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３回）

令和元年６月２０日

【濱田座長】　おはようございます。今日は皆様、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の第３回会合を開催させていただきます。

本日は、田村構成員が欠席、江崎座長代理の到着が少しおくれると伺っております。

また、本日は、トレンドマイクロ社の櫻井様にお越しいただいております。よろしくお願いいたします。

冒頭、カメラ撮りがございますので、少々お待ちください。

【中川消費者行政第二課課長補佐】　それでは会議冒頭、カメラ撮りの報道関係者が退出いたしますので、しばらくお待ちください。

（報道関係者退出）

【濱田座長】　トレンドマイクロ社は櫻井様と申し上げましたが、木野様ですね。失礼しました。よろしくお願いします。

それでは、まず、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】　それでは、配付資料について確認をさせていただきます。本体資料は、資料３－１と３－２。さらに、参考資料３－１となっております。なお、資料３－１につきましては、傍聴の方にお配りしている資料に一部マスキングがございますので、ご留意ください。

また、今回、席上にタブレット端末を置かせていただいておりまして、これは第１回目及び第２回目の過去の資料を電子で格納しているものでございます。もしパスワード等がかかっていたり、使い方がわからなかったりする場合には、挙手をいただきますと事務局の者がそばに参りますので、よろしくお願いいたします。また、過不足等ございましたら、同様にお申しつけください。

【濱田座長】　資料、タブレットはよろしいでしょうか。

それでは、議事に入りたいと思います。最初にトレンドマイクロ社の木野様からフィルタリングの取組についてご発表いただくことになっております。

木野様、よろしくお願いいたします。

【トレンドマイクロ（木野氏）】　皆様初めまして。トレンドマイクロの木野と申します。よろしくお願いいたします。本日、このような機会をいただきまして、まことにありがとうございます。私どもはトレンドマイクロと申しまして、一般のお客様向けですとか、あとは法人様向けのセキュリティソフトを開発、販売している会社になっております。私は一般のお客様向けのセキュリティソフトのプロダクトマネージャーを担当しております木野と申します。

では、私から、お配りしております資料「コンシューマー向けエンドポイントセキュリティ製品でのフィルタリングの取組」につきまして、我々でどういった取組をやっているのかというところをご紹介させていただければと思います。

ページをめくっていただきまして、本日、３点ご説明させていただければと思います。まず、１点目は国内の一般のユーザ様のセキュリティ対策のソフトの利用状況をまとめたものがございますので、こちらのご紹介と、２点目に、我々の「ウイルスバスター」という製品について、どのような対策を行っているのかということのご紹介になります。

３点目が、我々で感じている課題ということで、ご説明をさせていただきます。

では、４ページ目になりますけれども、まず、「エンドポイントセキュリティ製品の利用状況」ということで、大きくパソコン系とモバイル端末、アンドロイドですとか、ｉＯＳということで分けて記載をさせていただいております。こちらの調査結果は、我々が独自で、外部の調査機関を通じてインターネット調査を今年の４月に実施したものになっております。

まず、４ページ、パソコン向けになりますけれども、我々のシェアが二十数％ということで、その他、他社のベンダーさんも含めて、有償のセキュリティソフトを使われているお客様が６８．１％という形になっております。無償のセキュリティソフトのほうは、最近ですと Windows１０には Windows Defender ウイルス対策という製品が標準で搭載されていることもございますので、こちらを含めたもので１９．８％という形になります。こちらは、お客様がご自身で認識されていらっしゃる回答を基にしたものになりますけれども、セキュリティソフトを利用していないというお客様が１２．２％いらっしゃるといった結果になっております。この調査の中では、利用状況が「わかりません」と回答された方は除いたものになっております。

続きまして、次の５ページ目になります。こちらがモバイル、アンドロイドとｉＯＳでのセキュリティソフトの利用状況になります。まず、見ていただきますと、利用されてい

ないお客様が４４．０％ということで、パソコン向けに比べますとまだまだ対策ソフトを利用されていないお客様が多い状況になっております。有償のセキュリティソフトが３６．８％、我々が１０％強のシェアになっております。無償のセキュリティソフトもアンドロイドになるかと思うのですけれども、かなり利用されている状況でして、全体の１９．２％になっております。こちらまでがエンドポイントセキュリティ製品の利用状況になります。

続きまして、２点目、「トレンドマイクロが提供しているフィルタリングサービス」になります。ページをめくっていただきまして、７ページ目になりますけれども、我々で提供しております、ウェブサイトにアクセスしようとした場合に当該アクセスをブロックする機能としましては、大きく２つございます。１点目がＷｅｂ脅威対策機能というものになっておりまして、２点目がペアレンタルコントロールの中に含まれますＵＲＬフィルタリングという形になります。どちらも我々のクラウドに巨大なデータベースのようなものがございまして、お客様がアクセスをしようとしたときに、そのＵＲＬがどういう性質のものなのかということを問い合わせした結果を受けて、セキュリティソフトでブロックする、しないといった形で機能を提供しております。

こちらの２つの機能の違いを８ページに書かせていただいております。Ｗｅｂ脅威対策になりますけれども、こちらはもともとマルウェア対策のソフトでございまして、主にウイルスの感染、不正プログラムが隠されていて、例えば、脆弱性が放置されたままのパソコンをお使いのお客様がブラウザでそのサイトにアクセスした場合には、何かクリックをしたりとかしない場合でも、ウイルスに感染してしまう。例えば、ランサムウェアがそのサイトにアクセスしただけでパソコンに感染してくるといったこともございますので、こういった不正プログラムが隠されているページですとか、あとは正規のページを改ざんして情報を盗み取るフィッシング詐欺のような、ネットバンキングのサイトに見せかけて、そこに情報を入力するとその情報が盗まれてしまうといったセキュリティ対策上の危険なサイトをブロックするという機能になっておりまして、こちらは初期設定がオンになっているウイルスバスターをインストールしていただきますと、こちらのサイトについては自動的にブロックされるという形になります。

もう一点、ＵＲＬフィルタリングにつきまして、こちらはペアレンタルコントロールの機能になっておりますけれども、管理者のご両親が利用者であるお子様がパソコンですとか、スマートフォンを使われる場合に、この機能を有効にしていただきますと、見せたく

ないページをブロックするといった機能になっております。こちらは利用用途によって変わってきますので、初期設定はオフになっておりまして、お客様が任意で設定していただける形になっております。

現状、海賊版サイトのブロックにつきましては、このＵＲＬフィルタリングの中のカテゴリの１つという形で位置づけて、いろいろな団体様から提供いただいたＵＲＬをこのカテゴリの中に追加させていただきまして、お客様が設定していただいた場合にブロックができる形になっております。

その次のページからフィルタリングの設定方法、主にこちらはＵＲＬフィルタリングの設定方法について記載をさせていただいております。

まず、９ページがWindows版になります。メーン画面から設定をしていただいて、この中でフィルタリングを行うカテゴリをお客様に選択していただくものですが、その中に「違法と思われる行為」というカテゴリがございまして、こちらに海賊版サイトと思われるＵＲＬを我々で追加させていただきまして、こちらをブロックするという設定をした場合に、ブロック画面が表示されます。

