

産業構造審議会知的財産分科会 第8回営業秘密の保護・活用に関する小委員会議事録

○諸永室長 皆さん、こんにちは。定刻となりましたので、ただ今より、産業構造審議会知的財産分科会営業秘密保護・活用に関する小委員会の第8回会合を開催したいと思います。

本日は、ご多忙の中、ご出席いただきまして、まことにありがとうございます。

では、岡村委員長、お願いいたします。

○岡村委員長 岡村でございます。朝の会議であれば、おはようございますで始まるのですが、どうもこんにちはというのも変な感じがいたしますけれども、ひとつよろしくお願いたします。

まず、審議に先立ちまして、本日の配付資料の確認などを事務局からお願いしたく存じます。

○諸永室長 まず、本日の出席状況でございますが、本日は、久貝委員がご欠席されています。

そして、オブザーバーとして、内閣府知的財産戦略推進事務局、法務省、文化庁の方にもご出席いただいております。文化庁の方は5分ほど遅れるというご連絡をいただいております。

お手元の資料でございますが、資料1の裏面でございますように、資料1～8、参考資料1～3としまして、前回の資料、前々回の資料をつけております。お手元にない方がいらっしゃいましたら、事務局の方にお申しつけください。

では、岡村委員長、よろしくお願いたします。

○岡村委員長 大変ありがとうございました。

それでは、早速、本題に入らせていただきます。

本日は、まず、前回までのご議論と、その後の委員と事務局との意見交換をもとにいたしまして、データ保護に関しての検討の方向性について事務局におまとめいただきましたので、その説明をお願いいたします。

なお、本資料に関連した議論につきましては、次回以降行わせていただく予定でございます。

○諸永室長 ありがとうございます。

前回、前々回という中で、データの保護に関してのご検討をいただきました。そこで多くのご意見をいただきましたので、資料3に、こちらの議論をこういう形で進めていこうという方向性を示させていただきました。

そして、今、岡村委員長からいただきましたように、こちらの議論に関しましては、次回、今日ご議論いただく論点の積み残しも含めてまとめて議論をさせていただきたいと思っておりますので、本日はご報告までとさせていただきます。

それでは、資料3を御覧いただきながら進めさせていただきたいと思っております。

まず、前回いただいた中で一番大きかったところは、どういうものをデータの保護の不正な行為として検討するのかといったところでしたが、不正な手段によりデータを取得する行為、そして、さらに不正な手段により取得されたデータを使用・提供——提供の中には開示も含まれますが、その行為に関して、新たな不正競争行為として規定してはどうかということで、ご議論をさせていただきたいと思っております。

そして、規制対象とする行為といたしましては、新たな制度の創設——営業秘密の要件自体を変えるというわけではなく、新たに不正競争行為の類型を設ける形で、データの利活用が進まなくなるとのご意見にも配慮しながら、まずは、「不正な手段」による行為を規制するというのはどうか、ご議論いただきたいと思います。「不正な手段」としては、我々としては、「撮取、詐欺、脅迫その他の不正な手段によりデータを取得する行為」を念頭に置きながら、この言葉も含めて、どのようなものが必要かをご検討いただきたいと思います。

そして、念頭に置いています「その他不正な手段」とは、パスワードや暗号がかかっているものを外して、プロテクトを無効化してデータを取得、そして、データにアクセスしていくような行為を「不正な手段」としてはどうか。

もう1つ、データを預かる上で、そのデータを使用や取得はしないよと約束をしていたにもかかわらず、その約束をした人が約束を破って取得やアクセスを行うこと、このような類型を「不正な手段」としてはいかがかと思っております。

そして、「ただし」として書かせていただきましたが、その「不正な手段」をその後、転々流通としていくような、例えば、正規に預かっていた本人から外に、第三者に出ていくような場合、ここは図利加害目的でデータを使用や提供する行為に関しては不正競争行為と規定するという方向で、引き続き検討をいただきたいと思います。

裏面でございます。こちらも多くご議論いただきましたが、実際に保護の対象とするデ

ータですけれども、例えば複製禁止ということがわからなかったり、悪意を持たずにさわったりした場合、そうした人に対してもちゃんと認識ができるようにとご議論いただきましたので、第三者が客観的に見て、アクセスを認めていない方がデータを取得やアクセスするタイミングにおいて、アクセスすることを防止したいという意思がしっかりと認識できる状態、そうになっているデータを「不正な手段」などを通じて取得するということを保護対象とするデータとしたいと思っております。

例えば、こちらもさっきの行為の裏返しかもしれませんが、データに対して暗号もしくはパスワードでロックがかかっている、それらプロテクトを施した上で、メールなどで送信しているようなデータ、もしくは、ID、パスワードを要求されるようなホームページにアップされているようなデータ、そのようなものを想定していただきたいと思っています。

そして、先ほど申しましたように、例えば、営業秘密であれば、第2次取得、第3次取得というように転々流通していくことに関しても、不正であることを知った上でやっている場合においては、例えば、差止めであるとか損害賠償ということもございますので、こちら、データに関して不正な手段が介在したことを知って、その後、転々流通していく場合においては、規制対象とすることが必要ではないかというところは引き続きご検討いただきたいと思っています。

そして、前回は資料5と資料6で、そして、本日は参考資料1と参考資料2で示させていただいておりますが、これを前提に、さらにどんな要件が必要か、もしくは足りない観点として何があるかというところをより深くご議論いただきながら、そして、こんな要件も必要ではないかというご検討もいただきたいと思っています。

そして、今日お示ししましたのは、前回いろいろご意見をいただきまして、その後、委員の先生方と意見交換させていただいた上で、こちらの方向性でいかがかということを示させていただきました事務局の案になります。

以上でございます。

○岡村委員長　大変ありがとうございました。

それでは、引き続きまして、「情報のトレーサビリティに関する取組事例」につきまして、ゲストスピーカーによるプレゼンテーションをお願いしたいと思います。

では、諸永室長、プレゼンターのご紹介をお願いいたします。

○諸永室長　ありがとうございます。今申し上げましたデータの保護ですが、これはデ

ータが転々流通してしまった場合に自分のデータであるよということを立証していくという目的や、さらに、今日ご議論いただく技術的制限手段の無効化といったところと関連する検討をしていただく内容になります。そこで、技術的な部分に関して、本日、株式会社MONICの岡村様より、電子透かしであるとかトレーサビリティの技術に関しての最近の動向について、プレゼンテーションをお願いしております。

