出すこともできると思います。ただ、やはり途中の装置は本物の証明書を持っていないため、通信は成立せず、失敗してしまうのです。

（スライドp49）

それをどうやって実施するのかという話ですれけども、途中の装置が持っている証明書を、ブラウザに信頼できる証明書ということで、信頼できる証明書のリストに追加してもらうのです。これは、例えば社内ＬＡＮですとか、大学のＬＡＮ等であれば多分できるのではないかと思うのですけれども、これを商用のプロバイダで、ＩＳＰがやろうとするとどうなるか。おそらくこういうメールが皆さんのところに届くのだと思います。お客様のブラウザにルート証明書の追加をお願いしますというようなことになるのではないかと思います。

（スライドp50）

（スライドp51）

そうなると、おそらくＳＮＳはこういう反応になるんじゃないかと思います。プロバイダがルート証明書を入れろということは、普通はやりませんし、言ってこないはずなので、

非常に利用者の抵抗があるんじゃないかなということと、これは過剰反応ではなくて、ルート証明書を入れるというのは、本当に危険な行為であるため、これぐらいの意識は利用者の方が持ってくださるほうがむしろいいと思います。いろいろなそういった悪影響等も考えていくと、証明書を追加することが必要な手段は、少なくとも商用のＩＳＰではやらないほうがいいだろうというふうに思います。

（スライドp52）

実は、ほかにもう一つ方法がありまして、途中のＤＰＩが持っている、または、ＤＰＩ装置のための証明書というものをブラウザに最初に入れておいてくれとお願いする方法でございます。例えばブラウザの開発元に入れておいてくれとお願いすることは一応考えられます。これにブラウザの開発元が応じてくれるのであれば、対応可能なのですけれども、ただ、これは私の感覚で申しわけないのです、間違いなくこれは相手にされないだろうという気がしております。そもそもＴＬＳ、暗号化通信の目的自体が途中での介入を許さないためのものであるため、幾ら日本の社会で海賊版対策がこれだけ問題になっていて、正当な目的だと評価されていたとしても、やりたいことが途中での介入そのものである以上はなかなか無理なのではないかということと、それどころか日本がこういう働きかけをすること自体が世界の笑いものになってしまう可能性もございます。やはりこういったものというのは、国際的にいろいろな国がある中で、技術的な標準などが決まっているものなので、日本において例外が受け入れられるという話になってしまうならば、ほかの国が国家の安全を守りたいから同じようなことをやってくれと言われてしまうと、ブラウザのベンダーは断る理由がなくなってしまうと思うのです。ですので、こういったことはもう一律受け入れないということにおそらくなっていくだろうと思います。

（スライドp53）

大分駆け足で長くなってしまったのですが、まとめをしたいと思います。

（スライドp54）

技術的には、「ＤＮＳ＋Ｐｒｏｘｙ」を採用したとしても、ＤＰＩを採用したとしても、おそらくＨＴＴＰＳ、暗号化通信への対応が難しいことが一番の課題になってしまうのではないかなと思います。この暗号化通信そのものは、安全な通信を実現するためのものですから、電子商取引の基盤としても基本中の基本と言っていいと思います。ですので、今はこの暗号化通信を使った通信がほとんどを占めると言っていいぐらい増えてしまいまして、さらに申し上げると、この暗号化通信のエンドツーエンドの暗号化のやりたいことを

とことんまで実現するために、ＤＮＳの通信も暗号化しよう、電子署名をつけるようにしよう、そのほうが安全ですよね、という動きになっていますので、今度はブロッキングでさえも完全に塞がれてしまうと思うんですね。アクセス警告方式を実施するのにはやっぱりお金も労力もかかるとは思うんですけれども、今の段階でもう既に制御可能な通信というのが２割ぐらいしか残っていないということは、一応議論の前提として踏まえておいていただいてよろしいのではないかと思います。

（スライドp55）

最後のページになります。アクセス警告に限らず、根本的には技術的な流れというのが、エンドツーエンドの原則が徹底する方向で一貫しているのではないかと思います。ですから、どうしてもネットワークの途中で何かをしようとするということは、この流れと完全に逆方向であるということは間違いないです。もちろんネットワークの途中で通信を遮断しようとする、政府ですとか通信事業者というものも、世界を見渡せばないわけではないのですけれども、それをあざ笑うかのようにというふうに、もう口頭では言っていいのでしょうか、どんな通信でも通る方法というのが開発されてしまって、さらにそれが標準化されてしまうというのが、ネットの技術史、技術の歴史と言っても言い過ぎにはならないと思います。