実際のブロック画面につきましては、次の１０ページ目になります。この機能はＨＴＴＰＳにも対応しておりまして、ブロックの方法が異なるということで、ＨＴＴＰの場合には、ブラウザの画面上でこういったブロック画面を表示する形になります。

一方で、ＨＴＴＰＳの場合には、ウイルスバスターからポップアップの画面を表示してきます。ブラウザ上の画面は空白になった形で表示されます。主に小学生から高校生ぐらいのお子様向けのブロック画面ということで、振り仮名を振っていたり、なるべく漢字を使わないようにしたり、こういった工夫を施した形でユーザーインターフェースを表示しております。

こちらはＰＣになりまして、記載はないのですが、Windows のほかにＭａｃにも対応しております。

続きまして、１１ページになります。こちらはモバイルになります。モバイルはｉＯＳ、アンドロイド両方とも対応しております。少し画面のデザインが違ったり、名称が違ったりする部分がございますけれども、例えば、ｉＯＳでいきますと、「コンテンツシールド」という機能がございまして、これはローカルのＶＰＮという機能を使って、端末が通信をする際に通信の内容を見てブロックしていく形になっております。ですので、例えば、ｉＯＳ上で Safari を使っているお客様ですとか、Facebook 内のブラウザを使っている場合

にもこの機能でブロックすることができます。

同様にアンドロイドでは保護者による使用制限ということで、こちらでＵＲＬフィルタを有効にしていただくことができる形になっております。

モバイルのブロック画面につきましては、次の１２ページに記載させていただいています。

続きまして１３ページ、「フィルタリング機能を強化する取組」ということで、どのサイトが海賊版のサイトであるのかを判定することは、我々はセキュリティ対策の会社ですので、難しいことがございまして、知的財産を保護されている団体からリストをご提供いただいて、我々のクラウド上にあるデータベースに反映させる。これによって先ほどの違法とも思われる行為のカテゴリに登録をさせていただいてブロックをするといった仕組みになっております。

最後のパートになります。私どもで考えております現状の課題ということで、２点ほど１５ページに挙げさせていただいております。

１点目が、違法と思われる行為に関するウェブサイトのリストの強化ということで、我々でそういったリストを強化していくことが難しい部分がございますので、例えば、法的な機関ですとか、もしくはそれに準ずるような団体様から不正なＵＲＬをご提供いただき、先ほどのような形でクラウド上のデータベースに反映させることによって強化することが可能かと考えております。

あと、ペアレンタルコントロールの利用率の部分です。お客様が任意で設定していただく機能になっておりますので、こちらをより利用していただくために、もう既にいろいろな施策を実施していただいているかとは思うのですけれども、特に青少年を対象として、インターネットですとか、スマートフォンを利用した際のリスク等、その対策の啓蒙を継続していくことで利用率向上につながり、ひいてはこういったお客様のメリットにつながっていくのかと考えております。

私からの説明としましては、以上となります。

【濱田座長】　どうもありがとうございました。

それでは、ただいまのご発表に関しまして、ご意見、ご質問等ございましたら、いただければと思います。お願いします。

【上沼構成員】　ありがとうございました。２点ほど質問があります。まず、１つ目は９ページで、チェックがあるということはフィルタリングを行うカテゴリは自分で選ばな

くてはいけないということだと思うのですけれども、このときにおすすめセットみたいなものはあるのですか。それとも、保護者が自分でプチプチとチェックを入れていかなくてはいけないのですか。

【トレンドマイクロ（木野氏）】　こちらの設定ですけれども、画面の上に「フィルタレベルの選択」というのがございまして、「高・中・低」という形で設定ができるようになっております。こちらを選んでいただきますと、それに合わせた形で幾つか標準で設定がされます。そのフィルタレベルを選択していただいた上で、さらにこのサイトはご家庭ではブロックしたいという場合には、個別にそのカテゴリをセットしていただくことで、そちらもブロックしていただくことができるようになっております。

【上沼構成員】　ありがとうございます。ちなみに「低」でも、違法サイトは対象になりますか。

【トレンドマイクロ（木野氏）】　はい。こちらはすべてのフィルタレベルでブロックされる形になっております。

【上沼構成員】　ありがとうございます。

もう一つ、１０ページですけれども、「このウェブサイトにアクセスする必要がありますか」とか、「今だけ見られるようにする」、「これから見られるようにする」という選択があるということは、フィルタリングを設定していても、ユーザが選べば、アクセス制限の対象サイトを閲覧できるということでしょうか。

【トレンドマイクロ（木野氏）】　そうですね。こちらは、ペアレンタルコントロールの機能の一環になっておりまして、もしこのサイトを見たい、もしくは、これから見られるようにしたいというように設定を変更したい場合には、パスワードを入力していただく画面が出てきまして、保護者の方にパスワードを入力していただきまして、その設定を変更していただく形になっております。

【上沼構成員】　平仮名で書いてあるのは子供向けという趣旨かと思うのですが、これを選んでも、結局保護者のパスワードを入れないと先に進めないということですか。

【トレンドマイクロ（木野氏）】　そうですね。

【上沼構成員】　ありがとうございます。そのときに、例えば、警告画面みたいなものは特に出ないのですか。要するに、例えば、「違法と思われるサイトです」ということで、「それでも見たいですか」と。

【トレンドマイクロ（木野氏）】　そうですね。こちらに表示している警告画面以外の

もので何か追加というものは特にない状況になっています。

【上沼構成員】　ありがとうございます。

【濱田座長】　ほかに。お願いします。

【森構成員】　ご説明ありがとうございました。私も２点ほど教えていただきたいのですが、１つ目は８ページです。この海賊版サイトは、ＵＲＬフィルタリングによるブロックでの対処となり、これはユーザ側でオンにするということだったと思うのですけれども、この左側（Ｗｅｂ脅威対策）に海賊版サイトが入っていたりすることはないのでしょうか。それはたまたまその海賊版サイトがセキュリティ上の問題もあるという場合だと思うのですけれども、それが１点です。

もう一つは、ローカルＶＰＮというのがよくわかりませんでした。例えば、ＨＴＴＰとＨＴＴＰＳで画面が変わるとか、アプリでやるのだったら同じなのではないかと思うのですが、その２点について教えていただければと思います。よろしくお願いします。

【トレンドマイクロ（木野氏）】　まず、１点目ですが、Ｗｅｂ脅威対策機能の８ページで、海賊版のサイトがブロックされることはないのかという点につきましては、ブロックされる可能性がございます。と言いますのも、海賊版サイトの中にはそのページにアクセスしたときにウイルスに感染するような攻撃を仕込んでいる場合がございますので、そういった条件に該当した場合には、このＷｅｂ脅威対策機能によってブロックされる場合があります。

２点目のモバイルの利用で、先ほどローカルＶＰＮという形でご説明させていただいたのですけれども、機能としましてはいろいろなアプリでインターネットにアクセスしまして、ブラウザを利用された場合、アプリ内のブラウザ等でアクセスした場合ですとか、ＯＳ標準の Safari のブラウザでアクセスした場合にも、ブロックができる機能とご理解をいただければと思います。

