○岸本参事官　それでは、少し時間よりも１分早いのですけれども、皆様おそろいですので、勉強会を始めさせていただきたいと思います。

本日は御多忙のところ、御参集いただきましてまことにありがとうございます。

本日、御出席いただいております委員、関係省庁の方々は、座席表をお配りしておりますので、そちらをごらんいただきたいと思います。

まず開催に先立ちまして、事務局長の住田から御挨拶をさせていただきます。

○住田局長　本日は暑い中、お集まりをいただきましてありがとうございます。

きょうはいつもの会合とは違うということをより明確にするために、グループディスカッション方式にしてみました。これは知財事務局は割とお得意のパターンでございまして、知財ビジョンをことしつくったのですけれども、そのときも基本的にはこういうグループディスカッションの形式で、それぞれのグループでわいわいがやがややるということをやってございました。距離が相当近くなるので、ふだんの遠いところで横に並んでいるから誰がどんな顔してしゃべっているのかもわからないというのとは大分違って、顔が見える、心の通う会話がよりできるのか、あるいはよりバトルモードになるのかわかりませんが、いずれにせよぜひ自由にきょうも御議論をいただきたいし、できるだけ活発な御議論ができるような仕掛けを幾つか考えたいなと思いますので、よろしくお願いしたいと思います。

いろいろ多岐にわたるので３つに分けたわけですけれども、それを基本としながら、また最後には全体でのディスカッションなどもしたいと思いますので、それぞれのテーブルでどのようなことが話題になって、専門家の方がいらっしゃいますから、どういう質問、答えがあったみたいなことも後ほど、それぞれのテーブルから紹介していただくような形で進めたいと思いますので、暑い中３時間たっぷり時間をとってございますので、よろしくお願いしたいと思います。

○岸本参事官　ありがとうございました。

それでは、本勉強会の進め方の確認と配付資料の確認をさせていただきたいと思います。

お手元の議事次第と配付資料一覧をごらんいただきたいと思います。

本日の勉強会の進め方ですけれども、まず事務局で幾つか委員の先生方から事前にこういったテーマで話を聞きたいということで、御提案いただいた内容に沿った形でヒアリングをしておりますので、そのヒアリング内容の御紹介をさせていただき、その後で各省庁から基本的な法制度運用の説明ということで、それぞれの省からの御説明をお願いしております。

その後で、前村委員から少し技術的なところにつきまして補足資料をいただいておりますので、それについての御説明をお願いしたいと思います。

そこまで終わりましたところで質疑応答の時間を30分程度とりたいと思います。全体としてヒアリング内容の説明、各省庁からの説明、前村委員からの御説明と質疑応答で１時間ぐらい予定しておりますけれども、それが終わりましたらグループ討議に入らせていただきまして、グループ討議も委員の間での知識共有をより限られた時間で深めていただく

ということで、３つのグループに分かれて、それぞれのグループ内で事務局で設定させていただいたテーマに沿った形で知識共有をしていただければと思っております。

前半と後半に分けて進めたいと考えておりまして、まずはグループ内での知識共有の時間を50分程度とっておりまして、その後で30分程度、それぞれのグループでどういったやりとりがあったのかということについて簡単に御報告をいただいた上で、全体としての質疑応答、意見交換の時間をとりたいと考えております。大体その全てを順調に行いますと３時間で終わる見込みとなっております。

配付資料なのですけれども、お手元の配付一覧をごらんいただきますと、資料が14種類ぐらいございまして、資料１、２、９、10、11が事務局でヒアリングをさせていただいた結果、あるいはそのときに御意見をいただいた方から提供いただいた資料となっております。前村委員の説明資料が資料３、各省庁からの説明資料が資料４から資料８までございますけれども、資料４だけ直前の差しかえとなってしまいましたので資料番号がついておりませんが、総務省さんから御提出いただいた資料となっております。

また、資料３で前村委員の御説明資料の参考資料、英文のものになっておりますけれども、一番後ろにつけてございますのと、神田弁護士のヒアリング結果、資料10－２の参考資料が１つございまして「ブロッキング問題に関する意見書」平成30年８月５日付の１枚物が一番後ろに置いてあるかと思います。

最後にグループ内討議のときに御活用いただくために、机上配付で封筒に入れた形で、これまでのタスクフォースの配付資料を全部その中にまとめて入れておりますので、適宜御参照いただきながら議論を進めていただければと考えております。

何か不足等ございましたら今､お申し出いただければと思いますが､大丈夫でしょうか。

１つ、グループ討議における発言につきましてお願いがございます。委員及び傍聴の皆様におかれましては、グループ討議によって知り得た情報を外部で取り扱うときには、内容はお話しいただいて構わないのですけれども、発言をした方がどなただったのかという所属と氏名については原則として特定しないような形で、いわゆるチャタムハウスルールと言っておりますけれども、取り扱っていただきますようにお願いをいたします。もし発言者に言及されたいという場合には、個別に発言者の方の御理解をいただいた上でオープンにしていただくようにお願いをしたいと思いますが、いかがでしょうか。よろしゅうございますでしょうか。そういう形でグループ討議の時間については進めていただきますように、よろしくお願いいたします。

まず事務局によるヒアリング内容につきまして、私から御説明をさせていただきます。

資料１をまずごらんいただきたいと思います。Googleからいただいた資料でございまして、検索エンジンの取り組みということで事情をお伺いしたのですが、１つ、これはヒアリングさせていただいたのですけれども、その内容について正確性を期すために現在調整中といいますか､本社に確認中であると伺っておりまして､本日は配付できないのですが、事務局で聴取させていただいた内容につきましては調整がとれ次第、次回、第５回のタス

クフォースで配付をさせていただきたいと思います。

本日お配りしておりますのは、Googleからヒアリングの際に御提供いただいた資料でございまして、７月27日の文化審議会著作権分科会の法制・基本問題小委員会に配付された資料ということで伺っております。現在、文化審議会のホームページ、ネットのほうにもアップされているということで伺っております。

簡単に御説明申し上げますけれども、めくっていただきまして１ページ目、Googleのテイクダウンの取り扱いということですが、デジタルミレニアム著作権法、アメリカのDMCAに基づいた手続に従って行っていらっしゃるということで、１ページ目の下のほう、2015年だけで５億5800万のユーザーからのリクエストを受けて、98％以上は削除していると書いてございます。

３ページ、著作権侵害に関する通知の要件ということで、申し立ての際に必要とされる要件について簡単にまとめております。メールアドレスとか住所、電話番号などの情報、それから､侵害されていると考えられるコンテンツの個別のURLを知らせる必要があるということ。また、著作権者あるいは代理人としての物理的または電子的な署名が必要であるということ。こういった通知を受けたときに平均処理時間ですけれども、６時間以内に対応しているということが書いてございます。

４ページ､Trusted Copyright Removal Programというものがあると書いてございまして、適切な通知を提出しているという実績があって、毎日大量の削除リクエストを提出する必要のある著作権者を対象としたプログラムがある。TCRPといわれるものということで、このプログラムのパートナーになった場合、まとめて大量の削除リクエストを効率的に出すことができると書いてございます。

その下ですけれども､この著作権侵害による削除通知､DMCAシグナルというものですが、これを活用するという形で、一定のサイトに関して削除通知の有効件数が多かった場合、検索結果のランキングを考慮する際のシグナルの１つということで活用されているということで、有効な著作権侵害による削除通知が大量に出されているサイトに関しては、だんだんと検索結果も下位に表示されるような取り扱いになっていると書いてございます。

５ページ、このDMCAシグナル、削除通知ですけれども、Googleの広告サービスでも活用されていて、そういった大量の通知を受けているものに関しては、Googleは広告を出稿しないという取り扱いになっていると書かれております。先ほど申し上げましたとおり、ヒアリングの結果につきましては、次回のタスクフォースでも調整したものをお配りしたいと思っております。

資料２、海賊版サイトに対するフィルタリングの強化というテーマで、弁護士の上沼先生にお話を伺って簡単にポイントをまとめさせていただいております。

１ページ目、青少年のフィルタリングですが、2008年に成立しました青少年インターネット環境整備法に基づいて実施されている。ただ、概要につきましては後ろのほうに参考資料ということで簡単にまとめておりまして、改正もことしされていると伺っております

けれども、近年、青少年の間でスマートフォンが普及したことによる課題が浮上していると伺っておりまして、その対応としてポイントとなることを整理してみております。

１つ目がAppleとの連携体制の構築ということでございまして、携帯電話、これはガラケーとスマートフォン両方なのですが、インターネット接続におけるフィルタリング手法というのは、大きく分けてここに書いてありますような①と②の手法がある。１つ目はガラケーの場合ですけれども、携帯電話事業者のネットワーク回線にフィルタリングをかける手法。スマホの場合はこれでかけられる場合もあるのですが、そうでない接続の場合、②なのですけれども、Wi-Fiなどの携帯電話以外のISPを通じたインターネット接続ですとか、ブラウザ以外のアプリを通じたインターネット接続というものがありますので、それに対応するためにどうすればいいかというと、スマートフォンの端末に特定サイトの閲覧ブロックをできるようなフィルタリングのアプリをインストールするということですとか、特定アプリの起動制限処理を施す手法がある。

２つ目の〇ですけれども、ただ、スマートフォンのOSがiOSの場合、つまり機種がiPhoneの場合ですが、②（ａ）についてはフィルタリングアプリというものがプリインストールされていないということでして、店頭でインストールする、インストールから始める必要があるということで時間がかかる。②（ｂ）につきましては、iOS自身の機能制限機能を利用してアプリの利用可否を制御する必要がある。ただ、これも保護者の中にはこういった設定がわかりづらいとか、面倒だということで、そもそもフィルタリングを設定しないという人もいらっしゃるということでございます。

３つ目の〇ですけれども、iOSにはウエブ、アプリともに機能制限を利用することでフィルタリングを実施することができる。この場合、インストールする必要はないのですが、アクセス制限対象というのがAppleが独自に判断するという実情になっておりまして、必ずしもそのレイティングというものが日本の感覚といいますか、現状を反映していない場合がある。そうしますと保護者が日本で普通に使われているのに使えないということで、子供のリクエストに応じて外してしまうということが起きているということも伺っております。

このため、青少年ユーザーが安全に安心してインターネットを利用できるということを担保しながら、同時にフィルタリングが青少年のインターネット利用を過度に制限しないようにということで、Appleとの間でiOSの機能制限について適切なレイティングといいますか、情報というものを共有して反映する仕組みというものが課題になってございます。

ポイント２つ目なのですけれども、モニタリング体制でございます。モバイルコンテンツ審査・運用監視機構（EMA）が事業者の申請を受けて管理情報を審査し、青少年の利用にふさわしいサイトやアプリを認定し、その運用状況の監視を行うとともに、これらの認定サイト、アプリについては、EMAが認定したものに関してはフィルタリングの対象から除外、アクセスできるようにするための活動を行っていたということなのですけれども、スマートフォンの普及によるフィルタリング利用率というものがだんだん低下してまいりまして、

その辺の資料は後ろのほうに、11ページあたりにあるのですけれども、スマホで平成27年度で45.2%という利用率になっております。こういったことから会員企業による会費収入とか認定制度の審査・運用監視料がだんだん入らなくなり、EMAを運営することが次第に難しくなってきた。

保護者が青少年の利用の可否を判断するために有用な情報を提供する形のモニタリング、情報提供の枠組みというものをつくろうという調整が行われていたようなのですけれども、なかなか合意に至らず、ことし５月末でEMAが解散されることになった。現在、EMAの清算法人が来年４月末までの運用・監視を継続することになっているのですが、その後どうするかということに関しては、関係企業が独自にフィルタリングを実施することになっており、青少年のネット利用の健全化を担保するための枠組みについては、今のところ未定という状況であると伺っております。

３つ目のポイントなのですが、フィルタリングの枠組みへの著作権侵害サイトの追加ということでございます。現状、著作権侵害サイトの扱いがどうなっているかといいますと、そのフィルタリングアプリの中でウエブを通じてアクセスする場合、不法という類型でフィルタリングの対象となっております。きちんとフィルタリングをかけていればアクセスはできない状況になっております。

今後、広告に対する取り組みなどが進んでいけば、著作権侵害サイトというのはサイト自体も侵害コンテンツで不法ということで不適切なものなのですけれども、広告も不適切なものであるということであったり、サイト自身のセキュリティーの問題であるとか、個人情報の抜き取りといったような問題があり、アクセスが推奨されない要因が複数発生するだろうということが予測される。そういったことを考慮しますと、著作権侵害サイトへのアクセスというのがセキュリティーの上でも危険なものということで、青少年のみならず、成人を対象に含むセキュリティーソフトにおいてフィルタリング対象としていくこともあり得るのではないか。成人であってもみずからの意思で著作権侵害サイトのフィルタリングを受け入れることが前提であれば、そういった仕組みをつくることは望ましいのではないかというコメントをいただいております。

資料２につきましては以上でございます。

次に資料９をごらんいただきたいと思います。これはアクセス制限、ブロッキングに関する請求権について、実態法上どう考えることができるのかということにつきまして、東京大学の森田教授にお話を伺ったものをまとめたものでございます。