最後に申し上げさせていただくと、やはりネット上での不正行為の対策というのは、通信の、どちらかのエンドで行っていただく、つまり、例えば発信者を検挙するとか逮捕するとか、コンテンツそのものをネットの世界から削除してしまうとかですね。または逆にフィルタリングのようなものを使って、各自がアクセスをしないように守っていくとか、そういったことを基本に考えていただくほうがよろしいかと思います。そのほうが結局は着実な成果が出せるのではないかというふうに思います。

大変長くなってしまいました。２４分５５秒ですか。これでＪＡＩＰＡの発表、ちょうど定刻で終わらせていただきます。ありがとうございます。

【濱田座長】　どうもありがとうございました。

これまで３つの資料について報告をいただきました。資料２－１から２－３ですが、これから、これらについてご意見、あるいはご質問等ありましたら、委員の皆様に出していただければと思います。ここからは議論の時間になりますので、よろしくお願いいたします。いかがでしょうか。

【森構成員】　では、お願いします。

【濱田座長】　はい、どうぞ。お願いします。

【森構成員】　ありがとうございました。このパブコメの提案募集の結果概要もアンケートも、今の野口さんのご説明も非常に勉強になりました。予想どおりだったというものは一つもなかったのですけれども、特にこの提案募集の結果概要は、ここまで皆さんに反対されるとは、というのが率直な印象です。賛成意見がなかったと言ってもいいと思います。前回の検討会でもかなり反対の意見が強かったので、そういう意味では、この検討会の方向性とは外れていないのですけれども、ここまで反対ということもあまりない。そういう意味では、じゃあ、あんまり話すことないですねということなのかもしれませんけど、そのようなことはなく、結構いろんな重要な示唆を含んでいたのではないかと思います。特に、ほかの海賊版対策との関係で非常にインパクトがあったのではないかと思います。

今回、提案募集に対する結果、パブコメのほうですけれども、論点として、割とこう一般的な論点設定をしていただいていた部分が、論点１とか論点２ですかね。今、提案募集の結果概要、資料２－１をベースにお話をしていますけども、こういったところで割と一般的な、海賊版対策としてどういうことを考えればいいのか意見をいただいております。論点１は、その共通認識という、これはどんな対策にでも関係することですけれども、論点２もあるべきネットワークの姿ということです。２３ページ以下のところですけれども。最後に、１５番目までの論点に含まれないその他の意見、全体的なご意見というのもまとめていただいていました。やはりこの中で非常に強く感じるのは、通信の秘密の侵害に対して強い懸念を示されているということです。これにしたがって、ブロッキングの場合は法律をつくってやりましょうということでしたし、このアクセス警告方式の場合は、包括同意でどうかということでしたけれども、いずれにしても、そんな簡単にできることじゃないんだよという指摘が多かったと思います。

私は一応、Ａ３の大きなほうもパラパラと拝見はしたのですけれども、やはりまとまっているところ以上にそういうご意見が強かったかなというふうに思いますので、それは今後の海賊版サイト対策全体について心がけるべきだろうと思いました。

野口さんの強調されていましたエンドツーエンドのことも、このパブコメの意見のところには随分あったかなというふうに思います。エンドツーエンド原則にのっとったものにすべきであるというご意見自体も多数あったかと思いますし、その他のところにも結構、やはり何を主軸に据えるべきかと、海賊版対策のメーンにすべきかというところで、そういうご意見が出ていたのかなというふうに思います。

今回、特にエンドツーエンドの中の、一方のエンドであるユーザ側のエンドについては、フィルタリングの提案をこの検討会としてはしているわけでございまして、資料２－１の１９ページ、２０ページのところにそのフィルタリングについてどうかということへの意見がありますけれども、それを見てみると、おおむね好意的な意見だったのではないかなというふうに思います。

ですので、全く野口さんのご指摘どおりですけれども、今後の海賊版サイト対策として、そのエンドの問題、その犯人の検挙であったりとかフィルタリングであったりとか、そういうことが強調されるべきだということはこの検討会の一つの成果ではないかと思います。