【濱田座長】　よろしいですか。ほかにいかがでしょうか。どうぞ。

【長田構成員】　先ほどの上沼先生のご質問の続きのようになるのですけれども、ＰＣの場合は「今だけ見られるようにする」みたいなことが表示されますが、モバイル、１２ページには、この画面上はそれがないように思うのです。差をつけていらっしゃる理由を教えていただければと思います。

【トレンドマイクロ（木野氏）】　そうですね。各ＯＳ向けの製品によって仕様の違いがあるところが大きな部分になっていますのと、パソコンの場合には、親子共用で使われ

ているケースが多かったりするかと思うのですけれども、お子様向けの場合には、例えば、スマートフォンをお子さん自身が持っていて、そこで承認をするような作業をさせるというのが難しいところで、現状はこういった違いがある形になっております。

【長田構成員】　ありがとうございました。パソコンも、保護者は自分で見たい場合は、自分でログインすれば制限がかからないとか、多分、選べるのだと思うので、むしろ、こういう「今だけ見られるようにする」みたいなものが不要なのではないかと思いました。

【トレンドマイクロ（木野氏）】　なるほど。ありがとうございます。

【濱田座長】　どうぞ。

【出版広報センター（伊東氏）】　３つ質問があります。まず、１つ目ですけれども、今、保護者が海賊版サイトを見られなくなるようにという話が出ていたと思うのですが、特にモバイルの場合に関して、保護者においては、このトレンドマイクロ社の製品がどのように働くと考えればいいのでしょうか。

【トレンドマイクロ（木野氏）】　モバイルで保護者の方が海賊版サイトにアクセスしようとした場合ですね。現状、保護者の方がウイルスバスターをモバイルに入れていただいて利用した場合には、Ｗｅｂ脅威対策機能の機能だけしか有効になっていない形になりますので、先ほどありましたウイルスを感染させるような攻撃が仕込まれていない場合には、特にブロックはしない形になります。

【出版広報センター（伊東氏）】　なるほど。わかりました。

続いての質問ですけれども、これは他社さんの話にもなってしまうのですが、有償、無償含めて、他社さんの製品にもＵＲＬフィルタリング機能は大体が実装されていると思ってよろしいでしょうか。

【トレンドマイクロ（木野氏）】　そうですね。ベンダーさんによるところもありまして、我々ではセキュリティ対策のソフトにこの機能を一緒に入れてしまっているのですが、他社さんの場合ですと別のアプリで提供されていらっしゃるケースもございます。ですので、セキュリティ対策のソフトとは別のアプリを別途インストールしていただいて、そちらで設定をしていただくというケースもございます。

【出版広報センター（伊東氏）】　あと、御社の中で調査されているかどうかわからないのですけれども、このＵＲＬフィルタリングをオンにしている割合は何％ぐらいと把握されていますか。

【トレンドマイクロ（木野氏）】　全体の数としてはあまり多くないような形になって

おりまして……。

【出版広報センター（伊東氏）】　あまりというのは５０％なのか、３０％なのか、２０％なのか。

【トレンドマイクロ（木野氏）】　もう１０％に満たないような……。

【出版広報センター（伊東氏）】　１０％に満たない。

【トレンドマイクロ（木野氏）】　もっと低い感じです。モバイルについては、我々はデータがないのですけれども、ＰＣで言いますと、非常に低い形になっております。

【出版広報センター（伊東氏）】　モバイルのほうが高いという可能性もありますか。

【トレンドマイクロ（木野氏）】　可能性としては、そうですね……データが取れていないので何とも申し上げられないです。

【出版広報センター（伊東氏）】　わかりました。ありがとうございます。

【濱田座長】　はい、お願いします。

【曽我部構成員】　曽我部です。ご説明、どうもありがとうございました。９ページの右側、先ほど出たカテゴリの選択のところの、この赤く囲んである「違法と思われる行為」というカテゴリに海賊版サイトが入っているということですけれども、違法と思われる行為というのは、海賊版以外にもあるのでしょうか、また、フィルタリング対象となる海賊版サイトというのは、どういったものになっているのでしょうか。つまり漫画村みたいに、大体的な、もっぱら著作権侵害コンテンツがあるようなものに限っているのか、もう少し幅広に含まれているのかというあたりをお伺いしたいと思います。

【トレンドマイクロ（木野氏）】　かしこまりました。こちらのカテゴリに追加しているものにつきましては、１３ページにございますフィルタリング機能を強化する取組と書かせていただいている知的財産を保護する団体からいただいたリストを追加する形で、リストを強化しているものになりまして、何か我々で独自に基準をもって拡張しているということはございません。ですので、海賊版のサイトに該当するものだけがこちらに入っていると理解しております。

【曽我部構成員】　「知的財産を保護する団体」というように、一般的な書き方で記載されています、これは著作権に限るということでしょうか。

【トレンドマイクロ（木野氏）】　そうですね。具体的に申し上げますと、Ｂ－ＣＡＳ様ですとか、ＣＯＤＡ様等が含まれます。

【曽我部構成員】　どういう基準でリストをつくるかというのは、その先方の団体に委

ねているということですかね。

【トレンドマイクロ（木野氏）】　そうですね。

【曽我部構成員】　この知的財産を侵害するコンテンツのフィルタリング対象とするというのが、この違法と思われる行為の中身であるという認識でよろしいでしょうか。

【トレンドマイクロ（木野氏）】　はい。

【曽我部構成員】　ありがとうございました。

【濱田座長】　では、漫画協会さん。

【日本漫画家協会（赤松氏）】　その団体からのリスト提供の更新頻度はどれぐらいですか。毎週とか。ここ最近、先週から今週にかけて、漫画村の新しいバージョンが結構猛威を振るっているのですけれども、そういうのが入っているかどうかは承知していないですよね。

【トレンドマイクロ（木野氏）】　そうですね。

【日本漫画家協会（赤松氏）】　もしかして月１とかですか。

【トレンドマイクロ（木野氏）】　はい。直近で更新をしたのは３月になっていまして、それほど頻度を高くアップデートしているというわけではない形になります。

【日本漫画家協会（赤松氏）】　わかりました。

【トレンドマイクロ（木野氏）】　どちらかと言いますと、我々にリストを提供していただいた場合に追加するという形で対応させていただいております。

【日本漫画家協会（赤松氏）】　ありがとうございます。

【濱田座長】　はい。

【長田構成員】　今、これはペアレンタルコントロールのところでこういう仕組みができている。これを大人向けにもどんどん推奨していけばいいのではないかと思うのですが、そういうお考えはいかがでしょうか。

【トレンドマイクロ（木野氏）】　我々の提供している製品自体が、セキュリティ対策用ソフトということで、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何か被害を被ったりするといったような場合に対処するという位置づけの製品と考えておりまして、その中の一機能として保護者による使用制限を提供しているのですけれども、例えば、違法なコンテンツを標準でブロックしていくようなものというのが、セキュリティ対策ソフトの位置づけとしてほんとうに求められるものなのかどうかというところで、少し議論が社内でも必要なのではないかと考えております。

【濱田座長】　お願いします。

【森構成員】　先ほど更新頻度のお話があったのですけれども、１３ページの件ですが、これは最初にリストをもらい始めたときと言いますか、いつごろから海賊版がリストに入るようになったのでしょうか。