それでは、岡村様、よろしくお願ひいたします。

○岡村　ご紹介にあずかりました株式会社MONICの岡村と申します。よろしくお願ひいたします。

それでは、早速ですけれども、本日は、情報のトレーサビリティという観点で、事例のご紹介をさせていただきたいと思っております。

皆様は、電子透かし技術というものを耳にされた方もいらっしゃるかと思いますが、本日は、幾つかのデモンストレーションで、実際にどんなものかも御覧いただきながらご説明をしたいと思っております。

まず、プレゼンテーションの1枚目のみ簡単にご説明いたしますが、電子透かしというものは、基本的には、画像に人間の目で見にくい状態で情報を書き加えていく技術です。または、音声、音楽の電子透かしというものもございます。音の中の人間の耳ではとらえにくい状態で任意の情報を書き加えるという技術です。これを電子透かしとっております。

用途によって、過去、いろいろな表現方法、名称はございました。ステガノグラフィーといわれているものがあったり、古くは画像深層暗号などといわれてたりというような、そんな時代もございました。

そして、セキュリティという使われ方が当初ございましたが、マーケティングの測定のため、または、今ちょうど話に出ておりますけれども、情報のトレーサビリティという目的で利用されているケース、こちらが最近是非常に増えてまいりました。その理由はこれから事例をもってお話する中でご説明させていただければと思っております。

この電子透かしというものはどういうものに使われているか、下に簡単に書かせていただいております。

画像と申しましたので、このような写真、デジタルデータ、よくありますウェブコンテンツ、そういうもので使われているのが非常に多いものです。また、音楽、ビデオ——最近インターネットを初めとしまして、コンテンツの配信でこのようなものを皆様ご利用

いただいていると思いますが、その中に電子透かしで著作権管理の情報が含まれていたりします。また、最近では、電子書籍も同じようにこの技術を用いまして情報の管理のために利用されています。

また、ここ数年、非常に多くなってきているのは、企業の皆様の中の社内の貴重なデータに対して、情報管理目的でひっそりと管理番号を入れたり、そのような使い方も増えております。

また、もともとこの技術はアメリカから発展してきたものですが、アメリカを含めまして海外40カ国ほどで、運転免許証やパスポート、お金の紙幣など、そういうところでのセキュリティ技術の一つとして採用されてきているものでございます。

それから、最近では技術がどんどん進歩しますので、こういう画像技術も適用素材が非常に増えてまいりまして、今日は布などもご用意しましたが、金属であったり樹脂であったり、あらゆるものに対して、印刷なり何らかのマーキングができるものであれば、任意の管理情報を入れることが実現されて、実際に活用されているケースも増えております。

一旦、プレゼンテーションから離れますけれども、では、実際にどのようなものをちよっと実演してみたいと思います。

まず、わかりやすいところで、エンターテインメント的な部分ですが、これはあるタレントさんの写真集のようなものですが、この画像の中に透かしというもので情報を入れております。ここにスマートフォン用の専用のアプリケーションがございまして、これを電子透かしが入っております画像に当てます。そうしますと情報検出をしまして、この書籍を買った人だけがビデオがみられたりということで、サービスとして提供されたりしております。

これは写真の例でございますが、その他、例えば、こういう画像がない状態で真っ白なものに対して処理するということもできたりします。いろいろな技術が使われております。これは真っ白い箱の状態ですが、これをこのようにかざしますと情報検出をしまして、本来はこういう商品のパッケージの箱の紙だということになるのでわかるようになっております。

あとは、企業で利用されるケースの一つとしてこんな使い方がされますよということですが、例えば、社内で行き交います文書に加工してございまして、これもこのようにかざしますと情報検出されます。これはたまたま地図が表示されるような形で、中にそういう情報を入れております。

今デモしたものを実際に御覧いただければと思いますので、回覧させていただきます。

今御覧いただきましたとおり、これは主に印刷物としてご提供していますが、企業の中、または製品の流通、そういうものに対して、目に見えない状態で何か識別する情報を入れるということで、情報管理に役立てるという使われ方が実際にされています。

こういう電子透かしという技術はそもそもどういう法的根拠があるのだということも、この場でもございますので、疑問に思われる方がいらっしゃるかと思います。この技術はもともとは、1990年後半、インターネットが出始めた時代に、流通するウェブコンテンツの著作権をどう守るかというところから、いろいろ法整備というものについて皆様にご協力をいただいていた次第です。

そういう意味で、まず、著作権法の中でこのように定義されました。記載しているものは参照としても書かれておりますけれども、主には文化庁様で今後のデジタルコンテンツに対する権利管理でどうだというあたりで法整備をいただいたという経緯でございます。これが平成11年だったかと思います。

そこからこういうコンテンツビジネスにおける利用というのが始まったわけですが、近年、技術の進歩により、今御覧いただいているとおり、企業の中での電子データ——文書ですね。また、画像においても、企業の中ではデザインであったりとか製品情報として非常に貴重な取得データというものがございます。または、学術の分野でありましたら、当然、研究で用いました画像のデータや図面などの中に、管理をしなければいけない情報として入れます。

では、具体的にどのように使われているかということで、こんな図を1枚、資料としてつくらせていただきました。これは実際にある日本の企業様でご利用いただいている形態でございます。最近ではクラウドなどという形で情報の共有、利用も進んでおりますが、まず、企業として管理している情報がマスターデータとしてシステムの中でございます。

ここに対して、事業部ごとにそのデータが流通して、かつ、その事業部の従業員の方々がデータを利用されます。そして、この事業部に渡る際に、「この事業部に渡りましたよ」という情報がこの電子透かしという技術で埋め込まれるということになります。さらに、この事業部の誰がこのデータを利用しているかということ、画像の中に、または文書の中に入れてしまうような自動的な仕組みをつくっております。

仮に、B事業部のAさんという方に渡った書類、または画像データがインターネットで流出をしてしまった場合、Aさんが流したデータに関しては、B事業部のサーバーを経由して、「Aさんが使ったものです」ということが目に見えない状態で書類や画像の中に入っ

ていく、こういう利用のされ方をしています。

これで、流出データというものがどういう経路で、どこが流出のもととなっているかということを検知する。そういう仕組みを企業様の方では導入をしていらっしゃる。

最近ではクラウドサービスでさまざまなデータ共有の仕組みがございます。自社でこういうシステムを開発されるためには、非常に労力、体力、金銭も必要になってきます。コストがかかります。よって、お安いクラウドサービスというものを世界的に使うのが普通になってまいりました。そのときの社内の情報というものに対して、クラウドサービスを経由してどこに渡るか。これもこの電子透かしという技術を使って埋め込むことで、社外に出ていくデータの管理をしていく。そういうことを実現されている企業様も増えてきております。