以上です。

【濱田座長】　ありがとうございます。

どうぞ。お願いします。

【田村構成員】　田村です。大変勉強になりました。パブコメにしてもアンケートにしても、質問が非常に多岐にわたり、しかも、核心にかかわるところを尋ねていただいたので、私も今、森先生と同じような意見を持ちました。野口さんのプレゼンテーションも、大変勉強になったことが多く、それでいてまた、本当はもっと難しい話なのかもしれませんけれども、わかりやすくお話いただきありがとうございます。

そこで、一つ質問がございます。先ほど森先生からもお話があったとおり、今回のアクセス警告方式をどのように扱うかということに関しては、他の対策との優劣みたいなものがどうしても必要になってくるということでした。そのため、今日は対象外ということで、極力お話しされていなかったようで、そして、スライドにおいても文書では記載されていらっしゃいませんが、二度ほどブロッキングについてのお話をされていて、そのときにブロッキングにはもう風前のともしびであるようなことをおっしゃっていました。

今日は、アクセス警告方式の話だったので、私の理解した範囲では、要するに、技術的には、偽サイトに誘導することと変わらないから、暗号化方式ではうまくいかないということであると思いました。他方、ブロッキングはそうではなく、遮断なので関係ないだろうと思っていたら、最後の例えば５４ページのところのまとめ（１）と書いてあるところで、口頭でしたけれども、いや、ブロッキングのほうももはやうまくいかなくなる。そういう予想をされておられたので、恐縮ですが、少しかいつまんで、何が問題かをお知らせいただければ大変助かります。

【日本インターネットプロバイダー協会（野口氏）】　ご質問をありがとうございます。

ブロッキングについて言いますと、２０１１年から児童ポルノに限定して行っているところですが、これはあくまでも、まだほとんどその当時は、暗号化されたサイトの割合が少なかったものなので、偽のサーバに接続して、そこで児童ポルノサイトへのアクセスは禁止ですよという表示をするという仕組みをとっていました。

そのときの議論の中では、ブロッキングされたということについては、きちんと説明責任といいますか、プロバイダとしてもきちんと説明すべきであるということがありまして、アクセスは禁止ですという画面を表示することができたのですけれども、一つは今、暗号化通信が行われているサイトだと、それはやっぱり偽サイトということになってしまうので、警告画面は表示されなくて、かわりにブラウザがエラーの画面を出して止まってしまう。その意味では、法的な意味でおそらくブロッキングの説明責任を果たせていないという問題が出てくるだろうと思います。

さらに申し上げると、では、とりあえずアクセスができなければ何でもいいじゃないかというようなお話もあるかもしれません。ＤＮＳを曲げることによって、一応はそのどん詰まりをつくることは可能です。ただ、最近ではそのＤＮＳがうそを回答するということについても、プロバイダが正規の目的でやっているなら、法的にはいいのかもしれないのですが、技術的にはこれもやはりＤＮＳの乗っ取りと解釈されてしまいますので、それを止める方法としては、ひとつは、ＤＮＳの通信そのものを暗号化しましょう、または、署名をつけて、例えばプロバイダがうその回答をしたとしても、ブラウザがやはりエラーにするようにする、そのどちらかの技術というのが今、普及し始めているところです。

また、そこまで率が高いとは言えませんけれども、こういったものというのが主要なブラウザなどに、もう導入されてしまったら、オンラインアップデートで勝手にどんどんそういったふうなものが標準化されてしまったらということも考えていくと、（ブロッキングは）決して長続きする技術ではないのではないかと思います。一応そういった意味で、この辺の、例えば５４ページの真ん中辺のＤＮＳ通信について、かいつまんで説明させていただきました。

【田村構成員】　どうもありがとうございます。そのようなブロッキングで単にエラーに出すような方策でももう通用しなくなるので、新たな方式が普及し始めている、ということですね。それが、今お話を伺うと、技術的に見ると、いろいろな意味で通信の秘密などを守るために、あるいは、さまざまな弊害を守るために、すぐれているものなので、これが今後普及する見込みがかなり高いだろうというのが野口さんの予測であると理解して