【トレンドマイクロ（木野氏）】　今、情報を持ち合わせていないので、改めてお答えさせていただければと思います。

【森構成員】　わかりました。ありがとうございます。よろしくお願いいたします。

【濱田座長】　どうぞ。

【日本インターネットプロバイダー協会（野口氏）】　オブザーバーなのに申しわけありません。１０ページと１２ページのことでお尋ねしたいのですけれども、ＰＣではＨＴＴＰＳの場合にポップアップ画面、つまりブラウザの画面ではなくてアプリのポップアップになるということと、１２ページでは、ｉＯＳについては、ブラウザにはページは空白になって通知だけが出てくるという、同じようなことだと思うのですが、これはブラウザ側で証明書の検証ができないからという、技術的な制約に基づくものなのか、教えていただければと思います。

【トレンドマイクロ（木野氏）】　こちらは技術的な制約に基づくものになっております。

【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す。証明書の問題ですかね。

【トレンドマイクロ（木野氏）】　こちらは確認させていただいても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）】　ありがとうございます。

【濱田座長】　ほかにいかがでしょうか。

【デジタルコミック協議会（村瀬氏）】　質問ではなく補足ではあるのですけれども、最初の森先生、赤松さんからのご質問と関連するのですが、こちらの出版広報センターや漫画家協会さんとの協力も得て、ここ２カ月ほど海賊版サイトの情報に関しての集約を行っています。大体こちらの伊東さんがいろいろ確認されておられるのですけれども、それを見ると、集まってくる情報の３分の１ぐらいが、実はフィッシングサイトの形を取っていたり、マルウェアを配布したりということで、そのようなものが海賊版サイトの中に多いということ。それと、今、赤松さんがおっしゃった、第２の漫画村じゃないかと言われ

るサイトに関しては、マルウェアの配布が確認されていて、トレンドマイクロさんのウイルスバスターが入っているＰＣでアクセスすると、普通にブロックされます。

以上、補足です。

【濱田座長】　ありがとうございます。ほかにはよろしいでしょうか。

それでは、トレンドマイクロさんのご報告についてのご質問はここまでとさせていただきます。ありがとうございました。

【トレンドマイクロ（木野氏）】　ありがとうございました。

【濱田座長】　それでは、引き続きまして、事務局からこの検討会の論点の整理案について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、事務局から資料３－２についてご説明させていただきます。この資料の位置づけとなりますが、第１回、第２回目で構成員の方々がご議論していた内容ですとか、あとはユーザアンケート、Ｗｅｂアンケートですとか、意見募集を行いましたので、それらをまとめて整理したものという位置づけでございます。

それでは、１ページ目からご説明したいと思います。まずは、タイトルにありますが、「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」の整理でございます。

（１）で「関係者の共通認識の下での検討」といたしまして、下線部、「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」としております。

（２）「あるべきネットワークの姿を踏まえた検討」ということで、インターネットには自律・分散・協調という特徴ですとか、経済成長のエンジンという特徴、さらにユーザの表現活動や知る自由を刺さセる重要な基盤としての役割がございますことから、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）で「ユーザの意識や意向を踏まえた検討」といたしまして、「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」といった議論が前提とあったかと思っております。

次のページに参ります。２ページ目からは、タイトルにございますように、「アクセス警告方式について」の整理となっております。

（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」につい

て、まとめております。まず、アクセス警告方式の前提でございますが、ここでは海賊版サイトの認識が薄いユーザですとか、アクセス頻度がそれほど高くないユーザを想定して「カジュアル・ユーザ」と呼んでおりますが、そういったユーザが海賊版サイトにアクセスすることをみずから思いとどまることを促そうとするものという認識だという前提があるところです。

この目的といたしましては３ポツ目でございますが、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当然、目的であると思っております。

４点目でございますが、留意点として、静止画ですとか、ユーザのダウンロード行為が仮に違法となる場合には、ユーザに対して違法であることを知らせる意味や、あるいはユーザが意図せずに海賊版サイトにアクセスをして違法行為を行ってしまうことを防ぐといった意味合いも追加されるというご議論もあったところです。また、それによってユーザの理解が得られやすい面もあるというご意見もございました。

５ポツ目でございますが、ただし、ユーザアンケートの結果に鑑みますと、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は、あまり大きな違いはないという結果も出たところです。

３ページ目に移ります。（２）でございますが、「アクセス警告方式の効果・メリット」についてまとめております。ユーザアンケートの結果を鑑みますと、警告を出すこと自体には一定の効果が見込まれると整理しております。明朝で書いておりますが、現行法の場合でも９３．３％、違法化を想定した場合でも９５．９％の人が、警告画面が表示された場合にアクセスを思いとどまるという結果が出ているところでございます。

２ポツ目ですが、他方で幾つか留意点もございまして、例えば、オプトアウトすれば当然、警告画面が表示されませんし、暗号化通信の場合には警告画面を表示させることが困難ですし、また、警告画面で「はい」をクリックしても、当然、海賊版サイトにはいけるということがこのアクセス警告方式の仕組みでございますので、これらを踏まえますと、海賊版サイトの効果は限定的というご意見もございました。

４ページ目に移ります。（３）で「アクセス警告方式の実施の前提となる法的整理」について、まとめております。１ポツ目が、通信の秘密に関する、これまでの整理についてですが、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であるかと思います。ただし、通信の秘密は、憲法において基本的人権として保障されてい

るものであり、ユーザによる同意の成否は慎重に判断されるべき。さらに、通信の秘密の侵害に関して有効な同意といえるのは、基本的には個別具体的かつ明確な同意が原則でございました。

２ポツ目でございますが、アクセス警告方式の実効性や普及率を高めるためには、通信の秘密に係る同意について、サービス約款にそういった情報を記載することによって同意を取得する方法が考えられるという議論があったところです。こういった約款による包括同意が有効な同意とみなされるかについては、過去の総務省の整理に照らしますと下線部でございますが、「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」というものが大きな第一の条件として挙げられたところでございます。

３ポツ目として、このほか幾つかの条件が過去整理されておりました。

５ページ目に参ります。法的整理の続きでございますが、こういった一般的、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、ユーザの意向を把握することが必要だと考えておりまして、この点、ユーザアンケートを取った結果といたしましては、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」あるいは「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たところです。

２ポツ目でございますが、意見募集に際しましても、アクセス警告方式に対しては、通信の秘密や検閲といった観点から慎重または否定的な意見が多く見られたところでございました。

３点目の補足として、こういったユーザの意向というのは、静止画ダウンロード違法化の有無にあまり大きな違いは見られなかったところでございます。

４ポツ目、一定の結論として以上を踏まえますと、「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」とは言えないのではないか。したがって、「約款による包括同意を有効な同意とすることは困難ではないか」というご意見があったところです。また、この点については、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かと考えられるところです。

６ページ目に参ります。（４）として、「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・コストについて」です。１ポツ目は手法として３つほど挙げておりますが、アクセス警告方式を実施するためには、大きく分けて（ａ）ＤＮＳ＋プロキシ方式、（ｂ）として、プロキシ方式、さらに（ｃ）として、ＤＰＩ方式などが考えられるというヒアリ