これは法的な根拠を求めるといよりは、企業の観点からみますと2つ導入の目的があると聞きます。

1つは、まず、自社の事業の中でデータがどのように動いているかということ、デジタルデータだけではなくて、アナログの印刷物も含めてちゃんと把握できているかというところを立ち返って考えるということです。ニュースになるかならないかは別ですが、企業の中でも情報漏えい事件というのが非常に多く出ております。この導入をいただいた日本の会社様に関していいますと、発売前の製品データが社外に漏えいするケースが年間数百件あったと耳にします。

それは、社内でどのように情報というものが使われているかということが十分に理解できていない、どこにセキュリティの穴があるのかということもわからない。それに対して、対策、打つ手があるのかということ、なかなかない。そこはまずは社内の状態をリサーチするという意味合いで、こういう技術を導入する方々というのが第一に多いケースでございます。実際に出ていってしまったものをどうするというのは二の次で、まず現状把握というのが可及的な問題だということをご利用いただくケースが多いです。

かつ、実際にデータが流出したときに、「誰が出したの」ということがこれでわかるので、それが最初の目的ということよりは、企業内の情報管理という意味合いの目的の方が本当は多いです。ただ、実際に漏えいしているものからこうやって社員の情報が出てきますと、つつい犯人探しをしたくなるのが人の常でございます。導入いただいた企業様からは、「誰だ、誰だ」ということで、どんどん犯人探しに目が行ってしまうというのが、私ども技術提供者からすると、本来の姿ではないなと思ったりはしますが、こういう形でも利用

されている。または、意識として、どういう目的でやっていらっしゃるかについては、自分たちの事業の範囲の中で情報がどう流れているかを正確に把握するということに意識が行かれている方々が多いのかなと思います。

また、社外でこういう技術を使ってマーケティング情報を使うケースがございます。

お時間もありませんので、あとは簡単にお話しいたしますが、今みていただきましたとおり、皆様お持ちのスマートフォン、特に若い方はほぼスマートフォンをお持ちでいらっしゃいますので、若い方をターゲットにしたマーケティングビジネスでのご活用が増えてきております。印刷物、雑誌、音声を使った情報配信、デジタルサイネージ、そういうものをこのスマートフォンを使って、どこの媒体で、どのメディアが、いつ、誰が、何をしているということをとらえて、マーケティング情報として活用する。電子透かしだけではなくて、QRコードもそうですし、ARであったりとか、さまざまな技術を使って皆様ビジネスを始めていらっしゃいます。

これはある特定の方々に対して広告ビジネスとして何かを提供するという、視点はそこから変わってきております。情報を訴求する伝達方法としての信頼性であったり正確性であったり、IoTではないですけども、それぞれの効果測定であったり、ビジネスにどのように寄与するかということ把握しようとするために、こういう技術を使ってきていると思われまます。

あとは駆け足になってしましますが、最初にお話ししましたように、金属などにも入りますので、工業製品にもいろいろ使われます。これはどういうことかと申しますと、自社の製品がどのように物流として流れているか、または、その部品が正しいものがつけられているのか、いないのか、事故が起きたときに、どこでつくったものに事故が起きているのか、いろいろな使い方があります。真贋判定的な使い方もございます。本物か偽物かを見極めるというものもございます。

今お話ししたものをトータルで簡単な絵にしますと、製造というところでこれを使って、製造管理や生産性の向上や実態を把握するという、物流というところで物のトレーサビリティというものをこれで行う場合、または、販売測定、在庫管理、そしてそれを手元に投じました一般の皆様、生活者の方々の情報配信などで使われるマーケティング、そういうものをこの画像認識技術、電子透かし技術など、最近ではRFIDや、電波も含めて、多くの事業者の方が採用されて利用されています。

これらはいずれにしましても、物、人、そういうものがどのように動いていくかという

ところを皆様は集めていくという状態になってきております。それが営業的な価値があるというのは、事業者によって、データは1つでもさまざまな価値が生まれていますので、何をどう保護していくかは、事業者様によっても悩まれているところですので、今回、このような機会でお話しさせていただきましたが、皆様の議論をいただくことに関しては、非常に効果がある、価値のあることかなと思っております。

ちょっと中途半端な状態になってしまいましたが、目に見えない、耳に聞こえないこの技術を使いまして、一般の企業の皆様が、セキュリティまたはマーケティングという面で、このように情報を集めていますよということを事例としてご紹介させていただきました。

以上です。

○岡村委員長 岡村様、ありがとうございました。

それでは、ただ今のプレゼンテーションにつきまして、事実についての確認と申しますか、この点はどうかということについてのご質問があればお願いします。

なお、内容に関する質疑やご意見につきましては、次の議題と併せて一括してお願いしなく存じます。

いつものように、ご質問のある方は、大変恐縮ですけれども、お名前の札を縦にしていただけでしたら幸いです。

それでは、大水委員、お願いいたします。

○大水委員 1点、教えていただきたいのですが、これはトレーサビリティの情報タグが入っている状態のものを一般の人がそれを見分ける方法というのはあるのでしょうか。逆にいいますと、自分の目の前に来た情報が誰のものかというを見分ける方法が、何かパブリックなものとして提供されているのでしょうか。

○岡村 回覧いただきましたもので、タレントさんの写真集のようなものがございましたが、あの場合は、出版社様の方から、それを読み取るためのリーダーの告知というのをされていらっしゃると思います。ですから、企業様から公にしたい場合は当然告知しますし、ひっそりとした場合は告知しないでそのまま流しているというのが実情です。

○岡村委員長 よろしいでしょうか。

○大水委員 はい。

○岡村委員長 それでは、長澤委員、お願いします。

○長澤委員 キヤノンの長澤です。1つお伺いしたいのですが、先ほどのルーティンからいくと、誰のパソコンを通ったかがわかるというご説明がありましたが、これは個人情報

報保護法との関係が出てくる可能性があると思っっているのですけれども、そういう事件がこれまでに発生したことはございますか。

○岡村 導入いただいております企業様の中では、そのようなことは伺ったことはございません。企業様の中の社員の方または社外の方に対して、守秘義務契約に基づいて情報管理をお伝えされていることかと理解しております。

○長澤委員 特にヨーロッパは個人情報保護の規定がかなり厳しいので、我々もヨーロッパでは個人情報の取り扱いは非常に注意しているのですが、御社の顧客さんでヨーロッパの方はいらっしゃいますか。

○岡村 はい。ヨーロッパでご利用のお客様は実際にいらっしゃいまして、聞く限りでいいますと、ヨーロッパからの情報漏えいというのは非常に多いということです。実際にこの技術を使って解雇されたケースも聞いておりますが、そのときに、個人情報という観点で訴訟になったということは聞いていないです。