よろしいでしょうか。

【日本インターネットプロバイダー協会（野口氏）】　そうですね。特に、例えば銀行のウェブサイトが偽サイトにつながってしまうとなると、それはもう大変な話になってしまうので、やはり技術全般として、もうそういった脆弱なところをとにかく一個ずつでも塞いで、脆弱性をなくしていこうというのが流れでもありますし、私としては、それ自体はとてもいいことだと思います。でも、やはりそれに対応して、いくら目的が正当でも技術的には通らないことをやろうとしているのかな、というところは言えるのかなと思います。

【濱田座長】　はい。お願いします。

【江崎座長代理】　野口さんのところは多分とてもナイーブに、誘導先が海賊版サイトだとするとうそになるのですが、誘導されたところが誘導サイトだとすると、これはＨＴＴＰＳで通るので、そういう実装にすると違う話になってしまうため、そこは実装方法によって変わってくるというのを、正確には言っておかなければならないと思います。可能な実装方法もあるし、おっしゃったとおりの、要は、アクセスしたいところのサイトに対しての誘導されたところが大もとのＣＡを使う、サーティフィケーションを使うとすると、うそになりますけど、誘導された先は、誘導された先だということで、ＨＴＴＰＳを動かせば一応大丈夫ですから。

【日本インターネットプロバイダー協会（野口氏）】　すみません。それはホスト名が違うとエラーにならないですか。

【江崎座長代理】　ホスト名が違うところにリダイレクションするというのは可能ですから、実装上は可能なのです。

【日本インターネットプロバイダー協会（野口氏）】　はい・・・

【江崎座長代理】　はい。いずれにしても、手間がかかるし、そういうことが起こる。非常にＩＳＰでの手間がかかるというのはもう事実なので、正しいことをおっしゃっています。

それから、エンドツーエンドの原則に従って、これを進めていくということが、パブリックコメントの中でもたくさん出てきているということと、そのオペレーション上、実際の運用をしているところからしても、エンドツーエンドをある意味、バイオレーションするという運用はとてもコストがかかってしまうという、この２点はもう明らかに出てきているというふうに言えると思います。

それで、そうすると、エンドツーエンドが大事だよということをこれだけしっかりと議論したということで、もし結論が出ていくとすると、これはやはりグローバルにこのメッセージをしっかり出していかないといけない問題になってくると思います。つまり、我々は、通信の秘匿性と、全体のシステムのコストの問題、それから、守らなきゃいけないものという点を考えたときに、結論として、ブロッキングという手段が非常に厳しい実動サイトみたいなところを除くと、やっぱり守らなきゃいけないものだという結論が出たというのは非常に大きいところになってくるという点は、特に今グローバルで、やはり中間地点でのフィルタリング、ブロッキングというのが出てきているというのは重要な点でございます。しかも、ＤＰＩ、パケットの中身を見てフィルタリングするということがたくさん起こっているという事態に対して、我が国としては、ここでしっかりこの議論をしたというのが非常に大切なことになってくるのではないかと思います。

【濱田座長】　ありがとうございました。

どうぞ。お願いします。

【長田構成員】　今のお話は何かドンと来ました。とても大切なことだなと思いました。それなのにちょっと細かい話の質問となり恐縮なのですけれども、前回のときにもちょっと申し上げました点ですが、アクセス警告表示を出すのだとしたら、その行った先が違法なサイトであるというのは前提なのだろうと思っております。ダウンロードの違法化が検討されているということは、ダウンロードすることが違法だということですよね。

【森構成員】　そうです。それはそうしようと。

【長田構成員】　はい。そうしようというふうに動きがあるとすると、アクセスする段階では、ダウンロードをしようとしているのか、ただ閲覧しようとしているのか区別がつかないのかなと思っております。アクセスをしようとしている人の意思はわからないのではないのでしょうか。素人考えですが、機械的にそんなものがわかるなんていうことは多分ないのかなと思うので。結果的にダウンロードすることが違法という場合にこのアクセス警告を出すことというのがまず大きな問題があるのかなというふうに思いましたので、そこを確認させていただければと思います。加えて、ダウンロード違法化の検討のときに、非常に私が思っているよりもすごく幅広くご意見が出てきて、結局それが問題になって、立法化されなかったと思っているのですけれども、もし違法化になって、アイコンとかにアニメの絵がついているとかそういうものも違法化の対象とするとなった場合に、何もかもがもう、すごくいっぱいアクセス警告表示まみれになる可能性もあるのではないかと思