ング結果があったところです。

２ポツ目に移りまして、これらの３つの方式の全般的な共通の課題として、暗号化通信の場合には、警告画面の表示が極めて困難ではないかといったご議論があったところです。

また、３ポツ目ですけれども、日本には多数の通信事業者が存在して、構成も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、またはコストの問題が生じ得るおそれもあるというご意見もあったところです。

４ポツ目で、コスト負担のあり方については、慎重かつ丁寧な協議・検討が必要ではないかといったご意見もあったところです。

７ページ目に参ります。その他の事項といたしまして、１ポツ目では、警告表示の対象となる海賊版サイトの基準の公正・中立性の確保が必要であるといったご意見ですとか、サイトリストの管理・運営等の透明性も確保することが必要というご議論がありました。

２ポツ目、３ポツ目には、ユーザの情報の取扱いについて整理をしております。

２ポツ目ですが、個々のユーザが約款による同意からオプトアウトをしているか否かに関する情報というのは、少なくとも個人情報等考えられることから、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。

さらに、３ポツ目でございますが、警告画面を表示した際のユーザのアクセスログですとか、さらにはその警告画面を通じて、その表示にもかかわらず海賊版サイトにアクセスしたログの情報は、当然、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厳格な取扱いが求められるとまとめております。

（６）で、アクセス警告方式についてまとめを記載しております。これらを鑑みますと、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としております。

２ポツ目でございますが、技術的な課題やコストに鑑みれば、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ることから、そのほうが効率的、あるいは、本来のネットワークのあるべき姿にふさわしいというご意見も多かったところでございます。したがいまして、ここから先のページでは、端末側の対応策について整理をしております。

８ページ目で、タイトル部分、３ポツ目として、「その他のアクセス抑止方策について」の整理でございます。

（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」でございます。

１ポツ目ですが、端末側での対応策については、インターネットの End to End 原則に即した対応策の実施が可能であることですとか、通信の秘密に関する法的問題が生じない、

あるいは青少年向けフィルタリングサービスにおいて、一定の海賊版サイトへのアクセス制限の実績があること、あるいはネットワーク側での対策と比較してコストも比較的低廉ではないかといった、さまざまなメリットがあるというご意見をいただいたところです。

他方で、留意点といたしましては、こういった端末側での対応については、法律で義務づけのある青少年フィルタリング以外については、基本的にユーザがみずから申し出て導入する必要があることから、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ではないかというご意見もあったところです。

（２）「具体的な対応策」に参ります。具体的な端末側での対応策については、既存の青少年向けフィルタリングサービスですとか、セキュリティ対策ソフトへの組み込み、あるいはブラウザでの何らかの対応が考えられるといったご意見をいただいたところです。

これらを踏まえまして、まず１つ目として、２ポツ目でございますが、青少年向けフィルタリングサービスが考えられるのではないかとまとめております。この点、青少年が海賊版サイトへのアクセス経験が多いといったユーザアンケートの結果もございましたので、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としているところです。

３ポツ目ですが、他方でフィルタリングのソフトの利用に当たりましては、ユーザの利便性の向上ですとか、あるいは海賊版サイトのリストをフィルタリングソフト事業者へ迅速に提供するといった、いろいろなことを促進していくこと。こういうことが課題だとまとめております。

４ポツ目ですが、２つ目の主な対策として、本日、トレンドマイクロさんにもお越しいただきましたが、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のではないかとまとめております。ここは、セキュリティ対策ソフトに海賊版サイトへのアクセスに対する遮断ですとか、あるいは警告機能を追加することについては、ユーザアンケートの結果を見ても受容性は比較的高いのではないかという結果が出ています。具体的には延長部分ですが、７８％の人が海賊版サイト対策機能をセキュリティソフトに入れることについて肯定的な意見があったところでございます。

９ページ目でございます。その他について１ポツ目でございますが、ブラウザやＯＳなどの端末側の対応を効果的に実施するためには、ＯＳベンダーなどとの連携・協力をいかに得るかが課題といったご意見もいただいております。

また、コスト負担のあり方については、慎重かつ丁寧な協議・検討が必要であるといっ

たことですとか、３ポツ目でございますが、フィルタリングの対象となる海賊版サイトの判断基準ですとか、管理・運営等の透明性の確保の必要性も記載をしております。

（４）で、「その他のアクセス抑止方策について」のまとめでございますが、２つ記載をしております。

１点目として、青少年向けのフィルタリングサービスについては、繰り返しになりますが、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ですとか、周知の強化により、その普及を図っていくとともに、海賊版サイトのリストをフィルタリングソフト事業者への迅速な提供を促進することが望ましいと整理しております。

２点目のセキュリティ対策ソフトについては、これまであまり議論がなされていなかったことから、ペンディング、（Ｐ）としておりますが、本日の意見を踏まえて最終的に記載をこれから考えていきたいと思っております。

１０ページ目に移ります。最後、「その他」の事項といたしまして、２点ほど整理をしております。

意見募集で多く見られたご意見でございますが、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、通信の秘密の保護ですとか、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、意見募集において多くの指摘ですとか、懸念が示されたことに留意が必要かとまとめております。これを踏まえまして、ネットワーク側ではなく、端末側での施策を促進していくことを中心に、海賊版対策のパッケージの１つとして取り組むことが肝要であると整理しております。

２ポツ目でございますが、本施策は海賊版対策のパッケージの１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、また、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と整理しております。

私からは以上でございます。

【濱田座長】　ありがとうございました。

それでは、これからは、今、説明をいただきました論点整理案についてご議論いただきたいと思います。それに先立ちまして、前回会合で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いただきましたが、その内容に関して江崎座長代理からご質問がありました。この点について、野口様から補足があると伺っておりますので、少しご発言をお願いいたします。

【日本インターネットプロバイダー協会（野口氏）】　プロバイダー協会の野口です。前回の発表の中で、ＨＴＴＰＳの通信はブラウザからウェブサーバの間を End と End で暗号化しているので、どのような方式を採ったとしても、アクセス警告方式の画面を出すことが難しいと発表させていただきました。これについて江崎先生からＤＮＳのリダイレクションなどで困難ではあるけれど、実装の方法があるのではないかというご指摘をいただいたところです。

これについてですけれども、まず、暗号化がされていないＨＴＴＰの通信であれば、ＩＳＰのＤＮＳの設定を変えることで比較的簡単に通信を警告のサーバに誘導することができます。