○岡村委員長 長澤委員、よろしいでしょうか。

○長澤委員 はい。

○岡村委員長 では、あとお一人ぐらい、ご質問がございましたら。

それでは、時間の関係もございますので、また次にまとめてご質問などをお受けする機会もあろうかと存じますので、とりあえず次の議題に移らせていただきたいと思います。

岡村様、ありがとうございました。

次の議題は、「情報の不正利用を防止する技術の保護の在り方について」であります。

まずは、事務局から資料の説明をお願いしたいと思います。

○諸永室長 ありがとうございます。それでは、資料5、そして参考資料1として、第6回、前々回に配らせていただいた資料を御覧いただきながら進めたいと思います。

第6回においては、データの保護というところに加えて、不正利用を防止するような技術、暗号化などに対する保護についてのご検討をいただきたいとお示しいたしましたが、それに関する詳細なご議論をいただきたいと思ひまして、資料5を用意しております。

まず、資料5を御覧いただきたいと思ひます。

第1、検討の背景でございます。これは今まで不正競争防止法の中に技術的制限手段の無効化に禁止行為が入ってきた経緯を書かせていただきました。

1つ目のポツですが、平成11年の改正のときに、まず民事というところから入ったということでございます。こちらが入ったときは、コンテンツの流通を念頭に、差止め請求権、

そして損害賠償請求権が導入されました。

その際にご検討いただいた中では、技術的制限手段のその当時の技術においてなるべく具体的にということになりましたので、今回ご議論いただく際には、その平成11年のタイミングとの技術の進展であるとか、実際に使われている部分の差も検討いただければと思っています。

そして、その後、平成23年に、規制装置の見直しということで、もともとそれ専用に使っている機械のみという要件があった部分に関して、それを外すという検討と、そして、この検討のときに、刑事罰も導入されることになりました。

そして、今回、近年の情報のデジタル化の進展ですが、通信速度が上がったり、もしくは記録媒体の容量が増えてきたり、そして、さまざまな形で流通形態が変わってきているというところが、検討を始めていただくきっかけだと我々は思っております。

そのような中で、2ページ目でございますが、今回ご議論いただきたいところは、まず1つ目は、映像、音、プログラムに加えて、先ほどご議論のご紹介をいたしましたデータを保護対象として追加する必要があるかという点です。

2つ目は、最近使われている技術として、現行の法律の規定では読みにくい部分があるのではないかとということで、アクティベーション方式に係る技術的制限手段など、現行法の法解釈が必ずしも明確でないものについて、明確化を図る必要があるかといったところをご議論いただきたいと思っています。

3つ目は、現在、無効化機器の引き渡し譲渡を対象としておりますが、それを無効化のサービス——これは実際にサービスを提供しつつそれを使える状態にして提供するということ、この辺を行為規制の対象に加えていくかをご検討いただきたいと思っています。具体的には、不正改造サービスであるとか、役務として解像機器を提供するようなサービスというところをご検討いただきたいと思っています。

4つ目は、先ほどの電子透かしの話で少しイメージがあったかもしれませんが、データの出所を明らかにするような電子透かしの技術、これ自身の保護についてご検討いただきたいと思っています。

それでは、具体的に1ずついきたいと思っております。

1つ目は、検討事項1、2ページ目の下半分ですが、こちらは現行法の確認でございます。現行法は、映像の定義といたしまして、映像、文字、図形など、人が視覚により感知するもの、そして音——聴覚によって感知するもの、そしてプログラムといったそれぞれ

の対象物を規定していますが、それぞれの行為も一緒に規定しています。映像の視聴・記録、音の視聴・記録、そしてプログラムの実行・記録となっております。

具体的には、3ページ目の上方のポンチ絵をみていただきたいのですが、映像と音の視聴とプログラムの実行、そして、それぞれの記録が対象となっております。

実際に最近進んでいるところとして、映像と音の部分の下にあります計算機等による分析ですが、例えばAIに画像や音声を学習させる、こちらの方が実際に暗号化など制限をかけて行っている場合は、それを外すようなところは、コンテンツの保護と同様なものがあっても良いのではないかというご意見をいただいています。

さらに、その左半分、②と下に書かせていただきましたが、視覚、聴覚により認識できないデータ——これは現在、対象になっていないと思っておりますが、このようなものが仮にあって、それを電子計算機など、例えば工場などから出てくるような、本当の計測の熱であるとか、温度、振動などを数値化しないでそのまま飛ばして、それを分析するような、もしくは制御に使うような場面があるのであれば、このようなデータも条文で読めるようにしていけば良いのではないかと考えています。

3ページ目には、他法令の保護なども書かせていただいています。

続いて5ページ目、検討事項2でございます。これはこの後、BSAの方から事例のご紹介をいただきますけれども、アクティベーション方式というのは、平成11年に規制を行ったときには、CDやDVDでソフトウェアの販売が行われて、そして、そこに書かれているシリアル番号などを入力して海賊版などを防いでいくといった行為が行われていましたが、現行、皆様もソフトウェアなどを購入される場合に、ダウンロードをして、さらにお試し版があって、そしてその課金を払うと正規版にというように、段階を追って使える範囲が変わっていくといったものがあると思っておりますが、こちらはアクティベーション方式と呼ばれています。

これはプログラムという形で、ソフトウェアだけではなくて、例えば、ゲームソフトのダウンロードもしくはアイテムなどが出てくるときは、アンロック方式が使われており、スマートフォンのゲームアプリなどもこちらの方式がよく使われていると伺っております。

このような段階を追って使える範囲が認証を経て変わっていくのは、法律の条文上、お手元の参考資料1に、これは第6回に示させていただいております資料でございますが、その6ページや8ページを御覧いただきますと、これは法律の条文でございますけれども、「視聴等の機器が特定の反応をする信号を映像とプログラムとともに」と書かれています。

この「とともに」というところが、日本語として「一緒に」という意味か、「場所として一緒」なのか、「時間として一緒」なのかがわかりにくいということで、さまざまな判断が法廷などで行われていると伺っています。

この辺に関して、どのようなことがあるのかを今日ご紹介いただきたいと思います。

そして、資料5に戻っていただきまして、5ページです。今のソフトウェアの利用状況でございますが、不正なプロテクトを解除していくことが、クラックプログラム、クラックツールといわれるものだったり、プロダクトキー、そういう不正なものがインターネットのオークションなどに数多く出品されているそうです。こちらは少なくとも1ヵ月に数千件、数万件が実際にインターネット上で販売であるとかオークションなどが行われているのが現状でございます。