森田先生に伺った点なのですけれども、大きく２つございまして、１つ目は諸外国といいますか、イギリス、オーストラリアもそうなのですが、アクセスプロバイダみずからが著作権侵害を行っていないにもかかわらず、海賊版サイトへのアクセスをブロックする義務を法律上、位置づけることが日本の民事法上、可能かというのが１点目。２つ目が、その請求権というものについて実態法上の権利として存在するけれども、訴訟上でのみ行使できる権利、あるいは裁判によって初めて形成される権利とするような制度設計というの

は、どういう場合に採用されることが適当なのか。著作権侵害についてそういう制度設計を行うことが許容されるか、また、妥当なのかという点について伺った。

１つ目の点なのですけれども、みずから侵害を行っていないものに対するブロッキングの義務を位置づけることについて、日本の民事法上、可能かということについてなのですが、黒ポツの１つ目にありますように、可能ではあるけれども、類似の権利義務が存在しないので、どういった考え方に基礎づけることができるかに関する検討が必要である。例えばプロバイダ責任制限法の発信者情報開示請求権は、非侵害者に司法上の義務を負わせている例ではあるのですけれども、一般義務化された民事法上の文書提出義務の基礎にある真実解明に協力する義務と共通する性質を有する。これを実体法上の請求権として構成したものである。

民事訴訟法上、真実解明のために文書提出命令によって相手方、また、訴外の第三者から情報を得る方法というものが定められており、訴状が提起できれば文書提出命令によって発信者情報を得ることが可能になるのだけれども、日本の場合、発信者不明のまま訴訟を提起することが難しいということで、訴え提起前の証拠収集手続というものも当時はなかったということから、独立した権利として発信者情報開示請求権が定められた。

３つ目の黒ポツですけれども、仮に日本でサイトブロッキングを請求する権利を設ける場合、同様に何らかの基礎づけが必要である。現段階で考えられるものということで挙げていただいておりますが、インターネット上の権利侵害については侵害者に対して救済のエンフォースメントができない場合があるので、法の実現を確保するために権利侵害情報の流布を一定程度とめることができる立場にあるアクセスプロバイダに、公序維持のための協力義務を負わせるという考え方というのがある。どのように権利侵害に関する救済を実現するかという目的は本来的には公的なものであるけれども、インターネットにおけるアクセスプロバイダの公共性に鑑みて、職業倫理上の義務として協力義務を司法上の義務として構成して課すことも可能ではないか。

なお書きのところですけれども、サイトブロッキング全般にかかわる問題として、アクセスプロバイダに義務を負わせることがほかの分野にどういう効果を及ぼしていくのかということについては確認、検討が必要である。著作権のみに関する制度を設けることが妥当かということについても、検討が必要だろうというコメントをいただいております。

論点の２つ目、それを裁判上でしか行使できない、あるいは裁判によって初めて形成される権利を構成することは可能なのかということなのですが、１つ目の黒ポツにありますように、可能ではあるけれども、似たような権利義務が現在ないということで、どのような考え方に基礎づけることができるのかに関する検討が必要である。例えばほかの権利について少し整理しておりますが、２つ目の黒ポツのところで詐害行為取消権とか破産法上の否認権。これは実体法上の権利として存在するけれども、裁判上でのみ行使可能な権利である。その理由は、権利行使の効果が他の債権者の利害に重大な影響を及ぼすという点にある。

ハーグ条約に基づく子の引き渡し請求や裁判離婚については、裁判所の判断があって初めて権利が形成される例であるけれども、身分法上の権利義務であって、その点でサイトブロッキング請求権とは異なる。

プロバイダ責任制限法の発信者情報開示請求権についても、立法当時の議論において裁判上でのみ行使可能な権利とすることが検討されたけれども、実体法上の権利と構成する以上、要件充足の判断が容易な場合においても裁判外で行使を否定する理由がないということで、最終的に裁判外でも行使可能な権利として規定された。

サイトブロッキング請求権を裁判上でのみ行使可能な権利あるいは裁判において初めて形成される権利として位置づけるためには、何らかの意味において裁判所の判断が必要なものであるという理由づけが必要であって、その候補として現段階で考えられるのは、サイトブロッキングというのはサイト運営者のみならず、インターネットユーザーの自由を広く制約するものであり、通信の秘密の侵害に関する正当事由を与えるか否かに関する判断となること。また、インターネットへのアクセスの自由という基本的な権利を制約するものであることから、司法判断が必要と考える。こういった理屈が考えられるのではないか。

なお書きのところで、波及効果を考慮した総合的な検討が必要である。こういったコメントをいただいております。

資料10－１、10－２をごらんいただきたいと思います。こちらが海外事業者を相手方とした発信者情報開示・差止請求ということで、弁護士の神田先生にお話を伺った内容をまとめたものでございます。クラウドフレアということで特定の名前が出ておりますけれども、クラウドフレアに対する発信者情報開示請求ということで、神田先生、自分としてはやはりまず考えられるのは、サイト管理者の連絡先を調査し、わからない場合はサーバー管理者の連絡先を調査する。サーバー管理者のIPアドレスとしてクラウドフレアのIPアドレスが表示された場合には、クラウドフレアに対する発信者情報開示請求の仮処分を申し立てるだろう。

その下に､海賊版サイトは大規模なものに関しては通信量を考慮するとCDNを利用することは必須であって、クラウドフレアという名前が出てくることが多い。以下、クラウドフレアに対する請求を想定してと書いてあります。

発信者情報開示請求は裁判外でも可能ですので、まずは裁判外での請求を考えるけれども、ただし、神田先生の経験上、１年前くらいまでは裁判外で情報開示に応じてくれていたけれども、それ以降はどうも応じてくれないので、裁判所を通じた手続を考える必要があるのではないか。

仮処分により発信者情報開示請求を行うことを想定すると、クラウドフレアはアメリカにある事業者ですので、準拠法と裁判管轄の問題というのが出てくる。ただ、これに関しましては、また後ほど法務省さんからも御説明があるかと思いますが、一定の要件のもとでクリアできると考えている。

下から２つ目の黒ポツですが、準拠法と管轄の問題がクリアできた場合、次は呼び出しと決定正本の送達の問題が出てくる。一般に海外の小規模な事業者を相手方にする場合は、なかなかそれが届かない。呼び出しに応じるかどうかという問題が出てくるのですが、クラウドフレアに関しては最近、日本語のウエブサイトが出てきたとか、いろいろな状況に鑑みると呼び出しに応じてくる可能性はある。仮に手続に対応してきた場合には、うまく仮処分の認容決定が出せれば内容に従うのではないかと考えているので、仮処分を申し立ててみる価値はある。

２ページ、そのときの時間としては名誉棄損とかプライバシー侵害に関するものをもとにして考えると、およそ１カ月なのではないか。もう少しかかるかもしれないけれども、大体そのくらいである。

２ポツですが、開示を求めるべき情報についてということで、仮にそれができそうだということになったときに、何を開示請求すべきかという問題がある。クラウドフレアとして持っていそうな情報ということなのですが、海賊版サイトのコンテンツが蔵置されたホスティングサーバーに関する情報と、サイト運営者の情報を保有している可能性がある。ホスティングサーバーに関する情報については、仮に開示されたとしてもさらに運営者の情報は何なのでしょう、運営者は誰なのでしょうかという請求を行う２段階の手続が必要である。もしホスティングサーバーが日本企業でないとなかなか応じてくれないだろうということもあり、①だけではなく②も同時に請求すべきと考えられる。②というのはサイト運営者の情報を請求してみる。

ではクラウドフレアがどういう情報を持っていそうかということに関してなのですが、日本企業が代理店としてあるので、そちらのほうで何か情報を得ている場合、そして、日本国内で契約を締結していて、代理店が何らかの正確な情報を保有している場合は、それを請求してみることが考えられる。

ただし、代理店経由ではなくてサイトからも契約の申し込みが受けられることになっていまして、クラウドフレアが運営者から匿名あるいはアカウント名を偽名にした形で申し込んでいるとすると、信用できる情報としてはサイト運営者のメールアドレスか、利用料を支払うためのクレジットカード情報か、あるいは申し込みを行った際のアクセス記録ぐらいしかないのではないか。このうちクレジットカード情報については、現在のプロバイダ責任制限法と発信者情報を定める省令の規定により、開示対象となる情報に含まれていないので請求ができない。そして、申し込みを行った際のアクセス記録やログインIPアドレスについても、厳密には侵害行為を行った際のアクセス記録ではないので、開示請求が認められるかが不確定でわからない。これまでの裁判例で言うと棄却される例も多い。

さらにメールアドレスについては、Gmailなどのフリーアドレスかどうかを問わず、民事の手続では保有者は特定できないという問題がある。そのメールアドレスにつきましては、発信者のものについて開示請求が認められていますけれども、コンテンツプロバイダ、サイト管理者ですとかホスティングプロバイダのメールアドレスについては、開示が認めら

れていない問題もある。発信者について開示請求をするのであれば、仮処分ではなく本案訴訟を提起する必要があるのだけれども、今の裁判所の実務で言うと恐らく８カ月ほどかかるのではないか。その間に被害が拡大してしまう可能性がある。いろいろと不確実な点が多いということで書いております。

３ポツは簡単に申し上げますが、クラウドフレアが裁判手続に対応してこない可能性が高いということが、特に海外の小規模の事業者であって日本でのビジネス展開をそんなに真剣に考えていない事業者の場合、通常は対応してこないということですので、そういった点でも少し不確定なところが大きいということが書いてございます。

その場合でも４ページの上から２つ目にありますように、仮処分決定書というものをGoogleに提出した場合テイクダウンしてくれるということで、先ほども少し申し上げましたけれども、侵害情報があると認めたURLについて、Googleの運用で検索結果から落としてくれるということはできるだろうということもおっしゃっていました。

４ポツがクラウドフレアに対する著作権法112条に基づく差止請求の可能性ということで少しコメントをいただいておりますが、名誉棄損とかプライバシー侵害の場合にコンテンツプロバイダに削除請求を行うことがよく行われているのだけれども、これは裁判実務として客観的にそのプロバイダが名誉等を侵害していると評価しても差し支えないという運用、そういった判断が定着しているというのがある。これに対してインターネット上での著作権侵害については、そういった解釈というのは定着していないということで差止請求が認められるかどうかは不透明である。これに関しては一部の実務家、研究者がいわゆるカラオケ法理により認められるのではないかという可能性、あるいは112条準用により差止請求を認める可能性というのも主張されていますけれども、現時点で実務上、定着しているものではないのではないかというのが見解でございます。

ということで神田先生としては、現在の状況に鑑みると、海賊版サイト対策としてはできる範囲で発信者情報開示請求を優先すべきである。

まとめですけれども、以上のとおりということで、クラウドフレアが日本での裁判所を通じた手続に対応してこない場合、発信者情報開示請求の実効性に問題があるということもありますし、対応してくれたとしても、どの程度正しい情報を保有しているかという問題もあるということがございまして、ただ、対応してくれる可能性がないわけではないので、行ってみる価値はあるのではないか。

その他ということで、プロバイダ責任制限法あるいは省令を改正し、ログイン情報からの発信者特定を認めたり、クレジットカードの名義情報など、発信者の特定につながる情報を対象とすることも検討してはどうか。あるいは最近はWHOISのプロテクトが主流となっていて、ドメイン名の登録者情報が得にくくなっているので、レジストラを開示関係役務提供者に含めて開示義務を負わせるなどという御対応も考えられるのではないかというコメントをいただいております。

資料11が通信事業から見た効果的な海賊版対策ということで、日本IT団体連盟からいた

だいた御提案でございます。

簡潔に申し上げますと、いろいろなブロッキング以外の対策を検討することが不可欠である。技術的な対応の検討についてブロッキングというのは有効性に著しく欠け、オペレーションミスが発生した場合の損害が甚大である。憲法上、刑法上、電気通信事業法上の諸課題があるということで、ブロッキングにかえてアクセス集中方式の手段を検討することを提案したいということで、御提案をいただいております。

下に対比の表がございますので、そちらをごらんいただければと思うのですが、権利者本人が正当防衛の適用もあり得るということでアクセスを海賊版サイトに集中させる。これによって違法者の侵害行為をやめさせるということが考えられるのではないかという御提案でございます。

最後に、２ページ目の一番下の段落のところにありますけれども、効果的なアクセス集中手段の実装については、技術的支援を行っていくことを望んでおりますという言葉もいただいております。

ということで、私からヒアリングの結果についての御説明は長くなりましたけれども、以上でございます。

続きまして､各省庁から基本的な法制度運用について御説明をいただきたいと思います。まず総務省からお願いできますでしょうか。

○総務省中溝課長　総務省消費者行政二課長の中溝でございます。よろしくお願い申し上げます。

急な差しかえだったので資料番号がついておりませんけれども、資料４「電気通信事業法及び通信（信書等を含む）の秘密」と名前がついている資料をごらんください。まず私のほうからこれに基づいて通信の秘密について御説明をいたします。