一方で、暗号化されたＨＴＴＰＳの場合は、ブラウザの仕様上の問題ですけれども、ブラウザはユーザがアクセスしようとしているＵＲＬのアドレスバーに表示されているホスト名と、サーバが持っている証明書に書いてあるホスト名を比較照合します。海賊版サイトであれば、海賊版サイトの電子証明書をＩＳＰプロバイダが入手できない限りは、ブラウザで証明書の検証に必ず失敗をしますので、（アクセス）警告画面の表示までいかないで失敗するというのが通信の規格上も挙動として想定されます。多くのブラウザですと、検証に失敗しても「証明書が検証できません。危険です」というような、非常にド派手な（ブラウザの）警告画面が最近出るようになっていまして、これを無視して進むという選択肢は一応あるのですけれども、非常にセキュリティのリスクが高くなってしまうので、ユーザにそのようなリスクを踏んでくださいとはとても言えないことになります。ユーザがこれを気軽に踏んでしまうと何が起こるかですが、海賊版サイトの対策を始めてみたら、今度は銀行の海賊版サイトが横行してしまったということになりかねませんし、原則通り、踏むべきではないと考えるのであれば、今度はユーザとしてもブロッキングされたのか、それとも海賊版サイトになりすました海賊が現れたのか、それもよくわからない状態になってしまって、結局は説明責任を果たせないブロッキングのような扱いになってしまうと思います。これも前回、多少ふれたお話になるかと思います。

あとは、大規模なサイトの効率的な配信などにはＣＤＮというものが使われていまして、これはＤＮＳを使ってＣＤＮのサーバに転送しているので、確かにこれを応用するとアクセス警告画面に誘導することができるように思えるのです。この場合でもブラウザが検証するのは、アドレスバーに表示されているサイトのホスト名と、証明書に書かれたホスト名であるということは全く変わりがないので、ＤＮＳというのは、アクセス先のＩＰアド

レスを曲げることはできるのですけれども、その上で動いているブラウザのアドレスバーのＵＲＬを変える力まではないので、証明書はもともとのサイトのものが必要です。何でＣＤＮがこのようなことができるのかというお話ですけれども、サイトの運営者から証明書を預かっているのです。ＣＤＮというのはサイトの運営者が契約しているサービスなので、サイトの運営者から証明書を入手することはできます。ほかにも方法が幾つか考えられるのですけれども、基本的にはサイトの運営者が自分の意思で転送をしかけたりしているので、証明書を用意することが簡単ですが、アクセス警告方式は１つ大きな前提があって、海賊版サイトの運営者の協力を得られないという前提で考えないといけないので、そうすると証明書を入手することが難しいのではないかと思うのです。証明書の国際ルールがありまして、これはサイトの運営者の権限であるとか、意思を確認してから発行しないといけないことになっているので、無関係なプロバイダが海賊版サイトの証明書を入手することは現実的ではなくて、昔は証明書を発行するところのサーバが乗っ取られて、証明書を不正取得されてしまって、イランの国内で盗聴の行為に使われたのではないかという話があったのですが、私たちがそのような方法を取るべきとは、多分、合意が得られないのではないかと思います。

そろそろまとめになるのですが、技術的に方法がないと断言することは、ないことの証明になるので難しいです。ただ、そもそものお話として、ＨＴＴＰＳというもの自体がEnd to End の原則の下でブラウザとサーバの間を暗号化しまして、その途中にあるものが手を加えることを一切許さないという設計思想なので、そうすると技術的な規格であるとか、証明書のルールも基本的にはそれに合ったものになっています。ですから、プロバイダが内容を見たり、変更したりするような、差し替えるような手段がもしあるとすれば、それは証明書の不正取得であるとか、アプリケーションやプロトコル自体に脆弱性があると言ってもいいもので、それはおそらく直ちにふさがれてしまう性質のものなのではないかと思います。もう少し簡単な言葉で言うと、ネットワークの途中で海賊版サイトになりすます方法がもしあるならば、それは銀行になりすます方法もあるということになってしまうので、それは避けないといけないのかと思います。

結論としては、ＨＴＴＰＳの暗号化された通信において、ユーザか海賊版サイトの運営者の積極的な協力を得ることなしに、途中のプロバイダが無断で割り込んで警告画面に差し替えるということは、現実的な手段の中ではなかなか想定するのが難しくて、不可能と言い切れるかどうかはともかく、実質的に不可能と今の段階では言っていいのではないか

と思います。最初のトレンドマイクロさんの発表をいただいた中にもあったのですけれども、エンドポイントでの対策が普及するといいと思います。以上、補足をさせていただきます。

【濱田座長】　ありがとうございました。

江崎委員から何かありますか。

【江崎座長代理】　基本的には先ほどの説明で正しくて、技術的に非常に難しい。ただ、気をつけなくてはいけないのは、何らかの形でそれを可能にするような運用が少し性急っぽくやられる可能性がゼロではないということですので、現状では非常に難しいということで整理をしていいかと思います。ただ、それが完全性は証明できないものなので、常にそれをウオッチングしていかないといけないようなものだというスタンスかと思います。

【濱田座長】　ありがとうございました。

それでは、戻りまして、資料３－２の論点整理案について、皆様方からいろいろご意見をお伺いできればと思います。まず、構成員の皆様方からご意見を伺って、その後、オブザーバーの皆様から何かあればお伺いしたいと思っております。お願いいたします。

【曽我部構成員】　曽我部でございます。８ページの下半分のところですけれども、特に（２）の一番下のポツで、「セキュリティ対策ソフトへの組み込み」というところです。これは要するに、今日のお話からしても、フィルタリング機能を組み込むということでしょうか。（２）の前半がフィルタリングの話で、４ポツ目の「２つ目に」というのが、セキュリティ対策ソフトへの組み込みですけれども、これはフィルタリング機能をセキュリティ対策ソフトに組み込むということなのだと今日の話からすると理解したのですが、何か若干、この書き方が不明瞭な感じもするので、その辺をクリアにされるといいのかと思いました。全体としては特段、異存はないのですが、今のところだけ書き方について気になったので申し上げさせていただきます。

【濱田座長】　ありがとうございます。

今の点、事務局から何かどうですか。

【中川消費者行政第二課課長補佐】　ご意見を踏まえて検討させていただきますので、よろしくお願いします。

【濱田座長】　ありがとうございました。

ほかにいかがでしょうか。どうぞ。

【江崎座長代理】　どうもありがとうございました。特に最後の１０ページ目にも関係

するかと思いますけれども、前回での議論も含めて、通信の秘匿性というのは非常に重要視しなければいけないものだということが出てきているというのが、この報告書の中でも強調されるべきポイントだろうと思います。つまり、当然ながら違法な著作権等に関するものというのは避けるべき、没するべきものであるけれども、それよりもより通信の秘匿性というのは極めて重要なものであるということがちゃんと書かれるべきかと。

それから、この国際連携、国際執行の強化というところは、もちろん、マルチステークホルダーでの１つのメンバーとしての責任ということかと思いますけれども、特に今回のＧ２０でのＤＦＦＴという、Data Free Flow with Trust というのが、戦略的に日本として出しているし、これがグローバルなコンセンサスに近づいているということを考えると、リーダーシップを取っていくべきだというところがあったほうが実はいいのではないか。というのは、Data Free Flow with Trust を問うときに、通信の秘匿性が国外からも我が国の特徴として評価されている。これは当然、ＧＤＰＲの議論の中でのＧＤＰＲと日本の間での関係の中で、通信の秘匿性が非常に評価されているということもございますし、アメリカでのスマートシティのようなところでの日本のプロバイダがどうして信用されたかというところは、実は通信の秘匿性の部分が非常に重視しているところで、個人情報がきちんと保護されるというところから採用されているということにもあらわれているように、そこは非常に守るべきポイントであるということが改めてアンケートでも出てきたし、全体の意見としても存在しているし、国家戦略としても非常に重要だというところが少し出るような形にしたほうがいいのではないか。つまり、著作権違法のものだけの議論だけではなく、その後ろにある、もう少し大きなポイントもこの委員会の中での重要な議論のポイントだったということを出したほうがいいのではないかと思います。