っており、その辺との関係もやはり、ダウンロードに限らず、何を違法とするかというところが明確になっていなければならないと思います。まず、アクセス帰国方式が、非常に問題があるということと、そして、今、お話を伺ったように、アクセス警告方式そのものに非常にまた大きな課題があるということもわかりましたので、ご提案いただいたようにやっぱりエンドツーエンドのところで対応するということをきちんとやっていくべきことだなとますます思いました。

以上です。

【濱田座長】　ありがとうございます。今の点は野口さんにお伺いしてもいいですかね。

【日本インターネットプロバイダー協会（野口氏）】　はい。そうですね。アクセスの段階でダウンロードトラヒックなのかどうか区別がつかないという点については、おそらくそうだと思います。ＵＲＬ単位で、例えば画像ファイルを単独でフィルタリングすることができればいいと思いますし、ＤＰＩ方式でも暗号が一旦ほどければできるとは思いますけど、ただの閲覧であり、保存しない限りはおそらくダウンロード違法化での対象にならないという話になってくると、それがダウンロードなのか、ブラウザに表示しようとしているのかという区別は全くできないはずです。

【濱田座長】　お願いします。

【田村構成員】　もうおっしゃるとおりだと思います。アクセスしているだけなのか、ダウンロードまでするのかわからない段階で警告を出しますから、おっしゃるとおりで、今の二つのご指摘が妥当すると思います。

ただ、少し補足をしたいと思います。まずは、今回の導入の正当化根拠としてユーザの法的責任を回避するためにという理由をつけたら、非常に正当化が増すのではないかという点です。

今回のアンケート結果を見ると、アクセスしているだけなのか、ダウンロードまでするのかという点は、法的な整理はともかくとして、一般の方の意識に対してはあまり影響がない。そうすると、むしろ主たる理由は、ご本人の不利益を免れさせるというよりは、やはり権利者の方の利益を守るために実効的なものを入れるべきだということで押すしかないのだと思います。そうなってくると、ダウンロードはせず、アクセスする場合も、公衆送信を誘発しますので、ユーザご本人が違法にならないにしても、法的な責任は発生しないにしても、違法行為を助長することではありますので、その意味では全く理由がない措置ではないということが１点目についてです。

それから、２点目のダウンロード違法化の議論のときに大問題になったこともおっしゃられたとおりですが、これはむしろ、こういう警告方式を、どのようなサイトに出すのか。そういう話だと思います。ダウンロード違法化の場合は、エンドでやって、しかも、どのようなサイトから出てきたかと無関係に、そして、どんな目的でダウンロードするか無関係に、かなり広く抑えようとしたのが大きな問題だったのですけれども、もしこの警告方式をとった上で、非常に海賊版サイトに限って、こういう警告を出すような仕組みが担保されるのであれば、ダウンロード違法化の議論のときに反対した人も、そのときの懸念が大分取り除かれ、全員ではないにしても、大多数が賛成する可能性があるとは思います。

他方、今日のお話により、そのこととは全く別のより大きな問題を、いただいたような気もいたします。

【濱田座長】　ありがとうございます。

ほかにいかがでしょうか。はい、どうぞ。

【長田構成員】　ありがとうございました。おっしゃるとおりなのかもしれませんけれども、やはり何よりも、私どもがどこへアクセスしようとしているのかをチェックされるというところが一番大きな問題だとは思っていますので、やはりこの方式は取り入れられるべきではないですし、これがだめだからといって、じゃあ、ブロッキングを実施するといった議論がまた政府で起こるのは非常にもう大問題だなと思っていて、蛇足ですけれども、それは反対したいなと思っています。

【濱田座長】　はい。ありがとうございます。

いかがでしょうか。はい。

【森構成員】　ありがとうございます。すみません。今お話を伺いながら、なるほど、と思って聞いていたのですけれども、確かにダウンロード違法化が行われるかどうかということについて、今回のアクセス警告方式は、本当は個別の同意が必要ですが、包括同意で実施できないかということなので、通常であれば、ユーザが同意するような事柄であるということが成立していなければできなかったわけですけれども、それが今回の受容性調査で、６ページから、７、８、９にあるように、全く違法化されようが、されなかろうが、変わらないという点は、私としても想定外でした。