通信の秘密については、前回の第４回会合において宍戸先生から、憲法の観点から通信の秘密の意義等についても大変詳細な御説明がありました。その宍戸先生を前に御説明をするのは大変恐れ多いところではありますが、御指示ということですので、当方から電気通信事業法を所管する立場からということで、電気通信事業法における通信の秘密の保護の意義等について説明をいたします。

まず表紙をおめくりいただきまして１ページ目をごらんください｡冒頭ありますとおり、通信の秘密というのは、日本国憲法第21条において表現の自由の保障と並んで規定されております｡それを受けて電気通信事業法第４条及び第179条の罰則において規定が定められております。

まず電気通信事業において通信の秘密を保護する意義、つまり通信の秘密を保護するのは何のためなのかということについての御説明でございます。通信の秘密を確保するということ、つまり通信のユーザーが自分の通信の中身を誰からも見られないという安心感を持てることで、初めてユーザーは安心して例えば自分の連絡したい相手とコミュニケーションをとる。自分のいろいろな考えを伝えることができたり、あるいは自分の知りたい情

報、見たいサイトへのアクセスをして情報を収集する。例えば自分の趣味趣向あるいは思想・信条や宗教にかかわる情報などを集めたりすることが可能になります。

また、そのためにも通信を媒介する電気通信事業者による通信の秘密の厳格な取り扱いの確保というのは、大変重要になっております。自分の通信の中身を勝手に電気通信事業者が見たり、あるいはみだりに漏らしたりしないという電気通信事業者あるいは電気通信サービス、インフラに対する信頼があって、初めて電気通信サービスの利用が促進されることが可能になるということでございまして、つまり通信の秘密を保護するのは何の目的かといいますと、ここにある「表現の自由」や「知る権利」を実効的に保障するというのが１つ目の目的であり、第２に、これは同じことを裏から言っているだけかもしれませんが、電気通信事業法の目的である電気通信の健全な発展、国民の利便の確保を図るためということでございまして、つまり通信の秘密の厳格な取り扱いの確保というのは、電気通信事業の存立の根幹とも言うべきものと考えております。

そこで、電気通信事業者による通信の秘密の厳格な取り扱いを確保するための仕組みといいますか、担保するための措置ということで、主として以下３つのものがございます。

１つ目が通信の秘密の侵害に対する罰則規定でございまして、これは誰でも通信の秘密を侵害した場合には罰則が適用されるわけでございますけれども、電気通信事業者が通信の秘密を侵した場合には、より重い罰則規定が適用されます。この罰則というのは、電気通信事業法で定めているあらゆる罰則の中で最も重い量刑になっているものでございます。

２つ目が、総務大臣による業務改善命令というものがございます。

３つ目が、通信の秘密に属する事項の取り扱いについての指針ということで、下に書いてあります例えば電気通信事業における個人情報保護に関するガイドラインなどの指針を総務省において作成して、各事業者にその指針を踏まえた取り扱いを指導しているということでございます。

２ページ目は電気通信事業法等の条文の抜粋でございますが、該当部分は下線赤字にしておりますので、適宜御参照いただければと思います。

３ページ目に、通信の秘密に属する事項、通信の秘密の侵害の３類型などを示しております。これらの事項を先ほど御説明しましたガイドライン等あるいはその解説などに記述することで､各電気通信事業者による適切な取り扱いを確保しているところでございます。

１つ目として通信の秘密の範囲、ここに①、②とございますけれども、通信の秘密というのは通信の内容のほかに、その通信の日時、場所、当事者氏名、住所、電話番号なども含まれるということで解釈しております。

また、「２．通信の秘密の侵害」というのは、ここに３つの類型がございます。１つ目は知得ということで、通信の秘密を知ろうという意思のもとで知り得る状態に置く。窃用というのは発信者、受信者の意思に反して利用する。あるいは漏えいということで他人が知られる状態に置く、情報を漏らす。この３点のいずれかに該当すれば、通信の秘密の侵害になるということでございます。

これを今、議論になっておりますサイトブロッキングとの関係で言いますと、プロバイダはサイトブロッキングをしようとする意思のもとで通信の行き先をチェックする。すなわち知得する。知得した上で、また悪質なサイトへのアクセスを試みる通信の場合には、これをブロックする。つまり、ユーザーの意思に反して利用するという窃用に該当するということでございますので、通信の秘密を侵害する行為になるということだと考えられます。

３つ目は、通信の秘密の侵害の違法性阻却事由ということでございまして、ここにございますとおり、通信の秘密というのは非常に重いものではありますが、絶対不可侵ということではなくて、本人の有効な同意がある場合。その他、違法性阻却事由がある場合には阻却されると考えられます。ただ、その通信の秘密の意義を考えれば、違法性阻却事由により許容されるのは限定的なケースに限られるものと考えております。

ここに例示がございます。まず有効な同意がある場合としては、これは契約者や保護者の申し込みに基づいて、プロバイダ等がフィルタリングサービスを提供する場合が考えられます。また、法令行為としては違法性が阻却されるケースとしては、例えば裁判所が発する令状などに基づいて、犯罪に用いられた通信の履歴とプロバイダが捜査機関に開示するといった場合が当たるということでございます。正当業務行為はここにありますとおり、料金精算のために通信履歴を活用する場合。正当防衛、緊急避難については人命救助とありますが、ちょうど昔の例になりますが、例えば身代金要求のための脅迫電話がかかってきた。その発信元を逆探知して捜査機関に開示するみたいな場合は該当し得ると考えられます。

ここで１つ、サイトブロッキングというものとフィルタリングサービスというものがよく同じような形ではないかという議論がありますけれども、フィルタリングサービスはここにあるとおり、有効な同意のもとでの提供ということでございますので、フィルタリングサービスとサイトブロッキングを一緒くたに議論すると非常に混乱を招くと通信の秘密の整理との関係では考えておりますので、その点は十分整理した上で御議論いただければと考えております。

４ページ、こちらがサイトブロッキングのイメージ図ということで、通信の秘密の侵害というのはどういう形で行われることになるのかという図でございます。右側にユーザーＡとかユーザーＢ、これはプロバイダＸに加入している加入者、ユーザーＣやＤはプロバイダＹに加入している事業者でございます。左に問題のない正規のサイトα、β、そして海賊版サイトγがあったといたします。これをサイトブロッキングしようとした場合、プロバイダＸはユーザーＡがまずどこにアクセスしようとしているのかというのをチェックして、αにアクセスしようとしていればオーケー、βにアクセスしようとしていればオーケー、γにアクセスしようとしていたらだめ。あるいはユーザーＢのように海賊版サイトにアクセスしないケースであっても内容、行き先をチェックしてオーケーかどうか判断するという形で、結局、各プロバイダが加入する全てのユーザーの全ての通信の行き先をチ

ェックすることになりますので、通信の秘密との関係では非常に影響が大きいということでございます。

なお、この後の資料は、私は第４回からの参加となっておりまして、第１回タスクフォース会合に出席しておりませんが、第１回会合において信書の秘密に関連する御議論があったとお聞きしておりますので、御参考までにその運用や判例について資料をおつけしたものでございますが、基本的には信書の秘密についてもこれまで御説明した通信の秘密と同様に、違法性阻却事由は限定的なケースに限って該当するという厳格な解釈運用がなされておりまして、また、関税法第76条では郵便物の水際差し止めのための税関検査というものは、郵便物中にある信書以外のものを対象とする旨が定められております。

札幌税関検査事件の凡例において、差し止めの対象となった郵便物についても信書ではなかったということでございますので、知財侵害品が含まれる郵便物の水際差し止めがふえているということではございますけれども、信書の秘密侵害が許容されるようになっているというわけではないということでございます。

以上が通信の秘密に関する御説明でございます。

続いて、資料５－１に基づきまして「プロバイダ責任制限法の運用」についての御説明をさせていただきます。

１ページ目はプロバイダ責任制限法の概要を１枚にしてまとめたものでございますが、大きく２つのことを定めた法律でございまして、１つが第３条のプロバイダ等の面積要件の明確化、もう一つが第４条の発信者情報開示請求になります。次のページからそれぞれの概要を御説明いたします。

２ページ目、プロバイダの免責要件の明確化についての概要でございますが、こちらインターネット上のウエブページや電子掲示板に何か権利侵害情報が書き込まれたりする場合、その書き込まれた権利侵害情報によって生じる被害者の責任というのは、一義的には書き込みをした本人、アップロードした本人が負うのは当然でございますが、そのページを管理するプロバイダも削除しなかったこと等によって不作為の責任を被害者から問われるおそれがございます。逆に、削除等をした場合には、アップロードをした加入者等から契約不履行などの責任を問われるおそれがあるという立場にございます。

そこで削除しないことによる不作為責任を問われるのを恐れて、権利侵害情報でないものまでも含めて過度に書き込みを削除してしまうことになれば、表現の自由に対する大きな制約になり得ます。逆に削除等をすることによる債務不履行等の責任を問われることを恐れて、削除をちゅうちょし過ぎることになれば権利侵害を拡大させることになりますので、どちらの場合についても損害賠償を負うかもしれないプロバイダの免責要件を明確化することによって、また、その責任範囲を制限することによって、プロバイダ等による適切な対応を促すことを目的としたのがこの第３条の規定でございます。

つまり、上に書いてありますとおり、プロバイダ責任制限法は何か削除義務というものを定めたものではない。適切な対応を促すためのものでありますとともに、削除請求権的

なものを定めたものではございません。また、プロバイダ等による常時監視義務を規定したものでもなくて、プロバイダ等が被害者等からの申告によって違法情報が流れていることを知った場合に、適切な対応をとることを促すための規定ということでございます。

３ページは発信者情報開示に関する概要でございます。こちらも繰り返しになりますが、ウエブページや電子掲示板等に権利侵害情報が書き込まれたりした場合、アップロードされた場合、責任を負うのは書き込んだ本人、発信者でございます。したがって、被害者は自分の救済のために発信者を相手取っていろいろ責任追及等を行うことが基本になりますけれども、先ほどの御説明のとおり、誰が書き込んだかがわからないという状況でございます。

そこで損害賠償請求などの責任追及はできないということで、一方でプロバイダ等はアップロードした者が誰であるかといったこと、あるいはどこからアップロードされたかの手がかかりとなる送信元のIPアドレスなどの発信者情報を有している場合が多いと考えられます。そこで被害回復の手段として、加害者を特定して損害賠償請求等を行えるようにするために、被害者がプロバイダ等に対してこれら発信者情報の開示を請求することを可能としたものが、ここの規定でございます。

ただ、発信者情報というものは、発信者のプライバシーですとか匿名表現の自由あるいは通信の秘密として保護されるべき情報でありますので、本来、プロバイダは正当な理由なく開示することは認められないというものでございまして、むやみに開示すれば通信の秘密侵害の責任を問われることにもなり得るということでございまして、一定の厳格な要件が満たされる場合に限って、これはその第１項で２つの要件が具体的に定められておりますが、１つ目に権利侵害が明らかである。２つ目に開示を受けるべき損害賠償等の訴訟を行うため等で開示を受けるべき正当な理由がある場合に限って、プロバイダ等が正当行為として発信者情報を開示できるようにするものでございます。もしプロバイダ等が開示請求に応じない場合には、被害者はプロバイダ等を相手取って開示請求の訴えを裁判所に提起することができるというのが４条でございます。

４ページ、これはプロバイダ責任制限法が想定しているプロバイダ等がどこにいるのかを御説明するためのイメージ図になります。図の左の侵害者が、プロバイダＺが管理するサイトに権利侵害コンテンツをアップロードしたことを想定した図でございますけれども、この場合、被害者から権利侵害情報の削除申し出を受けて責任を問われる可能性があるのは、そのサーバーを管理するプロバイダＺとなります。プロバイダ責任制限法が想定しているのは、このように責任を問われる可能性があるＺのようなプロバイダになります。

一方、右の図のプロバイダＸやＹは、そもそも責任を問われる可能性がない、責任を負い得る立場にないということで、プロバイダ責任制限法が想定する対象のプロバイダではないということでございますが、今回のサイトブロッキングの実施対象となるのは赤枠で囲ったとおり、プロバイダＸやＹでございますので、サイトの削除というものと、サイトブロッキングでは実施する措置ももちろん違いますけれども、その実施主体となるプロバ

イダも全く異なるということでございます。

この後、資料５－２については、プロバイダ責任制限法の条文を全て参考までにおつけしておりますので、適宜ごらんいただければと思います。

プロバイダ責任制限法についての説明は以上になります。

○岸本参事官　ありがとうございました。

続きまして、警察庁から海賊版サイトの状況と課題ということでお話をお願いいたします。

○警察庁鈴木管理官　警察庁の生活安全局生活経済対策管理官の鈴木でございます。

著作権法と知的財産侵害事案の取り締まりを所掌する部門でございますので、簡単に御説明させていただきます。

まず海賊版サイト等の検挙状況についてでありますけれども、平成29年中、昨年中、警察では海賊版事犯を含む著作権侵害事犯を事件数にして172事件、人員にして207人を検挙しております。そのうちインターネットを利用した事犯というものが153事件、165人ということで、かなりの割合をインターネット利用事案が占めているところでございます。