【濱田座長】　ありがとうございます。今、ご指摘いただきましたが、それぞれ事務局からお答えいただくというよりは、今日のご議論を踏まえて最終的な取りまとめをしていただくという形で引き取らせていただければと思います。

それでは、ほかに。はい、どうぞ。

【森構成員】　ありがとうございます。今の江崎先生の意見に賛成ですので、かなり重複すると思いますけれど、申し上げます。アンケートという話がありました。アンケートというか、提案募集結果ですね。この端末のタブレットの資料だと１１番の提案募集結果のところに提出意見が整理されています。結局、こちらでは今回、アクセス警告方式を検討するに当たって、幾つか論点を出してそれについて意見を求めたわけですけれども、返

ってきた意見を見てみると、１１番目の資料２－１、「提案募集結果」とありまして、その６ページです。この「主な提出意見」のところで、「アクセス警告方式が通信の秘密を侵害する」、「通信の秘密への影響が大きい」ということで、「同種４５件」とあるわけですけれども、その代表的なものを見ますと、一番上のものも「アクセス警告方式はその仕組み上、通信の秘密を侵すので実施するべきではない。これは先の海賊版対策の議論の中でも問題になったブロッキング方式と全く同じである」。それから、２番目も、「アクセス警告方式には反対する。アクセス警告方式はブロッキングと比較して……幾分ましに思えるが、通信の秘密を侵害していることに何ら変わりない」。３番目ですが、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代替案として不適当となっていて、こちらとしてはアクセス警告方式のことについてお尋ねをしているわけですけれども、返ってきた意見はブロッキングも引用して、通信の秘密を侵害することに懸念があるという意見が非常に多かったということです。そのことは、先ほどのご指摘のとおり、しっかり書いていただく。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、たくさん出ているわけですから、それは海賊版対策のパッケージの中における位置づけとして、アクセス警告方式の話にとどまるものではなくて、そういったことについて反対の意見が多い。ブロッキングもアクセス警告方式も反対の意見が多いのだということははっきり書いていただくべきなのではないかと思います。それが１点です。

もう一つですけれども、海賊版対策のパッケージの話です。資料３－２の今回つくっていただいた論点整理ですけれども、１０ページ、今、私がお話ししたブロッキングも含めて通信の秘密の侵害について異論が多かったことはここに書いていただくべきだと思います。もう一つ、１０ページの２ポツには、パッケージの１つであることから、「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」とあるわけです。これは確かに、今のオフィシャルな海賊版サイトパッケージがこういうメニューになっていますので、こういう書き方になっているのだと思うのですけれども、ブロッキングのときから出ている議論として、さっき野口さんのお話にも出てきたＣＤＮの話があると思うのです。これは幾つか問題のあるところで、ネットワーク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思うのです。その有効な対策ではないかと思うというのは、議論すべきところがあって、まず、著作権法の問題として、著作権侵害でＣＤＮに対して削除請求できるのか

ということがあります。私はできると思いますけれども、できないというご意見もある。でも、これを掲示板と同じだから意見が分かれているということも言えるのかもしれませんけれども、掲示板と全く同じではないと思います。先ほど野口さんの話にもありましたけれども、ＣＤＮと海賊版サイトは契約をしているわけなので、少なくとも匿名掲示板などとは違うと思います。なので、１つは実体法上の整理、それから、もう一つは、ＣＤＮの大手はすべて海外事業者なので、海外の裁判所でやるかというところはまた大変な話ですけれども、日本の裁判所でできるのではないかと思います。管轄の問題、それから、準拠法の問題もありますので、ネットワーク側、通信事業者側からお手伝いできることとしては、ＣＤＮ対応ということが１つのカテゴリとしてはっきりあるかと思いますので、それについて検討してはどうかということを提案したいと言いますか、そのように書いていただいたらどうかと思います。

以上です。

【濱田座長】　どうもありがとうございます。

ほかの皆様はいかがでしょうか。はい。お願いします。

【上沼構成員】　ありがとうございます。上沼です。

今、森先生のおっしゃった意見は全くそのとおりだと思います。それとは別の観点で申し上げます。アクセス警告方式もブロッキングも、ユーザの行為を制限することで違法サイトへのアクセス数を減らそうという対策だと思うのです。今までの議論で出てきた結果、ブロッキングとアクセス警告方式は通信の秘密の問題もあるし、技術的な難点もあるというところが共通しています。ところが、同じユーザ側の行為を制限する仕組みとしては、端末側の制限という方法もあり、それがここでいわゆる「フィルタリング」として議論されているものです。「フィルタリング」という言葉のイメージがわかりにくいので、先ほど曽我部先生がご指摘くださった８ページみたいな言い方になってしまうのだと思いますが。要するに、自分の意思で自分のアクセス先をコントロールする仕組みという意味では、別に対象は青少年である必要がないはずのものだと思います。８ページで言われているのは、それがたまたまセキュリティ対策ソフトという成人も使っているソフトの中に入るのであれば、より普及しやすいのではないかということなのではないかと思うのです。そのように考えるのであれば、ユーザの意思でアクセス先を選べる仕組みの有用性をもっと広報することによって、この実行性は上げられるのではないかと思うわけです。先ほどのトレンドマイクロさんの資料５ページで、セキュリティ対策非利用が４４％というのが出て

いてかなり高いように見えます。これはスマートフォンのＯＳの仕組みなどで、実際に使わなくてもリスクが低いというのがもちろんあるとは思うのですが、この場合の非利用という数字の中にはもしかしするとＯＳ上の制限が入っているのに気がついていないという可能性もあります。ですので、ＯＳの機能も含めて、ユーザがみずからのアクセス先を自分でコントロールすることで快適なインターネット環境をつくっていこうということをもっと積極的にアピールするべきなのではないかと思います。以上です。

【濱田座長】　はい。お願いします。

【長田構成員】　今、上沼先生に整理していただいて非常によくわかると思いました。青少年とともに、特にモバイルの場合、今、大きく出てきているのがシニア世代というか、高齢者の、さまざまなサイトにいってしまったがための消費者被害みたいなものも非常に多くなっておりまして、そういう意味からも今回の報告書の中には少しわかりやすく今の仕組みを、上沼先生がご提案のように書いていただいたほうが、さまざまな人に届くのではないかと思いました。

今回のアクセス警告方式に対しての考え方のまとめについては異論ございませんので、その他のところを少し充実して、わかりやすく書いていただくのがいいのではないかと思いました。以上です。

【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。どうぞお願いします。

【長田構成員】　言い忘れました。「その他」のところで、さっき森先生もおっしゃっていたのですけれども、ブロッキングとの関係のところは簡単に示してくださっているからネットワーク側という表現になっていると思うのですが、そこもきちんとブロッキングという手法に対しての考え方もわかりやすく丁寧に書いていただければいいと思います。