6ページでございますが、こちらは、明確化したいといった思いでございますけれども、ケースによっては、「とともに」というところは、アクティベーション方式においても、実際に民事、刑事で扱われた事例がございます。ですので、認められている事例もある。

一方で、警察、検察と一緒に捜査協力などをいただいた過程においても、「とともに」の解釈が難しいということで、実際の立件まで至らなかったようなケースが、平成26年9月から足元2年4ヵ月ぐらいの間に10件中6件ぐらいは、残念ながら立件に至りませんでした。

その「とともに」は、片や他の法廷では認められて、読みにくい部分があったのかなと思いますので、この部分を現状の技術に合わせて変えることが必要かどうかをご検討いただきたいと思います。

そして、冒頭の過去の経緯をご紹介いたしました平成23年の改正においても、このプロテクトを外してはいけないよという「機能のみに」という条文がございましたが、この「のみに」という要件を外すきっかけになったところが、任天堂のDSのマジコン事件をきっかけに、「のみに」の要件は、それ以外の用途に使っていても、そういう機能があればということで、資料5の後ろの参考につけておりますが、「のみに」を外す改正を行いました。

今回も、今、何か読めていないというよりも、読みにくいところを現行に合わせていこうという検討をいただきたいと思います。

そして、3つ目のご議論をいただきたい点でございますが、資料の7ページ目でございます。こちらは、現行法においては、無効化機器の譲渡等ということで、物の移動を伴いながら規制対象としておりますけれども、だんだん事件として上がってくるものの中で、

サービスの提供など、実際に物が移動していないものが幾つか上がってきておりますので、これは法の趣旨から考えますと、使えるような状態にしていくことを提供しているということでは、同じぐらい悪いのではないかと考えております。

1つ目のイメージは訪問型サービスです。これは実際にご自宅であったり、もしくは工場に導入されている機械を不正改造するといったこと。あるいは、最近、あるだろうと思っているのがリモートアクセスで、例えば、我々もパソコンなどで不具合が出ますと、電話して、ネットにつながっていればオペレーターの方が対応していただけて、リモートアクセスで何かをとということがありますが、これも実際に物の移動は行われていませんので、同じような、例えば不正改造を行う場合においても、実際の物の移動がないので、対象にはならないのではないかと考えています。

そして、2つ目の類型が、店舗などにおいて、例えば、不正なB-CASカードを使って有料コンテンツを無償でどんどん提供するような、実際に機器を使いながら役務を提供していくような、こんな類型が足元でも摘発などされているものでございます。こういったものは今著作権による摘発がなされていますが、例えば、著作権が認められないようなものに対しての店舗型のサービスが仮にあるとすれば、同じような類型かと思っています。

3つ目は、改造サービスです。よくある例は、実際にインターネットなどで改造しますよというサービスをうたっていて、そして、例えば、自分のもっているゲーム機を不正改造してほしいなと思うと、送って改造してもらって送り返してもらうということがたくさんやられているようです。こちらは、実際に物が移動しているということをとらまえて警察などでも書類送検などがされているケースがございます。

4つ目は、例えば、不正改造の仕方であるとか、このプロダクトキーを入れればみられますよといった情報提供サービスも、実際にインターネット上にはたくさんあります。ただ、こちらも、過去、平成23年、平成11年という中で、このサービスも議論されていく中においては、情報提供に関しては、今回の技術的制限手段以外の部分も含めて、情報提供ということはさまざまなことを関与しながら、相当慎重な検討が必要というコメントがされているところでございます。ですので、今回も対象として検討いただく際にも、慎重なご議論をいただきたいと思っています。

そして、8ページ、9ページですが、こちらは、今ご紹介したようなサービスが、実際の案件に照らしまして、他法令違反として扱われているような例をご紹介しているところでございます。

そして、今回ご議論いただきたい点としては、今申し上げました技術的制限手段の無効化のサービスを念頭に、追加をしていくのか、いかないのか。これは他方で、例えば、著作権法においてカバーされているので、あえて追加する必要はないのではないかと、こういったご議論も含めていただければと思っています。

最後に、11ページ以降、トレーサビリティの部分に関してもあわせてご議論いただきたいと思っています。

先ほどご紹介いただいたような、著作権法に基づく権利管理情報を外すということに関しては、現在の著作権法においても禁止行為としてされています。外す、もしくは改ざんする、こんなところがあります。

そして、11ページの真ん中の部分にお示ししておりますが、著作権法にこの規定が入った際の目的のところ、導入時の整理という形でまとめさせていただいていますけれども、違法利用の発見のためと、自動的な権利処理——これは不正なことをしたい側ではなくて、権利を例えばライセンス料なども払いながら利用したいというのは、だれに許諾をとれば良いのかといった趣旨の規定でございますが、そんなことを目的に導入されているものでございます。

そして、これが保護の必要性ということで、権利管理情報が除去されてしまうと、インターネット上などで違法利用を発見することがすごく難しくなるということがあって、改変されてしまうと、使用料などをお支払いしたいといったところの処理がとどこおってしまうということで、著作権者が多大な損害を被ることが予測されるということで、平成11年にこの導入に至ったとまとめられております。

そして、こちらを念頭に置きながら、今回、データの利活用という観点からも、このトレーサビリティというのは増えていくと思いますが、これを外す行為を実際にこの不正競争防止法の中で担保する必要があるのか。この点をご議論いただきたいと思っています。

そして、12ページですが、著作権法にあるからといって、こちらに入れる必要があるのか、もしくは、「著作権が認められないデータの部分のみに」といった対象を加えるのかというところをご検討いただきたいと思っています。

そして、仮に入れる場合であれば、ほかの部分の規定は民事、刑事両方あるのがこの技術的制限手段の項目になりますので、救済措置としてどういうものを入れるか、もしくは罰則ということでどういうものを入れていくのか。例えば、トレーサビリティ外しということで外したタイミングであれば、損害額を考えますと、まだ発生していない部分がござ

いますので、その点も踏まえてご議論いただければと思っています。

以上でございます。

○岡村委員長　なかなか盛りだくさんでございます。ありがとうございます。

引き続きまして、今の説明に関連いたしまして、ゲストスピーカーによるプレゼンテーションをお願いしております。

では、諸永室長、プレゼンターのご紹介をお願いいたします。

○諸永室長　ありがとうございます。先ほどご説明した中での検討事項2の部分を中心にはなりますけれども、アクティベーション方式に関しまして、実際の技術的な現状、そして、その侵害などに関する現状を、BSA／ザ・ソフトウェア・アライアンスの水越様、そして、一般社団法人コンピュータソフトウェア著作権協会（ACCS）の中川様よりプレゼンテーションをいただきたいと思っております。