海賊版サイトというものの検挙事件数については、これは網羅的に把握しているわけではないのですけれども、実例を挙げますと、これはいずれも報道されている例でございますが、昨年、検挙した事例として１つ、いわゆるネタバレサイト事件というものでありまして、これは被疑者５名が発売前の漫画雑誌に連載中の画像、セリフを著作権者の許諾を得ないまま自身が運営する海外サイトに連載していた著作権法違反の事件。もう一つ、いわゆる「はるか夢の址」事件と言われているものですけれども、被疑者９名が市販されている漫画及び雑誌のデジタルデータを、自身が運営するサイトに掲載していた著作権法違反事件でございます。

先般、お尋ねがありました捜査上の課題、いわゆる困難性ということについて、これにつきましては捜査上の困難性について公にしますと、今後の捜査に支障が生じるおそれがあることからお答えいたしかねるということなのですが、ただ、この検討会議の中で既に権利者側から御指摘がありましたとおり、つまり権利者の方が海賊版サイトの運営者を探索する際の障害として挙げられている様々な問題は当然、捜査にも同様の影響をもたらすものだと認識しております。

いろいろと問題点はあるのですけれども、警察としては今後とも著作権法等に定める刑罰法令に違反する行為が認められれば、法と証拠に基づき適切に対処していく所存でございます。

もう一点、犯罪捜査と権利侵害行為の停止、例えば違法サイトの遮断、閉鎖というものについては、一応、別のものであるという点について１点、申し添えます。というのは被疑者を検挙しても違法サイトによる権利侵害行為がとまるかどうかというと、必ずとまるとは限らないということであります。以前こちらの検討会議でも事例として出されていましたが、ブラジルのAnitubeというサイトについてはブラジル警察が摘発したけれども、と

まらなかったといった事例が紹介されていました。

国内の事件では、大体捜査を契機として被疑者またはプロバイダがサイトを削除しているということだと思いますが、捜査をして被疑者を検挙すれば必ず違法サイトがとまるというものでもないという点、ここは一応そういうこともありますということを申し添えたいと思います。

いずれにしろ警察として今後とも関係機関等と連携しながら、こうした悪質事犯の取り締まりには努めてまいりたいと思っております。

○岸本参事官　ありがとうございました。

続きまして、文化庁から御説明をお願いいたします。

○文化庁水田課長　文化庁著作権課長の水田でございます。

資料６と資料７をごらんいただければと思います。まず資料６「著作権等の侵害行為及び『侵害とみなす行為』について」ということでございました。

「１．概要」をごらんください。著作権法につきましては著作者、実演家、レコード製作者、放送事業者、有線放送事業者、こういった方々の財産権として著作権または著作隣接権を定めております。例えば具体的には複製権とか公衆送信権といった権利でございますが、これらについて権利者の許諾なく著作物を利用する行為が、権利制限の適用がない限りは著作権等を侵害する行為となります。さらに著作者や実演家について人格権というものもございます。著作者人格権及び実演家人格権、これらの意に反する著作物や実演の改変等は、これらの人格権を侵害する行為となります。

これらに加えまして、著作権法第113条では、著作権法が定めます著作者人格権、著作権、出版権、実演家人格権、または著作隣接権の侵害行為には基本的に該当しないけれども、著作者・実演家の人格的利益や著作権者・出版権者・著作隣接権者の経済的利益を害することとなる一定の行為について侵害行為とみなし、こういった形で権利者の保護を図っております。

具体例が下にございます。例えば１つ目の外国で作成された海賊版を国内において頒布する目的をもって輸入する行為。これは具体的な著作権の支分権に該当していないわけで、輸入権というのはないのですが、こういった輸入する行為をみなし侵害としているものでございます。２つ目の海賊版を海賊版と知りながら頒布し、頒布の目的をもって所持し、もしくは頒布する旨の申し出をし、または業として輸出し、もしくは業としての輸出の目的をもって所持する行為。これは持っているとか、普通に一般的な著作者の権利としては個別の侵害に該当しないものなのですが、これもみなし侵害としているものでございます。

また、３つ目の海賊版のコンピューター・プログラムを、使用権限を取得したときにおいて海賊版と知りながら業務上電子計算機において使用する行為。ここでも別に複製とかではなくて、ただ使うというだけではあるのですが、特別な規定を置いているというものでございます。

他にも権利管理情報ですとか、そういったものにつきまして幾つかこういったみなし侵

害の規定を置いているところでございます。

２ページの「２．侵害行為に対する救済」をごらんください。上の２つのパラグラフは、一般的な著作権侵害でございます。著作権侵害につきましては民事責任を負うこととなります。権利者ですけれども、著作権法112条１項に基づく差し止め請求、それから、民法709条に基づきます損害賠償請求を民事上は被害者は行うことができる。一方、刑事罰につきましては、著作権法119条１項及び第２項第１号におきまして刑事罰の対象とされております。

みなし侵害につきましても第３パラグラフと第４パラグラフですけれども、同様の扱いとなっております。参照条文は３ページと４ページをごらんいただければと思います。

資料７は、「違法配信からの私的使用目的の録音録画の違法化について」ということでございます。静止画ダウンロードが私的使用目的の複製に係る権利制限の除外対象とならなかった経緯について簡単に御説明いたします。

１つ目の○にございますように、平成21年１月に取りまとめられました文化審議会著作権分科会の報告書に基づきまして、平成21年の著作権法改正によりまして、著作権等を侵害する自動公衆送信を受信して行うデジタル方式の録音または録画、これをその事実を知りながら行う場合に、私的使用目的の複製に係る権利制限の対象外とされております。これは違法という形にされたということであります。このときは民事での措置のみだったのですが、括弧内にございますように、平成24年の著作権法改正時に内閣提出法案に対する修正が国会でございまして、このうち有償著作物等に係るものが刑事罰の対象とされました。

録音録画以外の著作物の私的複製につきましては、この報告書の中の部分を引用させていただきますけれども、一部のプログラムの著作物を除いて、特に要望や複製実態についての報告が寄せられていなかったということで、複製の実態を勘案しながら、また、利用者に混乱を生じさせないとの観点にも配慮して、検討の熟度に応じて段階的に取り扱いを判断していくことを視野に入れつつ、引き続き検討を行っていくことが適当とされているところでございます。

なお、録音録画の部分が違法化されているということでございますが、例えば現在で言うとストリーミングみたいなものは視聴ということですので、そこは現在も違法ではないという扱いとなっています。

以上でございます。

○岸本参事官　ありがとうございました。

それでは、最後に法務省から御説明をお願いいたします。

○法務省内野参事官　法務省民事局の参事官の内野でございます。よろしくお願いいたします。

この検討会におきましては、しばしば国際的な要素を有する事項について取り上げられることがあり、今日も関係省庁の皆様方からの御説明の中に、不法行為という部分につい

ての民事責任に触れる点もございました。そこで本日は、知財事務局から、そういった御議論の前提となります知識を共有するという観点から、国際的な要素を有する裁判事件における国際裁判管轄というものと、準拠法に関して一般的な御説明をしてほしいとのご依頼を受けましたので、御説明申し上げたいと思っております。

まず国際裁判管轄でございます。資料８をご覧いただきながらになりますが、国際的な要素を有する裁判事件、例えば被告になるべき者が外国に住所を有するという場合には、日本の裁判所でその事件を審理、裁判をすることができるのかということが問題になります。これを国際裁判管轄の問題と呼んでおります。

個別的な具体的な事案におきまして、日本の裁判所が国際裁判管轄を有するかどうかというのは、最終的にはその事案における裁判所の判断となりますので、法務省といたしましてその有無というものを網羅的に御説明することは、なかなか困難なところがあるのですが、現在の民事訴訟法における規律の概要を御紹介したいと思います。

第１に、まず民事訴訟法第３条の２によりますれば、日本の裁判所は被告の住所が日本国内にあるときには、その事件について管轄権を有するとされております。そのため、例えば原告に対して不法行為をした被告が日本に住んでいるといったような事情がある場合には、原告はその不法行為があった地が日本国内であるかどうかにかかわらず、例えば、日本の裁判所においてその不法行為に基づく損害賠償請求の訴えを提起することができるといった規律になります。

それに加えまして、先ほど資料10－２にも若干御紹介がありましたが、民事訴訟法第３条の３の第８号によりますれば、不法行為に関する訴えは、不法行為があった地が日本国内にあるときは、被告が外国に住んでいたとしても、原則として日本の裁判所にその訴えを提起することができるものとされております。どういった場合にこの要件を満たすかにつきましては、最終的には個別の事案における裁判所の判断となりますけれども、一般論として申し上げれば、例えばこの不法行為に関する訴えというものにつきましては、知的財産権の侵害に基づく損害賠償請求事件及び差止請求事件が含まれると解釈されておりまして、また、一般にこの不法行為があった地というのは加害行為が行われた地と結果が発生した地の双方が含まれると解釈されております。ですので、これに対する当てはめが個別の事案では問われることになります。

もっとも、民事訴訟法第３条の３第８号の括弧書きによりますれば、不法行為の結果が発生した地が日本国内であったといたしましても、行為が行われた地が外国であって、日本国内におけるその結果の発生が通常予見することができないというものであれば、日本の裁判所の国際裁判管轄は認められないこととされております。国際的な要素を有する不法行為の裁判事件というものにつきまして、どのような場合にこれに当てはまるのかというのが具体的な事件では問題になり、それが裁判所の判断に委ねられているという現状であります。

次に、準拠法についてでございます。国際的な要素を有する法律関係について、どのよ

うな場合にどの国の法令が適用されるのかという点が問題になりまして、この問題を取り扱う法律といたしまして、法の適用に関する通則法というものがございます。この通則法の定めるルールに従って適用される法のことを準拠法と呼んでおります。本日お配りされております資料の中にも準拠法という言葉が出てまいりますが、これはまさにこれらの通則法などの国際私法によって定められる準拠するべき法律を準拠法と呼んでおるわけであります。

先ほどの国際裁判管轄の御説明と同様に、特定の具体的事案を念頭に置いた場合に日本の法律の適用の有無を確定的、網羅的に御説明するというのは、なかなか困難なところがあるわけでございますが、この準拠法選択の一般的なルールといたしまして今、申し上げました通則法がございますので、この規律の内容を御紹介いたします。

第１に､通則法第17条によりますれば､不法行為によって生ずる債権の成立及び効力は、加害行為がどこで行われたかということにかかわらず、原則として加害行為の結果が発生した地の法によるとされています。その例外といたしまして通則法第17条のただし書きでは､結果の発生地における結果の発生が通常予見することができないものであったときは、加害行為が行われた地の法によると規定しています。

第２に、通則法第17条の規定に従って定める地よりも明らかに密接な関係がある他の地があるときには、通則法第20条によりまして当該他の地の法によるとされています。この密接関連性の有無は、例えば不法行為の当時において当事者が法を同じくする地に住所地を有していたということや、当事者間の契約に基づく義務に反して不法行為が行われたといったような事情がありますれば、そういった事情を総合考慮して判断されるものとされております。

第３に、これらの規律によれば外国法が適用されることとなる場合におきましても、同じく通則法22条第１項におきまして、これを適用すべき事実が日本法によれば不法とならないときは、当該外国法に基づいて損害賠償請求等をすることができないという定めになっております。

このような国際的な要素を有する不法行為につきまして、どのような場合にどの国の法令を適用されるかというのは、こういったような規定を踏まえて準拠法が判断されることになるというのが一般的な規律でございます。このように国際裁判管轄と準拠法という若干性質の異なる問題が、国際的な要素を有する裁判事件については問題になるということでございます。

御説明としては以上でございます。

○岸本参事官　ありがとうございました。

次に、前村委員からブロッキングに関する補足説明をお願いできればと思います。

○前村委員　JPNICの前村でございます。

お手元に資料３、そして、これは傍聴の皆さんには実は回っていないようなのですけれども、ISOCのレポートをカラーコピーしたものが構成員の皆さんにお手元にはお配りされ

ているようです。

こちらのレポートなのですけれども、パブリックに公開されているものでございまして、そのURLは資料３の１ページ目の脚注１にあります。英語なのですが、比較的読みやすくて全部で二十何ページかというドキュメントなのですけれども、一度ごらんいただけるといいのではないかと思います。

この資料３に関しまして説明してまいりたいと思います。

もともと私は第４回までの会合で、ぜひとも勉強会ではこのドキュメントなどを使って技術的な整理をしたほうがいいのではなかろうかと申し上げておりまして、前回の会合では私なぞよりも適切な方に御説明いただくこともと申しておりまして、実は東京大学のISOCの理事もお務めになっていらっしゃいます江崎先生に御説明をお願いしようと思って、資料の作成までお願いしていたのですけれども、構成員からの説明のほうが適切であるということで、今回、私が説明させていただきます。