やはりここでの「通常のユーザであれば想定できるであろうこと」と言うためには、それはあまり規範的にこう、法律が勝手に考えていいということではなくて、もちろんそういう理屈が立つということも一方では必要だと思いますけれども、他方で、やはり受容性

調査をやってみて、通常であれば同意するという数字が出ていないとだめだろうと思うのですけれども、これを見ますと、結局、同意する、許容できるという人のほうが過半数より少ないというわけですから、やはりそういう意味ではなかなかといいますか、基本的には難しいのかなということかなと思います。

ちなみに、もう一つ、私も想定外でしたし、皆さんももしかしたら想定外だったかもしれないなと思うのは、この１０ページ、１１ページですね。この受容性調査のですね。これは現行法と、ダウンロードの違法化の後と両方、全然変わらないのですけれども、この棒グラフの下の３分の１ですね。これは海賊版サイトアクセス経験別でクロス集計をしているのですけれども、海賊版サイトアクセス経験のうち、頻繁にアクセスのところだけ、この「断じて許容できない」が４５．５％になっていますので、意外にもこの効果があるというか、もしかしたら後ろめたいと思ってやっているので、非常にこのアクセス警告方式を導入されると、それは頻繁に使っている人は嫌なのだろうという、そういうことも私としてはちょっと意外でした。

以上です。

【濱田座長】　はい。お願いします。

【江崎座長代理】　この調査は、森先生がおっしゃったとおり、我々にとっては驚きの部分もあるし、アクセス方式に関してはちょっと警戒だということだと思いますけども、これはやはり、ひとつの組織が調査したデータであって、これがひとり歩きするのはちょっと怖いかなという気がしています。科学的には複数の調査でやるということがとても重要かなと思います。そのためには、これがどういう調査の方法でやったかというのをできるだけ正確に出してくださいということは言ったわけですけれども、それは恣意性がない、それから、客観性があるということを考えた場合には、できればもうひとつか、ほかのところで同じような調査をするということが、この調査結果の客観性と信憑性を担保するという意味においては、非常に科学的には重要ではないかなと思います。多分同じ結果が出るのではないかなと思いますけれども、それはよりこの結果を正当化する、客観化するために、もしできればそれがいいのではないかなというふうに思います。

【濱田座長】　ありがとうございます。

はい。お願いします。

【森構成員】　江崎先生、もう一度別の角度からというお話でしたけども、ただ、念のために申し上げておきたいのは、このポイントになるのは７ページと９ページですよね。

アクセス警告方式の受容性についてのところですけれども、この（ｎ＝２，０００）でやっていて、現行法想定で、「許容できる／気にならない」が４４．７％。違法なダウンロード想定で、「許容できる／気にならない」が４６．８％なので、これは８割ぐらいまで来ないと多分無理だと思いますので、多少これがやり方を変えたら５割５分ぐらいになりましたとか、６割になりましたと変化した場合でも、やはりきついとは思っています。そういう意味では、果たしてもう１回やって、その結果、もう少し慎重にということになるのかなという感じはちょっとします。

【濱田座長】　はい。お願いします。

【江崎座長代理】　ちゃんとしたことはやってらっしゃると思うので多分大丈夫だとは思うのですけれども、やはり一応科学者としては検証可能であるということ、それが複数の人からちゃんとチェックできるようにしておくということを、調査側が「大丈夫です。もうこの方法でやりましたので、客観的ですよ」と言っていただけるだけのものが欲しいなと思うところです。というのは、実はこれは内閣府の中でも、データのとり方がはっきりわからないと、実態がわからないというところでデータがひとり歩きしたという例を認識しているところで、これは大学の学生に聞いたときも、ちゃんと複数のソースで検証できるようにデータ収集をやらないとまずいですよねと言うわけです。特に大きな方針を決めるようなときに数字が非常に恣意的に出てくる場合というのは往々にしてあるわけですから、多分大丈夫だと思いますけども、そこだけが少し、できればそれがあると非常に、よりこのデータに基づいた議論をしっかりとできるのではないかなという意味での話です。