アクセス警告方式がだめなら、ブロッキングしかないという展開にならないように、きちんとそこは考え方を明確に書いていただければと思います。

【濱田座長】　ありがとうございました。どうぞ。

【江崎座長代理】　先ほどのご意見、僕も大賛同で、しっかりとユーザが選択してできるというところを担保するべきであるというところはかなり強調して書くべきではないか。これが通信の自由に対しての我々日本、それから、世界にちゃんとやっていく姿勢をしっかりと出すべきではないか。逆に言うと、今、世界的にはそれと逆の方向が出ているところも無きにしも非ずということをかんがえると、ここをしっかりとエンドユーザの選択権

を持つことが非常にデジタルコミュニケーションにとって重要なアジェンダであるということはしっかりと書いたほうがいいのではないかと思います。

【濱田座長】　ありがとうございます。

それでは、オブザーバーの皆様、どうぞ。

【日本インターネットプロバイダー協会（野口氏）】　江崎先生、先ほどのコメント、どうもありがとうございました。通信の秘密を守るプロバイダというものが国際的に信頼されているという話はとても貴重なご意見として、私どもとしても利用者の皆さんのプライバシーでもありますし、産業にとっては産業機密というものは国の成長戦略の柱の１つでもあると思います。そのすべての基盤となるものだと思いますので、エンドの利用者を主体にした通信の秘密をこれからもきちんと守っていきたいと思っています。

森先生からＣＤＮのお話についてご意見があったのですけれども、End to End の原則で、途中にいる人が中身を見えませんよということはそのとおりですが、実はインターネットの世界では通信の存在そのものを完全に秘匿するということは、これまた難しいので、トレーサビリティというものは結構まだあったりします。つまり、完全な匿名のインターネットというのは、なかなかできないというのがあります。ですので、発信者に近いところまで寄ろうと思えば寄っていける。つまり、発信者に近いところまで迫ることは基本的にはできるのです。ＣＤＮというのは、実は発信者に代わって通信のエンドポイントになっているところという見方ができるので、そのエンドポイントになっているＣＤＮに対して対応を求めていくことは、考え方としては非常に説得力があるといいますか、現実的なの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。

ほかにいかがでしょうか。どうぞ。

【森構成員】　野口さんから、今、しっかり技術的に補足をしていただいて、ありがとうございました。End to End の原則に反しないということですけれども、我々からしてみれば掲示板に誹謗中傷を書かれたことの削除請求というのは、一大カテゴリといいますか、仮処分の７割とも言われるような事件なので、そういった難しいことを抜きにしても、非常に頻繁に行われていることでしたので、素朴に申し上げたところです。

補足をさせていただきますと、そうすると、発信者情報開示を、といった話ももちろんあるわけですけれども、ＣＤＮは多分、発信者のＵＲＬはすぐに教えてくれる。元サイトはすぐ教えてくれるのだと思うのです。元サイトは防弾サーバだということだと思うので

すけれども、発信者情報開示の場合、別に元サイトのＵＲＬを教えてくれれば、それで終わりということではないので、もう少し発信者に迫ることができますから、そのあたりも検討の余地はあるのかという気はします。以上です。

【江崎座長代理】　関連してよろしいですか。

【濱田座長】　お願いします。

【江崎座長代理】　管理技術的に発信者に寄っていくことができるような技術というのは存在するし、開発することはできるのだけれども、できることとやらないことというのはちゃんと区別しなくてはいけなくて、できるのだけれどもやってはいけないというところをしっかりと区別してやる。しかもそれが特にＣＤＮに関して言うと、森先生がおっしゃったように、グローバルドメインでのプレイヤーとしての話になってくるので、そうすると総務省の中ではプラットフォームサービスに関する研究会でも議論されているように、域外適用みたいなもののコンセンサスをしっかりつくっていかないと、この問題は解決できないということで、単独の国で解決できるような問題では、技術的にはできそうに見えるけれども、それができるかを考えたときに難しい問題が存在していることをしっかりと認識した上で対策をやっていかないといけないとになると思います。

【濱田座長】　ありがとうございます。どうぞ。

【森構成員】　何度も申しわけありません。今の江崎先生のお話で、私の趣旨としては、もちろん、いろいろな国、ＣＤＮも外国のプレイヤーですけれども、いろいろな解決すべき課題はあって、実体法上もありますし、民事訴訟をどこの裁判所でできるかとか、どこの法律が適用されるかということもありますが、方向性としては、日本法でできるのではないかということを検討できるのではないか。つまり、これはぜひともいろいろな国で検討されるべきである、それによって乗り越えるべきであるというよりも、むしろ日本でできるのではないのと。そのことを検討する。間違いなくこうだとは私も言えないわけですけれども、そういうことを検討する余地があるのではないかということです。

【濱田座長】　ありがとうございます。

構成員の皆さん、あるいはオブザーバーの皆様、さらに何かございましたらどうぞ。

【上沼構成員】　話がどんどんクラウド何とかにふれちゃうのですけれども、クラウド何とかは元のサーバを教えてくれないのですか。

【日本インターネットプロバイダー協会（野口氏）】　もとのサーバまでは教えてくれると思います。

【上沼構成員】　　ＵＲＬでは？

【日本インターネットプロバイダー協会（野口氏）】　　ＵＲＬというか、オリジンサーバのＩＰアドレスまでは教えてくれないと思います。ただ、オリジンサーバがどこの会社にあるのかということは権利侵害を受けた人に対しては答えているという運用であることを聞いたことがあります。

【上沼構成員】　　その何とかに聞いても、どこに侵害のサイトがあるのかというのをきちんと教えてくれないので、そういう意味でも、現在、ほんとうに悪い人のところにいくための追跡ができない状況に問題があることを言いたかっただけです。

【日本インターネットプロバイダー協会（野口氏）】　　確かに技術的には１個隣までトレーサビリティがあるといったらいいのでしょうか。つまり、例えば、そこの発信元、オリジンサーバがどこのＣＤＮを使っているというところまでは明らかで、おそらくＣＤＮというのは発信者とは契約関係があるので、そこのＣＤＮに聞けば、または対応を求めれば、一応、対応ができるのかもしれないということも確かです。ただ、法的な話もあるのかもしれないですけれども、そこが協力的かどうかというお話で、協力的でないときにどのような形でそれをちゃんと権利侵害に対して対応してもらうかという話は、おそらく政策の議論なのかという気がしています。

とりあえず、以上です。

【濱田座長】　　ほかにはいかがでしょうか。ございませんか。

それでは、活発な議論をいただきまして、ありがとうございました。

今後ですけれども、今日説明いただきました資料３－２、論点の整理案、それから、ただいまいただいたご議論を踏まえて、この検討会の取りまとめを事務局で作成いただければと思います。そして、それを次回会合において提示いただきたいと思います。

最後に、事務局から連絡事項ございましたら、お願いします。

【中川消費者行政第二課課長補佐】　　事務局からは特に連絡事項はございません。次回会合については別途ご案内したいと思っております。

以上でございます。

【濱田座長】　　それでは、本日の議事は全て終了ということで、第３回会合を終了させていただきます。皆さん、お忙しい中、ご出席いただいてありがとうございました。