水越先生、よろしく願いいたします。

○水越　ありがとうございます。ただ今ご紹介いただきました水越でございます。

BSAというのは、いわゆるビジネスソフトウェアの業界団体でございます。OS、アプリケーションソフトといったビジネスソフトウェアを開発・提供しているメーカー、また、IT業界ということでハードウェアメーカー等が会員企業になっている団体でございます。

私たちの立場から、日ごろ困っていることとしまして、今、室長よりご説明いただきましたいわゆるアクティベーション方式のクラックプログラム等での回避ということについて、現状をご説明しまして、皆様にこの機会に触れていただけましたらと思っております。

まず、室長からもご説明がありましたけれども、不正競争防止法の技術的制限手段、いわゆる平成11年改正法の当時は、パッケージソフトウェアが出てきまして、パッケージ販売で、インストールメディアにソフトウェアが入っていて、それを販売店等で買ってきて、パソコンにインストールをする、ということが行われていたと思っております。

今では、回線も高速化し、ダウンロード販売ということが技術的にも可能ですし、その方が柔軟なライセンスプログラムをユーザーに対して提供できるということで、圧倒的にダウンロードモデルにビジネスモデルが変化してきております。

その中で、アクティベーション方式という言い方でご説明があったのですが、私どもはライセンス認証システムと呼んだりしておりますが、このシステムについてご説明させていただき、クラックプログラムがどう動くのかというお話をさせていただきたいと思いま

す。

この図の上段の方が正規に対価を払って、正規の制限なしバージョンになるまでの動きです。この下段の方がクラックプログラムを当てて、ライセンスの認証サーバーに行くことを妨げて、その認証を回避するという動きになります。

今、まず、無料体験版を試してもらい、実際に使うかどうかを決めていただいて、「よし、新しいバージョンにしよう」ですとか、「このプログラムを使おう」ということになったときに、製品版にお金を払うということが非常に多く行われております。この無料のバージョンを正規のメーカー等のダウンロードサイトからダウンロードしてきまして、パソコンにインストールしますと、その際に図の①に示されるように、体験版認証データ——後で認証済みという言葉が出てきますので、それとの対比で仮にこれを未認証のIDと呼びますが、これがパソコンに、このダウンロードにユニークなものとして生成されて、PCに保存されます。

そこに、当該ソフトウェアメーカーが定めた無料体験版の期間という、そのような情報等も保存されまして、1週間なら1週間、1ヵ月なら1ヵ月間でその体験版の制限期間経過後は、あるモジュールですとか全体ですとか、プログラムの実行が不可となるような仕組みが採用されております。

その途中で、「無料版を使ってみてどうですか。今度は正規版にかえて本格的にお金を払って製品版を使いませんか」ということで、「買いましょう」ということになると、この製品版用のライセンス認証のためのプロダクトキー等の製品版用のキーというものを入力します。そして、ここでお金の支払いもしながら、この製品版用のキーを入れて、これが行われますと、メーカー側の認証サーバーへの認証のリクエストが行われます。

ここで、当該デバイス、ハッシュ値等のデバイスを特定する情報と、その製品版の電子情報というものが行きますと、ここでデバイスIDと製品版情報を登録した上で、認証済みIDというものを返します。この信号を検知することによって、制限なしバージョンということで、期間制限もないですし、機能制限もないということで、パペチュアル・ライセンスですとか、そのライセンス条件に合った製品版としての完全な実行が認められることとなります。

我々は不正だと思ってエンフォースメント活動をしているのですが、そういう場面ではどうことが行われているかということ、1つは、キー自体を不正に入手してきて転売する。例えば、企業用のIDですとか、たくさん使えるようなIDを窃取してくる。または、

流出させる等。そして、このキーを入れることによって、こちらに通ってしまっただけで制限が無くなる。お金を払っていないのに制限が無くなるということもあります。

もしくは、この体験版を入れておいて、うまくキーが通らないということであれば、このプログラムをPCに当てることによりまして、ソフトウェアに組み込まれているファイル情報を書きかえてしまっただけで、権利者への認証サーバーへのアクセスを妨害します。そして、この製品版の認証データと同じような動きをするデータを偽造しまして、それをインストールされたソフトウェアに記録することによって、対価を支払うことなく、あたかも製品版のように機能の制限、期間の制限が解かれたものとして利用ができる。というのが、正規のライセンス認証の動きと、クラックプログラムを当てた場合の動きとなります。

これはオークションサイト等に行ってください、例えば「プロダクトキー」と検索していただきますと、かなりの数が出てきます。メーカーは、その「プロダクトキー」だけ転々流通させたりということはしておりません。本来は、ダウンロード販売の一環として、その「キー」による認証を行う。そういう販売方法です。

ところが、オークションサイト等では、プロダクトキーのみの販売です。ほかの物はメーカーのダウンロードサイトに行ってください。それが通らなでしたら、最後まで面倒をみます。そういう販売が行われていることが多々あります。その面倒をみますよという中で、このプログラムを当てていただければ認証も通りますので。そういう言い方をして、何ら制限のないものにしてしまう。そういうものが多数出品されております。

こちらは、あるオークションサイトでの出品について、BSA団体として削除要請をしている数です。BSA会員企業のみに限った数字ですので、実際には世の中の他のビジネスソフトウェアを数えればもっとたくさん出品があるのではないかと思います。月数千件から数万件の出品が行われております。それについて、2014～2016年にかけて刑事判決で有罪、不正競争防止法違反というものが出ましたので、その際には若干減るといって減少傾向はみられたのですが、エンフォースメントを続けていくことが必要と考えております。

その課題ですが、不正競争防止法上、2条7項の技術的制限手段該当性と回避行為の該当性が問題になるのですけれども、先ほどのアクティベーション、ライセンス認証のシステム自体が少し複雑で、最初に体験版を入れて、そこで未認証IDが入っていて、期間の制限、実行の制限がかかって、その後、新しい認証サーバーと認証してということなので、例えば、先ほどの時間的な問題ですとか、どこに記録されるのかですとか、昔のメディア、

記録媒体、インストールメディアをずっと頭に置いてあると、あちら側に信号が無いんじゃないとか、法的位置づけがなかなか不明であるとして、オークションサイトでも一概に削除するのは難しいですとか、捜査の協力をしている中でも、ちょっと難しいのではないかという話があります。

昔に作成されたものですけれども、準則においても、技術的制限手段の該当性等の記載がありまして、私どもは、ライセンス認証システムは、時代の変化とともに販売方法が変わっているので枠外と思っているのですが、捜査機関からは、もっとはっきり「不正競争防止法に違反するよ」というガイダンスが無いとやりにくいというところもありまして、エンフォースメントがなかなか思うようには進まずに、私どもが不正であるとする販売がそのまま放置されているという状況です。