【森構成員】　なるほど。ありがとうございます。もともと海賊版サイト対策は、４２カ国でブロッキングを導入済みとか、３，０００億円とか、非常に適当な数字で検討されてきたという、悪しき伝統がありますので、それを破って、今回からきちっとやると、そういう意味でもまさにご趣旨はごもっともだと思います。冒頭にこういう、論点を提示して、パブコメをされている段階でも、そしてまた、受容性調査をされている段階でもきちんとされていると思いますけど、趣旨には賛成です。

すみません。１点お聞きしてもよろしいでしょうか。さっきの江崎先生がおっしゃっていた、ドメインをリダイレクトすれば実装できる場面があるのだというお話についてですけれども、さっきの野口さんのスライドについて、非常に私は納得して、証明書のところなど見ていたのですが、どの辺が実際にはエラーにならずにできるということなのでしょうか。

【江崎座長代理】　これは、要は、リダイレクトして次にアクセスさせるところが、いわゆるＤＮＳで教えられているＤＮＳのところであるというふうにすると、当然ながら、そこでエンドツーエンドできなくなっちゃうわけですけども、技術的には、ここにアクセス行ったときに、こちらにリダイレクトしますという方法は上手にすればできるので、そうすると、そのリダイレクトされたサイトは大もとのところではないというふうには、できないことはないですよね。少し複雑ですけども。

【森構成員】　でも、リダイレクト、結局、警告画面をまず表示するというのは案としてもあって、その後で、「はい」を押せば、本来のウェブサイトも見せてあげなきゃいけないわけですけれども、それもできるということですか。

【江崎座長代理】　それだともう一回、リダイレクトする、大もとのところに返してあげるということをすると、できないことはないですね。手間はかかりますけど。

【濱田座長】　今の点はあれですね。場合によっては、江崎先生にまた説明をいただくのがいいかもしれません。

ほかにいかがでしょうか。まだ時間はございますので、この機会に何かございましたら。

オブザーバーの皆様から何かコメント等ございますか。よろしければ。特によろしいですか。大体皆様よく調査結果を消化されたということでよろしいですかね。

今日は特にこれ以上の議題は予定しておりませんので、何かございましたらこの機会に、この時間にと思いますが。はい。

【森構成員】　ありがとうございます。今度はちょっと海賊版対策から外れてしまうのですけれども、結構私もひっかかったのは、このパブコメの資料２－１の１１ページの包括同意のところでして、これはどちらかというと、海賊版対策に限らず、通信の秘密を制同意で制限する場合の一般の考え方として、この１１ページの「主な提出意見」の２番目のカテゴリーですが「ユーザが約款に気づかず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」ということで、「通常の利用者であれば承諾するという想定が困難」というのは、受容性調査のほうでも明らかになったわけですけれども、前半の意味を正しく理解せず同意することになるというところは、ちょっとこれは固有の注意が今後は必要だなと思っていまして、最初のご意見だと、下線部分ですが、「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不適切とか、２ポツですけれども、通信の秘密の侵害に対して、「通常の利用者であれば承諾することが想定される場合」を想定することはそも

そも困難。それから、その下ですが、「個別具体的かつ明確」な同意ではなく、「約款等による包括的な同意」で済ませることは通信の秘密の侵害のおそれが極めて高いということですので、意識はされていた問題点ではありますけれども、包括同意化する、個別同意を包括同意に下げることについての警戒心というものも非常に強いのだなということもわかりましたので、これは今後のほかの場面でも意識していくべきことなのかなというふうに思いました。

【濱田座長】　ありがとうございます。

それぞれの資料、なかなか味わいがあるものですが、何かさらにコメント、ご質問等ございましたら。よろしいですか。はい。

それでは、まだ若干時間の余裕はありますけれども、このあたりで今日の討議は終了させていただければと思います。

最後に、事務局のほうから連絡事項ございましたら。

【中川消費者行政第二課課長補佐】　次回会合については、また事務局から別途ご案内させていただきます。

事務局からは特にございません。

【濱田座長】　それでは、これで本日の議事は全て終了いたしました。検討会の第２回会合、終了させていただきます。お忙しい中、ご出席いただいてありがとうございました。

また、野口さん、報告いただいてありがとうございます。

【日本インターネットプロバイダー協会（野口氏）】　ありがとうございました。