なお、江崎先生は傍聴人としてお越しいただいていますので、もし御本人に御質問があれば、お答えいただけるかもしれないと思っております。

それでは、資料３の御説明をしてまいります。

まずISOCと申しておりますが、必ずしもすべての皆さんISOCを御存じであるとは思わないので、まずはその説明をさせていただきたいと思います。

インターネットソサエティと申します。法人としては米国バージニア州のチャリティーなのですけれども、事業内容としてはインターネットの普及と高度化を事業内容としています。IETF（Internet Engineering Task Force）という技術標準を策定する団体がありますが、このIETF自体は任意の団体でありまして、そのリーガルアンブレラの機能を果たしているのがISOCであります。技術的な面だけではなくて、政策面においてもアドボカシーを活動としてやっているということなのですけれども、あらゆるステークホルダーによるインターネットに関係する政策の調査と提言を行っているということで、グローバルなインターネットの展開を見ると、こういう技術、運用、政策に関してエキスパートから構成されて、一番権威を持つ団体だと我々としては見ているわけであります。

今回、御紹介しようとしているInternet Society Perspectives on Internet Content Blocking: An Overviewというドキュメントなのですけれども、2017年３月に公開されております。どういうドキュメントかといいますと、これはそこに書いていることを読もうとしているのですが、ISPやキャリアで実施するコンテンツ遮断方法、幾つかありましてIPアドレスベース、DPIベース、URLベース、プラットフォームという言葉を使いますけれども、主に検索エンジンのことであります。検索エンジンベース。そしてDNSベースという５つがあるのですが、それぞれを列挙して、それぞれの技術的な解説と特質を明らかにしたものであります。

資料３には、この原典であるISOCのレポートの中で要約として非常に有効なページが幾つかありまして、21ページに各遮断方法と評価結果の一覧、22ページに結論、そして６ペ

ージはサマリー、オーバービューのほうなのですけれども、コンテンツ遮断による不利益の一覧というものが書いてあります。４ページが非常にサマリーとして有用でしたので、こちらはJPNIC、私どものほうで限られた時間でやりましたので、ちゃんとした訳ではないのですけれども、私訳を提供いたしました。それが２ページ以降に書いてあるものでございます。こちらを少し御説明してまいります。

まず前後いたしますけれども、３ページのほうから。これは21ページにありますContent Blocking Summarizedというもので、端的に列挙した５つのコンテンツ遮断技術に関してそれぞれの技術的な概要、効果、影響範囲、作用のきめ細かさ、種別、副次的な損害の大きさ、一般的な回避策、副作用または技術的な問題というものを、それぞれに列挙して非常に一覧性が高いものになっています。効果のところに一部、非常に効果的な局面もあるという御説明もあるのですけれども、全体として非常にネガティブに効果が少なく、副作用のほうが多いという感じはごらんいただくと見てとれると思います。なお、こちらの訳はそれなりに注意深く訳しましたが、もし御不明な点がある場合には原典をさらっていただいたほうがよろしいかもしれません。

そして、このような分析をもとに５ページを開いていただきますと、このISOCレポートでは22ページ、23ページに示されていますConclusionと言われている結論に関して和訳をしてみました。結論のところでは１、２とありまして、非常に端的にコンテンツ遮断技術によっては問題が解決しない。なぜならば、インターネット上からコンテンツを取り除くわけではないからであると書いてある。もう一つは副次的な被害を引き起こすということで、オーバーブロッキングや逆にアンダーブロッキングという場合もある。また、回避策に走ったユーザーに対して、プライバシー侵害などのほかの被害を引き起こし得るということが指摘されております。

こういった結論をもとに、少し戻っていただきまして２ページには公共政策の観点から見たインターネットコンテンツ遮断に関する主な問題点ということが列挙されておりまして、全部で８ポイント問題点があると指摘しております。ここで公共政策の観点から見たという言葉が並んでいるのはなぜかといいますと、もともとISOCのレポートが公共政策担当者に向けたアセスメント文書であるということであります。つまり、こういった場に非常に適しているドキュメントであるということが言えようかと思います。

それぞれ細に入ってまいりますと少し時間が足らないということもありますので、以降、こういったレポートを通じて、どういった背景で書かれた文章かといいますと、2017年３月ということで比較的最近なのですが、既に各国で法制化を含めてコンテンツのブロッキングというものが実施されていくという状況の中で、ISOCの見解といたしましては、ISPキャリアによるコンテンツの遮断が技術的な有効性に乏しいにもかかわらず、インターネットに対する影響が顕著であるということを憂慮した。その上でこういった技術的なアセスメントレポートをまとめるという動機にその辺がなったということであります。

以下、１から５まで、これは江崎先生が御指摘しているという要約になるのですけれど

も、それぞれこのISOCレポートの内容から引き出されているところが多いということであります。

まず１番目といたしまして、ISPキャリアにおけるコンテンツブロッキングは、幾重にも回避策があって効果が薄いということをまず指摘していますが、この脚注にありますのは、その回避策の典型例でありまして、これはまだ正式な決定として方針立てされているようではないようなのですけれども、代表的なウエブブラウザの１つであるFirefoxにおいては、普通、Firefoxというブラウザが動作するのはパソコンやそういったマシンの上なので、そのマシンのDNSの指定に従うのですが、最近のFirefoxの開発中のバージョンにおいては、システム指定のDNSに従わず、DNS over HTTPS、これは以前の会合でも御説明いたしましたけれども、ウエブ上、http上の暗号化を施したパスの上でDNSの検索を行うという技術です。これによってFirefoxが指定するDNSを参照する方向にある。

つまり、これはもともとローカルのDNSを信用しないということを、この開発の方向性は指し示していまして、こういったものがブラウザで実施されてしまうと、そもそもISPやキャリアでDNSをベースとしたブロッキングをしても、そもそも意味がないということを示しております。これが非常に端的に回避がたやすいということを示しているのではないかと思います。

また、一部ではなく全てのISPやキャリアで対応する必要があるため、非常に大きなコストがかかるということを１番では指摘しております。権利者、侵害者以外の第三者において費用がかかり、かつ、その効果が回避策が非常にたやすいということで著しく悪いということが言えようかと思います。

２番目、利用者における回避策の検索と実装は、悪性コンテンツサイトの検索と発見と同様に容易であるということです。

３番目、インターネットはグローバルに運営されています。そのため、その一部だけに適用されるローカルルールは、グローバルには効果がないということです。仮にローカルな遮断が一時的に功を奏したとしても、つまり功を奏したということなので遮断ができてしまったという暁には、単純に犯罪行為を国内法制では対応できない形、地下化する、巧妙化するというところに追い込んでいくことで、本質的にそのコンテンツを除去するという対応がとりづらくなるということで、結果的に経済的な損失も減らないということが想定されるということです。これは本文書の６ページの表の中の第６項で示されているものでございます。

４点目、アクセス遮断などの措置はあくまで一時的なものであり、それは機敏に手段を変えていくことが必要なのですけれども、法制化された場合には手段の硬直化を招くおそれがある。また、法の網の目をくぐる回避策の連鎖を呼ぶという結果にもなりかねないという指摘をしております。

５点目、有効な対策はコンテンツのテイクダウン、これは23ページのａ項に示されているもの。ウエブブラウザなど利用者システムにおけるアクセス遮断、これはｅ項で示して

あるものなどインターネットの末端における措置､つまりISPやキャリアなどインターネットの中でこういった遮断を行うのではなくて、インターネットの末端、コンテンツ自身のテイクダウンあるいはブラウザの中でフィルターをする、そういった末端における措置が有効。あるいはウエブサイト運用の資金源の根絶、これは広告出稿における対策といったものを指摘していると思いますけれども、こういった技術以外の方策が有効であると５番は指摘しています。

このように法律をつくるということよりも、経済のいろいろなこういった事業にかかわるステークホルダーの協力によって対策していくことが重要だというふうに江崎先生の資料では指摘しているということです。

私からの説明は以上とさせていただきます。どうもありがとうございました。

○岸本参事官　ありがとうございました。

それでは、ここで質疑応答の時間を20分弱とりたいと思います。これまでの説明について皆様から御意見、御質問がございましたら挙手をお願いできますでしょうか。

○川上委員　２点あります。

まずは警察庁の方に御質問したいのですけれども、説明の中で悪質な海外サイトがとられている、なかなか摘発が難しい国、サーバーを分散して置いたりですとか、そういった技術に関しては、捜査においてもコンテンツ会社が実際の違法配信者を突き詰めるのは難しいということと、同様の困難さが捜査の場合もあるというお話でしたけれども、ということはネット上の情報からだと、警察だったらいろいろなIPアドレスの発信者情報などがとれたりとかしてわかったりするような警察側のメリットというのは、基本的にはほぼないという理解でよろしいのかどうかということを確認させていただきたい。

○警察庁鈴木管理官　今おっしゃったように例えばネット上だからわからないというものについては、警察であってもアドバンテージがない部分はあると思います。

○川上委員　警察だったら何でも捜査できると思っている方がたくさんいらっしゃるので、そうではないということをここで確認したかったので、ありがとうございます。

○警察庁鈴木管理官　我々から見ると過大評価されている部分もあるかもしれないなというのは、個人的には思います。余り大っぴらには言えないのですが。

○川上委員　ありがとうございます。

もう一つ、前村さんの説明で指摘させていただきたいのですが、まず今回、資料としてはすごく英文のものを持ってきたり、東大の先生の資料とか添えていたのですが、まずこの資料の内容は非常に不十分だと思います。なぜかといいますと、この中で今、私もちらっと見たのですが、今、焦点になっているDNSブロッキングが有効でないというような議論の英文の内容は、英文なのですが、書いている内容は非常に薄くて、例えばOP53Bについてのことも書かれていませんし、今、言われていた例えばDoHみたいなこととかについても一切触れられていなくて、正直この内容でしたら前回、立石さんが書かれていたまとめのほうがよっぽど中身も濃かったので、はっきり言うとこれは議論の資料としては正直、少な

くとも技術的な中身を議論とする資料としては非常に不十分なものだと思いますけれども、いかがでしょうか。

○前村委員　ありがとうございます。

前回の立石さんの資料は非常によくできていて、あれがすごくわかりやすい中身が図解されていたり何かしてわかりやすくなっているというのは、そのとおりだと思います。

この資料ですけれども、特によくできているなと思うのは、おっしゃるポイントを否定していくわけではないのですが、例えば21ページの全体のサマリーであるとか、こういったところに簡潔なレベルの記述にとどまるとはいえ、それぞれの技術に関して網羅的に書き出してあるというところは、非常にわかりやすいドキュメントになっているのではないかと思います。

○川上委員　なのですが、網羅的に書き出しているのですけれども、その中でDNSブロッキングだけをとって見ても、書かれている議論の内容ははっきり言って全然低いレベルで、正直こんなのが根拠になっているというのが私にはよく理解できないです。

例えばDNSブロッキングでこちらの英文を見ましても、結局、効果がないものというのが、やはり根拠が説明されていないのです。例えばDNSブロッキングがまず非常に難しくてコストがかかるということが一番最初の説明として書かれているのですけれども、現実的には日本国内においては少なくとも児童ポルノでもブロッキングはされているわけです。そういう意味では、少なくとも児童ポルノでできている程度の困難さであるわけで、そのことをもって否定するのは少なくとも日本の場合についてはおかしいと思うのです。

そして、例えばオーバーブロッキングが大きいという指摘がその次に書かれていますが、それに関しても今回、問題になったような漫画村のような違法サイトの場合は、ほぼ全てが違法情報であるサイトで占められているわけで、そうするとこれも今回の議論の根拠にするにはふさわしくないなと。

その他の書かれている記述に関しても、余り今回の件に当てはまるようなことが、少なくともDNSブロッキングにしても私は今ぱっと、見ていませんが、DNSブロッキングの議論でここに書いてあるものは、余り有益なものはないと思います。

○江崎氏　回答させていただいてよろしいですか。東京大学の江崎です。ISOCのボードもしております。

御回答すると、実は立石委員よりもより専門家の者がこの作成にはかかわっております。IETFでインターネットにかかわる全ての技術標準を決めております。そこには当然ながら機器を提供している人たち、それから、ISPを運用している人たち、Googleなどのコンテンツを提供している人たちの運用者、開発者が全て議論した上でのことをやっています。その上でのドキュメントになっている。したがって、おっしゃったような技術の問題というのは全てわかった上でのドキュメントと御理解いただければと思います。