資料に、刑事事件4件、民事事件1件の情報を載せております。

刑事事件4件はいずれも、クラックプログラム、今ご説明したようなものを提供した行為について、懲役、罰金等の刑が科されたという事件になります。

民事の方は、神戸地裁の刑事の事件の後に、民事の裁判も行って、損害賠償請求もしたという事案でございます。この中で、チェックマークの3つ目をみていただきますと、不正競争該当性について、ライセンス認証システムについて技術的制限手段該当性を認定して、回避行為についても認められたという判断となっております。

最後はまとめページになります。ビジネスソフトウェアのライセンス提供がパッケージからダウンロードに大きくシフトしておりまして、ただ、このライセンス認証システムはその技術の方も非常に高度になってきておりますが、なってきた分だけ、平成11年当時に書かれた条文については逆に読みにくくなってきているのではないかと。

そういうことがありまして、この定義や回避行為の明確性によって十分なエンフォースメントができるように、今の時代に合った、できれば改正をしていただきたいというのが私どもの希望でございます。それによって、分からないとか、疑義がなくなっていく、認証に関わる時間が長いので『ともに』ではないのではないかという疑義が生じるままの状態が放置されない、ということを望んでおりますので、参考にしていただければと思います。

ありがとうございました。

○中川 コンピュータソフトウェア著作権協会の中川と申します。

先ほど、BSAの方から、ビジネスソフトに関する回避の実態についてお話をいただき

ましたが、ゲームソフトについても簡単にご紹介だけさせていただければと思います。

ゲームソフトと一概にいいましても、これまでのように、パッケージを買って、それでおしまいといったようなゲームから、昨今では、ダウンロードをして追加でお金を払うことで新しい面で遊ぶだとか、また、最初は無料で遊べる部分があるのだけれども、途中からお金を払って使っていくといったようなゲームの体制が増えてきています。

ただ、ゲームソフトを一般的にこういうものということでご説明をしづらいですので、全てが全てこれに当てはまるものではございませんし、また、多くのものということでもないのですけれども、実際にアクティベーション方式を利用しているゲームとしては、ダウンロードしたものについて、アンロックをして新しい面に進むであるとか、また、スマートフォンのアプリのスパン搭載のゲームなどについては、無料で遊べる部分と有料で遊べる部分を別途でもっていて、有料で遊べる部分についてはお金を払わないと遊べない。そういったものが多いというイメージをお持ちいただければと思います。

普通に使う場合であれば、課金情報と端末情報、ユーザーのID等をサーバーと認証することでロックが外れて使えるという状況になる。ただ、不正な利用をする場合は、ゲームソフトそのものを改変する。また、ゲームソフトの端末側にもってありますそういった認証済みのIDを偽装して、サーバーと認証させないようにするなどの行為が行われており、そういったビジネスソフトのいわゆるライセンス認証システムと似たようなシステムを使っているということだけご紹介させていただければと思います。

ありがとうございました。

○岡村委員長 大変ありがとうございました。

それでは、今のBSA様とACCS様からのご説明と事務局からの説明、それから、先ほどのMONIC様からのプレゼンテーションも含めまして、どの点からでも構いませんので、ご意見、ご質問がございましたら、お名前の札をお立ていただければと存じます。多少お時間が押しておりますが、よろしく願いいたします。

○諸永室長 1点だけ、事務局から、資料の取り扱いに関してでございます。資料6の3ページ目の「オークションサイトでの出品の実態」でございますが、これはオークションサイトなので日々どんどん変わっていきます。ですから、こちらの資料は今日この場では使いますけれども、ホームページにアップする資料からこの3ページ目だけ削除する形で公表させていただきますので、ご了承をよろしく願いいたします。

○岡村委員長 では、相澤委員、よろしく願いします。

○相澤委員 事務局から説明がありました資料5について、「データ」はありとあらゆる情報を含むので、極めて広範な範囲になります。したがって、データというだけでは、対象が不限定になるのではないかと思います。

アクティベーションその他を含めて、現行法でどういう場合が侵害になって、どういう場合が侵害にならないのかについて、著作権法等も含めて、明確にする必要があります。

それから、「技術」は、どんどん変わるので、技術的対応ができるのであれば、さらに、立法の必要があるのかということを考える必要があります。

トレーサビリティについては、パッケージ型についてはそのパッケージが不正なものだということを追跡するのによかったと思います。ただ、今は、ネットワークでつながっているので、個人情報保護の問題も生じるおそれがあります。追跡情報により、個人の情報が集積されることとなります。ヨーロッパの場合は規制が厳格であるということがありますので、それも含めて、トレーサビリティを広げていった場合に問題がないかということを考えていただいた方が良いでしょう。

○岡村委員長 ありがとうございます。

では、引き続き、高山委員からお手が挙がっていますので、よろしくお願いいたします。

○高山委員 B S A様に確認の質問をさせていただきたいのですが。ご発表の事例のご紹介として、一方で、裁判所では民事・刑事で有罪とか損害賠償を認める判断が出ているけれども、捜査機関の方で立件に至らないケースがあり、また、スライドの3番目などをみますと、オークションサイトでかなり堂々とした形でこういうものが販売されているところからいたしますと、いろいろな場面で人々の認識が全くばらばらではないかという印象です。

裁判所の違法判断の方がちょっと勇み足的になっているのか、それとも一般のオークションに参加している人であるとか、あるいは捜査機関が無自覚であるのか、全体を御覧になって、どのような印象をもっておられるかをお聞かせいただけますか。

○岡村委員長 B S A様へということでしたので、よろしければ、水越様、お願いできますでしょうか。

○水越 この問題は、まず、オークションへの出品者ですけれども、出品者は確信犯です。次から次へと出品をして、そこでうまくいけばお金が入るし、うまくいかなければ入らないだけ、という。もちろん、刑事の判決が出たときは、逮捕を免れたいという思いもありますので、数が減ったりですとか、また、しばらく無いとふえたりですとか、自

分たちの手間をかけないで利益を得ようということに確信をもっている方々は、違法か適法かということは余りにせずに動きをしているように思われます。

私どもはこの2条7項の条文を何度も何度も読みまして、裁判所に対して意見書を出したりですとか、検討をしておりますので、この記録媒体記録方式に該当することについてそれで良いと言っていた裁判所のご判断どおり、という気持ちになっているところなのですけれども、この方式を限定する条項を読むときに、記録媒体というのはCD-ROMではないかと思った途端に次に進みにくいというところもあります。恐らく捜査機関としましては、例えば経産省さんなりが、こういう場で、この判決も段々オーソライズされてきて、これがコンセンサスなのですよ、ということであれば、さらに安心されるのかなと思います。そこがどの程度どちらが及び腰かというのは、なかなか難しいところでございます。