○川上委員　そこに関しては非常に権威主義的な回答だと思っていまして、だとしても書かれている内容はずさんであり、大したことが書いていないというのが私の率直な印象で

す。
○江崎氏　そのようにおっしゃる方がいても、それは不思議ではありませんし、IETFの立場としては､そういう意見が出てくることは大変健全であると理解しております｡つまり、権威を持っているという御指摘ですけれども、権威を持っているがゆえに全ての人たちのステークホルダーの意見を聞くという体制で､このドキュメントは全てつくられています。
○岸本参事官　よろしいでしょうか。どうぞ。
○後藤委員　前村さんの資料の件でございますけれども、前回、私は代案はないのですかというお話をさせていただきまして、今回、このレポートの６ページから弊害の最小化ということで記述されてございます。ａからｅまでということであります。これは至極ごもっともでございまして、特にｅです。「グローバルに考え、ローカルに行動する。ローカルなコンテンツ遮断やフィルタリングは、グローバルに影響する可能性があるものの、一般的にコンテンツ遮断を極力局所的にすることはグローバルへの影響を最小化する」ということで、まずこれがある。そして、後段では「理想的には利用者の末端でブロッキングするのが最も効果的で副次的に被害を最小化する」と書いてあります。
　これで読めることは、まず末端のブロッキングということで、多分これはフィルタリングだと思うのです。このフィルタリングをどう考えるかということが非常に重要でありまして、いわゆるIPフィルタリングが可能になれば、私はかなり効果があると思います。
　ただ、先ほど総務省さんから御案内がありましたように、有効な同意がある場合ということで同意がある場合なのです。ここをどうクリアするかということだと思います。絶対に反対する人、同意しない人がいますから、そうなるとやはり遮断、司法的に裏づけられた接続遮断を考えるべきだと思います。いわゆるIPフィルタリングを他国にない高度なものを求める。さらには司法的な判断に基づく遮断を法的に裏づけることが、私はこのレポートを読んで、現況を含め対応できると思います。
　もう一点、当該３サイト、いつも言っていますけれども、漫画村だけではありません。MioMioやAnitubeもあるのです。Anitubeについてはブラジルで刑事告訴しているのです。これ以上ほかに何があるかということです。MioMioも中国国家版権局に行って行政摘発しているのです。この次に何があるかということなのです。そういうことを考えると、先ほど冒頭に先生からありましたように時間がかかるということもあるので、やはり止血的な方法論を具体的に絞ってIPフィルタリング、それと司法的な接続遮断を考えていくべき時期だと思います。
　以上です。
○岸本参事官　ほかにどなたか。
○宍戸委員　いろいろな人にいろいろなことをお伺いしたいのですが、まず今、後藤さんがおっしゃったことというのは要するに、絶対フィルタリングは受け入れないという人がいる。そして、その人たちが海賊版サイトにアクセスするのをどうしてもとめるために、ほかの大多数のユーザーの通信の秘密の制限をしないと、比較衡量としてやむを得ないと

いうことをおっしゃっているということですね。
○後藤委員　はい。
○宍戸委員　わかりました。そのことについて恐らくここから議論していくことになるのだろう。その比較衡量するための具体的な立法事実になるようなもの、衡量の要素になるものを今、集めている段階なのだろうと私は理解をしております。
その上で、これは事務局にお伺いしても仕方がないのかもしれないので、もしできれば上野先生にぜひ御見解を伺いたいのは、神田先生のペーパーの中でCDNの通信を遮断する。CDNに対して削除要請のようなものを行うのは著作権法112条で今、いけるかどうかということは必ずしも難しいのではないかというお話があり、それで神田先生御自身は厳しいのではないかというふうに思われている。
それから、きょうお配りいただきました神田先生を含むITの弁護士の方々は、これはいける可能性があると思っているということなのですけれども、この点は上野先生の御見解からすると、今、学説というのか、あるいは上野先生が考えるとどういう点が論点になりそうかとか、結論というよりは少し考えの筋道を教えていただきたいのですが、お願いしてもよろしゅうございますでしょうか。
○上野委員　御質問ありがとうございます。
まず、CDN事業者に対する発信者情報開示請求については、私もできるだろうと思います。CDN事業者が他人の通信を媒介等するプロバイダに当たると考えられるからです。
他方、差止請求に関しては、一般論として、そもそもプロバイダに対して、どうやって差止請求するのかが問題になるところです。CDN事業者であればなおのことです。この点は前回の会合でも、森先生に御質問させていただいたわけですが、そのときは、CDN事業者を通常のホスティングプロバイダあるいは掲示板事業者と同じように評価して差止請求できる、というお答えをいただきました。
ただ、今日の資料10-1で、神田先生が、カラオケ法理や112条の類推適用などといった最近の解釈論についても触れられながらも、しかしクラウドフレアに対する差止請求の可能性については「少なくとも現時点で実務上定着しているものではない」とおっしゃっているとおり、日本の著作権法112条によりますと、侵害者に対する差止請求はできるのですが、侵害者と評価できない幇助者に対する差止請求を定めた明文の規定はなく、また、これを認めた裁判例もほぼないことからいたしまして、従来の議論を前提にする限りは、CDN事業者に対する差止請求はなかなか難しいのではないかと考えられるわけです。
もちろん、従来の裁判例でも、動画投稿サイトの運営者に対する差止請求を認めた「TVブレイク」事件というものがあり、これとCDN事業者を同視できればよいのですが、TVブレイクというのは、YouTubeのような通常の動画投稿サイトとは異なりまして、控えめに見ても侵害率が約50%という非常に悪質性が高いものでした。そういう「本来的に著作権を侵害する蓋然性の極めて高いサービス」を提供し、ユーザによる侵害行為をあえて「誘引」するようなことをしておきながら、運営者は、特段の侵害防止措置を講じることなく、侵害

行為を容認し、蔵置したという状況にあり、このことを理由に、裁判所は、運営者が「自ら複製行為を行ったと評価することができる」として、差止請求を認めたという裁判例であります。

そうしますと、そうした侵害を誘引するような動画投稿サイトではない通常の動画投稿サイトの場合に、どういう理屈で差止請求を認めることができるかという点が問題になるところですし、まして、CDN事業者というのは、その具体的内容にもよりますが、動画投稿サイトや掲示板といったプラットフォームを自ら提供するのとは異なり、汎用的・一般的なネットワークインフラを提供しているに過ぎず、さらには、単なるキャッシング事業者だと自称している場合もあると承知しておりますので、そうしたCDN事業者に対して差止請求するというのは、従来の我が国における議論に従う限りは、その是非はともかく、現実としてなかなか容易ではないものと認識しております。そういう意味におきまして、私は、先ほどの資料10-1における神田先生のご指摘と問題意識を共有しておりますし、これは著作権法学でも基本的に同様と思われます。ただ、きょうの資料のうち、資料10-3の意見書では、――ここには神田先生のお名前も入っているのですが――、「CDN事業者に対する送信防止措置を求める裁判・仮処分が可能です」という結論だけ書いてありまして、私としましては、これはどういう意味なんだろうなと思っているところであります。

以上です。

○宍戸委員　そうすると、CDN事業者に対する削除請求が難しいということになると、基本的には発信元をたたく。先ほどの話にあったような閲覧者が見ようとしているときに、閲覧者にインターネットへのアクセスを提供するISPに対する著作権法上の差し止めのようなものもどちらにしろ難しい。後者のほうのことを言ったのですか。

○上野委員　そうですね。CDN事業者につきましては、たとえデータを分散キャッシュしているに過ぎないとしても、違法コンテンツ全体を自ら蔵置しているものと評価して、ぎりぎりホスティングプロバイダと見ることができるかもしれませんので、CDN事業者が、権利者から通知を受けて侵害状態を認識しながらも、あえてその侵害状況を放置しているという状況があれば、当該CDN事業者は侵害者に当たると評価できる可能性があるといたしましても、アクセスプロバイダにつきましては、さすがに侵害行為を自ら行っている者と評価するのは困難ではないかと思います。

そこで、これは前回お話したことですけれども、日本の著作権法112条について、侵害者のみならず侵害幇助者に対する差止請求もできるのだという解釈論をとった上で、アクセスプロバイダも侵害を幇助している者だと評価して、アクセスプロバイダに対する差止請求としてのブロッキング請求を認めることが、現行法の解釈としてできる可能性は皆無ではないわけですが、私個人の考えとしては、それもやはり現状では困難ではないかと考えている次第です。

○岸本参事官　ほかにどなたかいらっしゃいますでしょうか。それでは、瀬尾さん、福井先生の順番でお願いいたします。

○瀬尾委員　私のは簡単です。総務省さんにお伺いしたいのですけれども、勉強会の場ということなので本当に素人っぽいことでお話を伺いたいと思うのですが、通信の秘密の範囲ということについてなのですが、総務省さん資料４の３ページの上に、通信の秘密の範囲ということで、①個別の通信にかかわる通信内容のほか云々とあって、最後に「知られることによって通信の存否や意味内容を推知される事項全てを含む」と書いてありますが、この知られるというのは知覚で、これは人が主体になると思っていいのでしょうか。

例えば蓄積もせず、単純に相手側のアドレスだけを知って通信を機械的に選別して、それを遮断した場合。もちろん蓄積も何もしない。人は知覚できない。ログも残らない。そういう形のブラックボックスの中で相手をすることも知る、誰が知るんですかとか、知れないですよね。これってどういうふうに完全に相手側のところだけを機械的に遮断することも知ることになるのかどうか、私はすごい疑問に思ったので、ぜひ総務省さんにお伺いしたいと思います。

○総務省中溝課長　非常に難しい御質問をいただいたと思っておりますけれども、この場で総務省として今、御質問のあったものが通信の秘密に該当するかどうか、明確にこの場で私はお答えできないと思うのですが、ただ、通信の秘密の範囲を考えるに当たっての基本的な考え方は、１ページ目で申し上げたとおり通信の内容を誰からも見られない、あるいは電気通信事業者がしっかりとそれをもらしたりしないという信頼とか安心を確保するというのが、この法律の通信の秘密の保護という規定を設けた趣旨ですので、その趣旨に照らして今、委員がおっしゃったようなことが通信の秘密の侵害に当たるのかどうかというのが判断されることになろうかと思います。

○瀬尾委員　ではちょっと簡単に。例えばAIがきちんとこれを選別して、ブラックボックス化して、内容がきちんと担保された基準とか国際的な基準があって、そして、そういう機械があった場合は知られていないし、見られていないというふうにしたら、先ほどの２ページ目のところが担保されれば大丈夫かもしれないという理解でしょうかね。

○総務省中溝課長　そこも明確には明言できません。ただ、機械とはいえ結局、人の指示に従って、機械はあくまでも物ですので、管理する人の指示に従ってプログラムが組まれて動作させているということですから、結局そのプログラムをつくる人がその責任を負うということから考えると、一切、機械で何も見られないから直ちに通信の秘密の侵害になる、ならないということは言い切れないのではないかと思います。

○瀬尾委員　わかりました。

○福井委員　福井でございます。御説明いろいろありがとうございました。

私も素人くさい質問になってしまうかもしれないのですが、総務省さんに対してです。

総務省さんは今回、アクセスの遮断は通信の秘密の侵害であると言い切ったように思うのですけれども、他方で諸外国、42カ国でアクセスの遮断がされるときに、通信の秘密の侵害であるという議論がほとんど出てきていなかった。どうもこれが腑に落ちないところがございまして、それで今回の資料の中で郵便法のことを書いていらっしゃるので、素朴

な質問です。皆さんのお手元にはないですが、郵便法には31条という引き受けの際の説明及び開示という条文がありまして、いわゆる郵便会社、引き受けの際に郵便物の内容について差出人に説明を求めることができる。それから、その中に郵便禁制品、これは法律で頒布を禁止されたものが郵便禁制品なのですけれども、これが含まれている疑いがあるときには差出人に対して内容の開示を求めることができる。そして、もし説明の開示がないときには、郵便物の引き受けをしないことができるという規定があるようです。これは先ほどの説明からすると郵便内容、通信内容の知得と、郵便を行うこと以外の目的による利用、つまり窃用のように聞こえるので、通信の秘密の侵害であるけれども、郵便法によって認めている。この理解でよろしいのでしょうか。

○総務省　今の点も含めて、通信の兼ね合いも含めて整理をさせていただきたいと思いますので、大変申しわけないのですが、持ち帰らせていただいて、後日、回答をさせていただきたいと思っております。

○福井委員　お答えをお待ちしております。

○岸本参事官　先ほど失礼しました。森先生も挙手されていましたか。

○森委員　先ほどのCDNの削除できるかという話のところは、掲示板で削除できていないものもあるかもしれないのですけれども、できているものがあるので、私としては克服された議論なのかと思っていました。いずれ御紹介する機会があると思います。

お尋ねをしたいのは警察庁さんなのですが、資料10－１、神田先生の資料ですけれども、先ほど捜査方法に限界があるのではないかということではありましたが、神田先生はクラウドフレアに対して発信者情報開示請求だということでいろいろ頑張って、その場合分けをして書いていただいているのですけれども、こういうものについては民事でやろうとするとなかなか大変なのですが、これは令状でとることができるのではないかということが御質問の１つ目です。

もう一つは、お話にあったかどうなのかあれなのですが、日本の広告が張られているような海賊版サイトの場合、サイト上の情報から広告配信事業者のドメインがわかるのではないかと思いますので、そこから広告の取引をたどって管理者を検挙することに至るという方法があるのではないかと思ったのですが、それはいかがでしょうか。２点お願いしたいと思います。

○警察庁鈴木管理官　まず個別の事案にもよると思いますので一概には言えないかもしれません。先ほど検挙事例なども一部御紹介させていただきましたが、当然ながら警察が捜査している中で検挙に至るものもあれば、残念ながら検挙に至らないものもあるというのがまず一般の話でありまして、今おっしゃった令状によればわかるのではないかというのは、当然、令状を示す相手がいて、情報がとれる場合というのはとれると思います。ですから恐らく国内であればほとんど何らかできるのではないかと思いますが、以前も問題になっておりましたが、例えば相手が外国にいるような場合に、そもそも日本の令状というものが通用しない場合が当然あろうかなと思います。もちろんできる範囲のことはなるべ

くやっているはずですので､それでもできないものは残念ながらあるのだろうと思います。

それから、今おっしゃったように広告の関係でたどれるのではないか。これも多分、事件にもよると思いますけれども、そういう捜査もやっているのではないかと思います。御指摘された部分について確かにできるものはあると思いますけれども、ただ、全てができるわけではないという、全然答えになっていないかもしれませんが、そういうものが実態だろうと思います。

○岸本参事官　もうそろそろ時間ですので、林先生と前村さんでこの質問は一旦、区切りをつけたいと思います。お願いいたします。

○林委員　私も総務省様の資料４について質問をさせていただきます。

４ページ目のところで、「サイトブロッキングの実施のためには、各プロバイダが加入する全てのユーザーの全ての通信の宛先を網羅的に確認することが必要。」だから「→海賊版サイトへアクセスしようとする者のみならず、加入する全てのユーザーの通信の秘密を侵害。」と書いてあるのですけれども、これはその前のページの３ページにある通信の秘密の侵害のうちの知得、窃用という類型で言いますと、どちらに当たると考えていらっしゃるのか。すなわち先ほども御質問がありましたが、宛名解決の情報を通信履歴と同様に機械的に記録されたもの、これを「確認」と理解するとしますと、これも「知得」とお考えなのかどうか。

その場合に児童ポルノについてもフィルタリングを今されているわけですが、全ユーザーの全通信の宛先を網羅的に確認しているのだけれども、これも通信の秘密の侵害のうちの「知得」に当たるとお考えなのか。また、児童ポルノについて緊急避難ということでこれまでブロッキングをされているわけですが､この取り組みは非常に皆さん御苦労されて、これまで続けられてきたということで非常に敬意を表するところなのですが、その緊急避難という取り組みについて、総務省として今日まで立法に至らなかったのはなぜなのか。

また、知得ではなくて窃用の問題だと考えた場合には、窃用に当たるというのは、宛名解決のため全ユーザーからのアクセスについて確認した宛名情報全部について窃用しているわけではなくて、フィルタリングなりサイトブロッキングの対象の宛名についてだけではないのか。

さらに､持ち帰りで回答してくださるということなのでまとめて申し上げますけれども、５ページで最高裁59年の大法廷判決を挙げられており､アンダーラインが引かれています。「Ｘ宛ての郵便物には信書が含まれていなかったことから、信書の秘密を侵すものではない。」ここでわざわざ判決を挙げられているので御質問するわけなのですけれども、ここでの総務省の御理解としては、関税法上、輸入が禁止されている輸入禁制品については、信書ではないという整理をされているのだろうと思うのですが､信書でないものの送り先、宛名は、郵便法の信書の秘密に含まれないのみならず、憲法21条２項後段の通信の秘密の違反でもないという理解をされているということでよいのかどうか。

海賊版サイトへのアクセス制限に置きかえて考えますと、海賊版サイトアクセスで利用

者が取得するのは信書ではなく著作権侵害品、まさに関税法上、輸入禁制品として特定されているものですが、サイトにアクセスしたと同時に侵害品を取得することになりますので、このアクセス制限というのは受信制限、すなわち輸入差し止めと同様の効果を持つと思うのですが、その点で札幌税関検査事件をここで引用されている御趣旨というのはどういうことなのか、整理して説明していただければと思います。

○総務省中溝課長　幾つか御質問があったので、全てに個別にお答えできるかわからないのですが、まず大きなところでお答えさせていただきますと、４ページ目の図に「○○×○○」とございます。これらは結局、知得をすることには全て当たると理解しております。これは先ほどのDNSによる名前解決、すなわちつなげてあげるためにDNSをどこへつなげたいのかというのをチェックして接続する。これはまさに正当業務、つなげるというプロバイダ本来の業務のためにそれをやっているという意味で、知得した上でそれは正当業務行為として実施しております。

ただ、ブロッキングを目的として中身を見るという、結局、目的、意図が一番のポイントではないかと思っておりまして、サイトブロッキングするときに知得するということと、つなげるために知得するというところは、知得というか中身を知るということは趣旨が変わってくるということが、私どもの今の考え方でございます。

○林委員　もともとこの正当業務の中で宛先を確認しているのではないのですか。知得する行為自体は、ブロッキングを目的としない現在でも正当業務としてなさっているのではないですか。

○総務省中溝課長　まさにプロバイダとしてユーザーにインターネット接続サービスを提供するという、その目的のためにそういうことをしているということは、おっしゃるとおり正当業務行為でございます。

ただ、そこまで解釈をどう理解するか、なかなか一定の解釈を示すのは難しいと思っておりますけれども、いずれにせよサービス提供のためにそのようなことをするということと、サイトブロッキングのために中身をチェックして、海賊版にアクセスしようとする場合にブロックするという意図を持ってそのような行為をするということは、行為が異なってくると私ども考えております。

○林委員　ブロッキングの目的の問題は「窃用」のところで出てくるのではないのでしょうか。宛名を用いる行為について何のために用いるか。前の宍戸先生の資料でも「窃用」として整理されていたように私は理解したのですが。

○宍戸委員　先生の御質問を含めて若干、私の今までの説明の下手さ加減が露呈して、余りうまくいっていなかったことがよくわかりましたので、ごく基本的なことだけを御説明させていただきたいと思います。

郵便法上、秘密と書かれているのは信書の秘密でございます。郵便物はそれ自体としては物を運んでいるのと同じで、物でございますので、それ自体、通信でないからこそ福井先生がおっしゃったように変な、もともと通信、信書であれば当然に信書の秘密で守られ

ているものを、郵便物である場合には必ず守られるとは限らないので、いろいろこれちゃんと気をつけなさいよという規律があるわけでございます。皆様御承知のとおり、例えば郵便物とか何か箱を送るときに、中に信書を入れてはだめですよと言われることがあるのは、それがごっちゃになることを防ぐためでございます。

それから、恐らく林先生の御議論の前提になっているのは、禁制品が対象であるから信書でなくなるという御理解をされているのかもしれませんが、そうではなくて、そもそも信書ではない郵便物に対して、それが禁制品であるからとめるというのがこの税関検査のお話となります。これがまず１点目でございます。

知得の問題でございますけれども、これは通信の秘密を知るというときに、積極的に知るというところがポイントでございまして、少なくとも私の理解ではそうでございまして、信書を運ぶためにはどうやってもはがきとか封筒の宛名というのは見なければそもそも届けられないので、それは当然やる。しかし、それ以上に通信を成立させる以外の目的でいろいろなことを知ろうとする。そして、それを記憶に残すとか、それはもちろん当然別の問題、個人情報保護法でも同じ問題が起きますけれども、それは知得に当たる。知得というのはこういった形で通信を成り立たせる以上のことを知ることでありまして、およそ宛先情報とかを知っているのだから、それはどう使ってもいいではないかという話とはまた、個人情報保護法でも問題ですけれども、郵便法とか通信の秘密についてはそれが強化バージョンで問題になっているというふうに御理解いただければいいだろうと思います。

最後、瀬尾さんがおっしゃられたAIがというときですが、この場合はAIの持ち主が誰か、AIを誰が使っているかが問題でございまして、このあたりは福井先生と一緒にAIの本を出させていただきましたけれども、要するにAIを人が使っている、通信事業者が使っているのであれば、結局のところそれは道具でありますので、通信事業者がAIを通じて結局、知ったわけでございます。人間が見ていないということであっても、基本的には法人といいますか事業者として知ったものでございます。

そうでなくてAIが独立の法人格を持って通信事業者の手を離れたところでいろいろなことをやるというのであれば、これはAIというものが人の人権とか通信の秘密を侵害できるのかという高度に哲学的な問題になりまして、この点はぜひまた福井先生といろいろ御議論する機会を別のところでつくらせていただければと思いますけれども、差し当たり当面のこの場での問題ではないだろうと思っております。

以上でございます。

○福井委員　御説明ありがとうございました。ただし、この時間は発表に対する質疑の時間であって、委員間討論の時間ではないはずですので、その辺は議事のほうでよろしくお願いしたいと思います。

とは言えせっかく御説明いただいたので１点だけ追加でお尋ねいたしますと、先ほどの宍戸先生のお話だと、この郵便会社が内容の説明を求めたり開示を求め、場合によっては引き受けないことができるという郵便法31条の郵便物には信書は含まれないという御説明

でしょうか。
○宍戸委員　信書の場合には当然そういうことはしないのではないかと私は思います。そこは後で、それこそ郵便法を確認いただければといいと思います。
○福井委員　内容を見ないでどうやって信書かどうか確認するのでしょうか。
○宍戸委員　これははがきの形で来るとか、そもそも信書かどうかは確認できるという前提ではないですか。こういうあたりを、郵便事業会社を監督している総務省の方に調べていただいて、答えていただくのがいいかなと思います。
○福井委員　そうですね。次回の答えをお待ちしようと思います。ただし、郵便物としか書いていないので、恐らく信書は定義上、確実に入ってくるのではないかという気はします。
○岸本参事官　それでは、まとめて総務省さんから後で、もし最後にお答えいただけることがあれば、そのときにお願いするということでよろしいでしょうか。
　前村さんのほうは。
○前村委員　手短にしようと思います。
　森先生が個別にもできるが、ここで大げさにとおっしゃったので、私も後藤さんの先ほどの御質問に対してちゃんと答えておいたほうがいいのかなと思いまして、私どもの資料あるいはISOCのレポートの中で、最後の部分で弊害の最小化ということでオルタナティブを掲げているところのｅで、ローカルな対応をするというところに御反応なさって、フィルタリングというふうなところに反応して、IPフィルタリングと後藤さんはおっしゃったのではないかと理解しているのですけれども、一応ここはこのような言葉遣いがとても難しいなとかねてから思っているところなのですが、ここのフィルタリングというのは、クライアントの中でPCやスマホなどに入れてフィルタリングをするということであって、IPフィルタリングというのは､ISPやキャリアのレベルでIPアドレスをもとにフィルタリングするということなので、これは別のことで、IPフィルタリングに関しましてはこのレポートでも示してあるように回避可能だということなので、そういった観点から検討していったほうがいいということで、明確化させていただきました。
○岸本参事官　ありがとうございました。
　それでは、大変中身の濃いやりとりをしていただきまして、残る時間があと60分となっております。これよりグループ討議に入りますけれども、討議の方法につきましては机上に配付しておりますグループ討議の流れをそれぞれごらんいただきたいと思います。
　前半のグループごとの討議を40分、そして後半の全体での共有、意見交換を20分程度という形で割り振らせていただきたいと思います。傍聴の方はグループ討議の妨げにならない範囲で、席を自由に移動していただいて結構です。
　最後の全体でのグループ内でのやりとりの共有と意見交換の時間を20分、グループ内でのそれぞれのやりとりを40分ということで、時間配分を変えさせていただければと思います。

それぞれ事務局が数名ずつ入りますので、皆様よろしくお願いいたします。

（グループ討議）

○岸本参事官　まだ御議論いただいているグループもあるかと思いますけれども、時間ですのでここで一旦、区切っていただきまして、各グループからグループで討議された内容について２～３分程度で御説明をお願いしたいと思います。よろしいでしょうか。

それでは、私のほうからまずグループＡで討議された内容について、簡単に御説明をしたいと思います。

グループＡでは、まず先ほどの全体での質疑応答の続きということで、CDN事業者への差し止め請求の可能性というものについて少し議論が出ていまして、いろいろな御意見、異論もたくさんあると思うのですが、トライしてみるべきだという御意見ももちろんありますので、ただ、そのトライしていく中でコストの問題というのは無視できないので、そういったところも重要なポイントなのではないかというお話が出ていました。

違法コンテンツのダウンロードの刑事罰化の話も少し出ておりまして、その中に静止画を含めていくということは、いろいろな意味で非常に社会的な影響も大きい話ではあるけれども、もしかするとそういったところに青少年を行かせないという意味で、フィルタリングのさらなるカバー率向上に向けた事業者の努力の向上みたいなところにつながっていく可能性もあるのではないかという御意見も出ていました。

国際捜査共助のお話も出ていまして、いろいろ可能性はあるかもしれないけれども、結局のところ現地の捜査機関を介して動いてもらうことになるので、限界があるのではないかという話が出ておりました。

あとはいろいろ総合的な対策を考えていくべきであって、その中にサイトブロッキングというのはやはり後ろのほうであるべきなのだけれども、１つの施策として入れるべきであるという御意見と、今の通信の秘密の再定義がなければ難しいのではないかという御意見がございました。

その他の海賊版対策としてやるべき政策については、もう少しきちんと議論をして、その進捗状況をきちんとフォローしていくことが必要なのではないかという話が出ておりました。そんなところかと思いますが、福井先生、何か補足はありますか。

○福井委員　なぜ私ですか。みんな補足し始めると１人30分しゃべりますから、これは禁止ということで。

○岸本参事官　大丈夫ですか。

では、続きましてＢグループお願いいたします。

○住田局長　Ｂグループですが、ホワイトボードでやりましたので、みんなに共有できる状態になっております。

左側がブロッキングの話、右側が他の手段の話であります。割と簡単に先に他の手段の

話をすると、リーチサイトのことはちゃんとやってくださいねと。これは改めて要望があり、現状どうなっていますかということで、通常国会に向けて文化庁のほうで検討をしているということであります。それから、静止画のダウンロードの違法化についても、これもやるべきだという議論がありました。これはもう少し時間がかかるかもしれませんが、この議論があります。

もう一つ、きょうの提案の中にIT連から提案があった攻撃、やたらと電話をかけてしまって潰してしまうというスタイルですけれども、これについては余りにナイーブにやると誰が権利者を語って、そういうひどい攻撃をするかわからないから、せめて何か司法みたいなものが入るとか、攻撃していい人はこの人だけよと決めるとか、何かそういうものがないとさすがにまずいでしょうという話がありました。

とにかくフィルタリングは絶対的にやるべきだというのが大勢でありまして、これはしっかりやっていくべきだし、今のフィルタリングとブロッキングの中間みたいなもので、フィルタリングはそのままはしないのだけれども、１回警告サイトが出る。ブロッキングとかなり似ているのですが、警告画面が出て、それでも行きたい人は行けるみたいな、悪意にするということですけれども、そういう仕掛けもあるかもしれないとか、約款をもっと強化して相当明確にどんどんフィルタリングをするようにしていくというようなことも、これはISP業者がかんでくるかもしれないし、ほかのいろいろな今やISP事業者だけではなくてWi-Fi関係の人とか、いろいろ関係していると思いますけれども、そういうところでいろいろなフィルタリングができるかもしれないという話です。

左側がブロッキングの話ですが、ここは憲法中心ということで、まずは憲法の話になったのですけれども、本当にこの宛名だけでも検閲の対象になってしまうのかという話とか、あるいは宛名なんて別に全部見なくてもカード番号の××××みたいな、前のほうだけ見ておけば当たりか外れかはわかるので、それは見ていることにならないのではないかという話とか、通信の秘密の範囲はどこまで入るんですかと、これは余り議論が十分できませんでしたけれども、そういう話。それから、AIで先ほど見きわめたらいいではないかということについては、AIで見て振り分けるほうが怖いという議論もありました。

児童ポルノについてはどうなっているんだよという議論があって、何で法律にしないんだという話もありましたし、明らかに著作権法の場合と違いそうなのは、誰が見ても明白にいかにもという感じがするかどうかという、多分そういうことだと思いますけれども、その辺が違うかもしれないけれども、例えばこの両方みたいなものをまとめて何か法律でできないのかという議論もありました。

費用負担の話は、誰が、権利者がどれぐらい費用を負担するのか。費用を負担するとした場合には当然、ブロッキングの濫用みたいなことにはきっとならないかもしれないという議論がありました。

さっきのところもそうですが、いずれにせよ司法が何らかの形で関与しないと、これは司法が入ったからいいというのではなくて、必要条件として司法は何らかの形で関与しな

ければいけないのだけれども、司法が入るようにするためには先に権利と義務というものを実体法上、明確にしてくれないとできませんということで、逆に言うと権利と義務が明確になっていれば判断は裁判でできる可能性があるし、そうなると司法手続でやるケースも出てくるかもしれないし、訴訟適格の問題としていろいろな段階が訴訟当事者になる可能性も出てきます。

あと、義務のほうですけれども、何が義務かというと違反をしないということではなくて、ISP事業者にはある種の公序良俗を守っていこうという公序の観点から公序を守っていくことをサポートするような義務があるという、多分そういうことだと思いますけれども、そのようなことを一種の義務のような形で構成すれば、何かうまくいくのかもしれません。このような議論がございました。

○岸本参事官　ありがとうございました。

それでは、Ｃグループからお願いいたします。

○曽根参事官補佐　Ｃグループなのですけれども、非常に技術的には複雑な、私にとっては複雑な話も多かったので、もし間違いとか補足があればぜひ委員の皆様からもお願いしたいのですが、私の受けとめとしましては大きく分けて２つのお話があったかなと思いまして、１つ目がサイトブロッキングの弊害ですとか有効性に関するお話と、２つ目がサイトブロッキングによりどれぐらいコストが発生するかというお話があったかなと思います。

１つ目のサイトブロッキングによる弊害とか有効性のお話につきましては、まずどのような話があったかといいますと、非常にたくさんの技術的には回避策がありますねという話が出まして、そういった回避策をいろいろ重ねていく中で、恐らくGoogleのパブリックDNSを使うようなユーザーでありますとか、あるいはDNSブロッキングなりを排除することを売りとするようなISP事業者がシェアをふやすとか、Firefoxのようなブロッキングに影響されないようなローカルなDNSサーバーを使わないことを売りにするブラウザがユーザーをふやすとか、そういった可能性はあるねというお話がありまして、そういったことが仮に起きた場合には、GoogleとかFirefoxがいられると思うのですけれども、外資系の企業であってもどこまで言うことを聞いてくれるかわからないけれども、いろいろと要請をしていく必要があるのではないかというお話がありました。とはいえ言うことを聞いてくれるかわからないので、なかなかどうなのだろうなと。だからといって確実でないからブロッキングをやらないでいいとするのか、それともいろいろ将来的な目測が立った上でないとブロッキングをすべきではないという方向なのか、立場はちょっと分かれていたようにも思います。

ブロッキングの弊害、有効性に関連しまして、トルコのほうでブロッキングを政府が無理に進めようとした結果、通信障害が起きたような事例を御紹介いただきまして、これについてはどうも実態がよくわからないものですから、というのはどういうことかといいますと、通常のブロッキングをしようとしたために、そういった通信障害が発生したのか、それとも通常のブロッキング以上にハイジャックなんていう表現があったのですけれども、

かなり無理なやり方をさらにしようとしたために通信障害が起きたのかわからないものですから、こういった技術的な側面についてもう少し解明していく必要があるのではないかというお話はありました。

コストの２つ目のお話なのですけれども、いろいろ費用が発生するようでありまして、例えばオーバーブロッキングなんかが発生した場合には、ユーザーさんからクレームが入るといったことも考えられますし、通常のサポートとかメンテナンスの費用なんかもかかるということなのですけれども、これについては数にもよるよねという話がありまして、要は現在、児童ポルノのほうでもブロッキングを運用しているものですから、この範囲でのブロッキングの数であれば対応可能かもしれないけれども、それを超えて相当大幅なブロッキングの数を要請されるようであれば、追加的な費用が発生するかもしれないねという話があったのかなと思います。

そんなところでよろしいでしょうか。

○岸本参事官　ありがとうございました。

それでは、各グループの説明に対して御質問のある方に挙手をお願いしたいのですが、もうそろそろ予定された時間に来ておりますので、もし御都合のある方は適宜、退室いただいて構わないと思いますので、よろしくお願いいたします。

今のＡ、Ｂ、Ｃのグループの各説明に対して御質問のある方は手を挙げていただけますでしょうか。よろしいですか。

では、先ほどの全体での質疑応答で総務省さんに御質問があって、その点について幾つか御回答いただけるということですので、お願いいたします。

○総務省　総務省です。

先ほど福井先生から御指摘のあった件について報告というか、回答させていただきたいのですけれども、質問の内容として郵便法の31条のところで、郵便物を引き受ける際に中身を見るというのは通信の秘密の侵害になるのではないか。引き受ける際に中身を確認するのは通信の秘密の侵害になるのではないかという御質問だったと思うのですが、そもそも郵便法上における通信の秘密というのは、先ほどの参考資料にも書かせていただいているのですけれども、特定の受取人に対し差出人の意思を表示し、また、事実を通知する文書に対して、郵便で送る際にこの部分について信書の秘密の保護が課せられております。

先ほどから郵便物というお話をさせていただいていると思うのですけれども、そもそも郵便物って何ですかという話なのですが、それは郵便法の14条にありまして、郵便物というのは第１種郵便物から第４種郵便物と定められております。皆さんにこれを言うとよくわからないので、基本的にはがきって何ですかというと、ここで言えば第２種郵便物のことを言います。ここで郵便物というカテゴリーで言うと、第１種郵便物ですと通常郵便、手紙の入ったものとか、手紙の入っていない日本郵便に差し出す郵便物もしくは第３種郵便物というのは定期刊行物、第４種郵便物というのは盲人用の点字とかいうふうにサービスが分かれております。

それでここで言う31条の趣旨なのですけれども、例えばよく現場であるのですが、今、言った第３種郵便物、要は定期刊行物しか送ってはいけないですよというところに例えば文書を入れてしまって、今、言っている信書、まさに特定の受取人に対し、差出人の意思を表示し、また、事実を通知する文書を入れてしまうと、第３種郵便物として引き取ることができませんので、その旨をここでうたっております。そういう疑いがある場合は引き受けることはできませんという話になっております。

要はここで言う信書と言われる、特定の受取人に対して差出人の意思を表示し、また、事実を通知する文書が入っていないものであれば、それは通信の秘密の侵害になるものではございませんので、入っている場合にこのものについてどうするかという議論に郵便法上はなります。

以上です。

○岸本参事官　よろしいでしょうか。今の御説明で特に御疑問の点がなければ。

○福井委員　疑問は解消しませんでしたし、31条の２項ではこの法律もしくはこの法律に基づき総務省令の規定または郵便約款に違反して差し出された疑いがあるときはとあって、これは対象が広く、12条の郵便禁制物を含んでいます。12条の郵便禁制物には国内において、法令によって頒布を禁止されたもの。これがはっきりと明記されているし、ほかに爆発物、毒薬なども明示されています。よって、おっしゃった説明はもう一度、検討されたほうがよろしいのではないでしょうか。

私からは以上です。

○岸本参事官　また何か補足がございましたら、次、第５回でお答えいただいてもよろしいかと思いますし、個別に委員にメール等の形で御回答いただいてもよろしいかと思います。また御相談させていただきたいと思います。

最後にグループ討議全体を通して、あるいは前半の各説明に対してでも結構ですので、何か御意見、御質問等ございましたらこの場で挙手いただけますでしょうか。

○宍戸委員　きょう随分私がしゃべって怒られた、福井先生、申しわけございませんでした。私は説明したつもりだったのですが、失礼いたしました。

きょうこの場でも議論をさせていただいたのですが、先ほど局長からもお話がありましたように、フィルタリングとブロッキングの中間みたいなものも少し検討してみてはどうだろうか。具体的に言いますと、ISPが約款で包括同意で特定のサイトへアクセスするということを何らかの形で遮断する。もちろんこれは通信の秘密の侵害になるわけですが、一定の包括同意としてできる場合というのがないのか。サイバーセキュリティーの関係ではしばしばとられる手法でございますので、そのあたりは御検討を誰がするのかもわかりませんけれども、論点として挙げた上で事務局もそうですし、あるいは総務省、ISPとかそうかもしれませんが、それがやれるかやれないか含め、１つ総合的な対策の課題として挙げていただけるといいのかなと思ったところでございます。

以上です。

○丸橋委員　今の話は、サイトブロッキングがいつでもできる状態にしておくという意味であるとすると､余りブロッキング議論と変わらないのかなと思って聞いておりましたが、いかがでしょう。
○宍戸委員　そういう点も含めて御議論いただければと思います。きょうはこれ以上、議論しません。
○岸本参事官　ほかにどなたかいらっしゃいますでしょうか。全体を通じての御感想でも構いません。あるいは今後こういうことを会議の中で話したいみたいな、よろしいでしょうか。
　では皆様、議論も尽くしていただいたということで、大変長時間ありがとうございました。
　最後に住田のほうから一言、御挨拶申し上げます。
○住田局長　本日はどうもありがとうございました。グループで議論すると大分何となく達成感というか、大分しゃべったな感というのがあって、最後のほうは何となくそうかなということになってよかったかと思います。ここのテーブルではこういうものを３回ぐらいやったほうがいいとかいう話もありましたが、さすがにそこまでやると大変かもしれませんけれども、いずれにせよすごく大事な議論なのでしっかりと議論を深めて、認識を共有しながら中間的なまとめに徐々に入っていきたいと思いますので、引き続き御協力をよろしくお願いいたします。
　きょうはどうもありがとうございました。
○岸本参事官　次回の御案内ですけれども、第５回の検討会議につきましては、８月24日金曜日の17時から19時半までの予定で開催させていただきます。場所等につきましては改めて御案内申し上げますので、よろしくお願いいたします。
　本日はどうもありがとうございました。
○曽根参事官補佐　委員の皆様に配付しております名前つきの過去の資料のセットなのですけれども、ホームページに公開していない資料も含んでいるものですから、回収させていただきますのでよろしくお願いします。