○高山委員　　ありがとうございました。

○岡村委員長　　今のこととの関係で、基礎的な事柄を整理するために、釈迦に説法だとは存じますけれども、付加してご説明いただければと思うのは、著作権法では、プログラムというのは著作物であるということに間違いはないわけですが、著作権法でこの問題の解決は対処できないというのはどういう形なのかということ、補足的に簡単にご説明いただければと存じます。

○水越　　ありがとうございます。著作権法も、もしTPP関連の改正がなされまして、アクセスコントロールまで幅広くカバーするということでしたら、そちらには私どもも期待していたところなのです。しかし、その改正が今ペンディングというところもございしますので、今の、コピーコントロールを、また暗号化について制限をしている著作権法では、ダウンロードで記録をして、実行について制限をかけていくというアクセスコントロールという形で制限するものには及ばず、不正競争防止法を頼りにしている、という理解しております。

○岡村委員長　　要するに、現行法では、プログラムはアクセスコントロールの対象には規制が及んでいないという趣旨ですね。

○水越　　著作権法ではということでしたら、ご指摘のとおりと思います。

○岡村委員長　　ありがとうございます。

では、野口委員、よろしく願いいたします。

○野口委員　　ありがとうございます。BSAさんにお尋ねをさせていただきたいのです

が、資料の4ページでデータが出ておりますが、合計数、月平均数等を拝見いたしますと、年々、被害状況自体、件数は減少しているように拝見するのですが、こちらでご紹介をいただいたような、例えば、刑事罰、民事訴訟のようなところで現行法でもある程度対策ができていくゆえであるのか、何かご見解をいただければと思います。

○岡村委員長　では、水越さん、よろしく願いいたします。

○水越　ありがとうございます。特に昨年末ですと、民事も含めて、私どもで刑事と民事の判決が出ましたと広報しておりますので、その広報時にはよい影響がみられるところですが、ただし、時間が経ちますと戻ってってしまうということがあります。2014年ごろにとっても増えて、また、2015年も例えばひと月に2万6,000とかという数字があるのですが、少し広報に休みがありますと数が増えるということがあります。少なくともエンフォースメントは確実にできるという状況でないと、自主的な解決は難しく、そういう判決を経て、その抑止力によって効果が出るということですので、確実なエンフォースメントができる環境は必要であると考えております。

○岡村委員長　ありがとうございます。野口委員、よろしいでしょうか。

○野口委員　はい。ありがとうございます。今の点は、主に検討事項2のところ、この「ともに」というところが逆に支障になっているので、ここを改正すると、BSAさんの取り組みとしては大きく改善されると、こういう理解でよろしいでしょうか。

○水越　ありがとうございます。いろいろとやりとりをしておりますと、やはりひっきりやすい条文の文言でございますので、特に「ともに」という時間なのか場所なのか、ですとか、先ほどハードウェアに記録という話をしましたけれども、例えば、技術的な変化によって、メモリーだったらどうかですとか、USBと分離していたらそこは同じなのかとか、いろいろな技術のちょっとした構成の違いでこれに該当しないというのも少しおかしいと思っておりますので、やはり「ともに」というのは限定的にすぎるのかなと考えているところです。

○岡村委員長　野口委員、いかがでしょうか。

○野口委員　はい、ありがとうございました。今の点はその点としまして、もう1点、検討事項1については、先ほど相澤委員の方から、データというのがその対象として特定性があるのかどうか、そうでないと何でも対象に入ってしまうのか、そういう問題意識のご指摘がございましたけれども、その点については私も同じような印象をもっておりまして、どのあたりにどんな立法事実があるのかについて、より掘り下げをいただけると大変

ありがたいかなと思っております。

あわせて、行為の点で、現在、視聴、実行、記録という行為が入っているところを行為として、さらにコンピュータによる分析というものを加えたらどうかというご提案と私の方で理解をしていますが、こちらは分析をする前に何らか記録をされた上で分析をすることも多いのではないかといます。したがって、コンピュータによる分析の前行為として必ず記録があるのであれば、そこでつかまえば良いので、これをさらに足す必要はないような気もするのですが、その点、特に記録をされずに、コンピュータでの分析のみが行われるということがどの程度あるのかないのかについて、事務局にご質問させていただければと思います。

○岡村委員長 事務局へのご質問ということですので。

○諸永室長 ありがとうございます。冒頭の相澤先生からのご意見と同じ意見の部分もあると思いますが、映像、音に加えてというところは、引き続きニーズ調査などをしながら、そして今日この場でも、こういうニーズがあるよということがあれば、むしろご意見としていただきたいと思っています。我々として、この部分は文言上多分足りない部分があるかなと思いつつも、先生方がおっしゃっているように、データとってしまくと非常に範囲が広いということも我々は認識しておりますので、むしろその部分をご検討いただきたいというのが1点でございます。

もう1つ、記録ということに関しましても、すべてが記録に当たるのか我々は把握していない部分もございますので、まさに同じようにご意見をいただきつつ、そして、引き続き、委員の方々なども通じてご意見を集めていきたいと思っていますので、あわせてご意見をいただければと思います。

○岡村委員長 ありがとうございます。

林委員、お願いいたします。

○林委員 ありがとうございます。2条7項は、現行、機器に着目した規定の仕方になっているのですが、機器に着目した規定を前提として、「ともに」要件の解釈の明確化とか、不正改造などの無効化サービスの提供も対象とするといった、その限度の見直しをして、もっと広い意味でのアクセスコントロールは、本日の議題の資料3にある別の不正競争行為類型として考えるという事務局の整理なのでしょうか。

といいますのは、アクセスコントロールを正面から考えるということであれば、その行為は重なる部分があり、現状の7項での規制の対象をどこで線引きして考えるのかという

のが、今、わからなくなっているのですが。あくまでも、本日の議論の設定としていただいている7項関係は、機器に着目した規定の範囲でというお考えなのでしょうか。

○諸永室長　ありがとうございます。まず、発射台としては、現状の条文での足りる足りないということで機器に着目して、そして、もう一方で、先生がおっしゃっているようなところというのは、行為の方も注目してといったご議論だと思いますので、分けて、でも、この場で両方いただければと思っています。

そして、最後に、テクニカルに条文をどうするかというところは引き続きご相談させていただきながらやっていきたいと思いますが、いきなりこれを全部チャラにしてもう一度なのか——というよりも、まず、現行法から発射台にしつつ、足りない部分は、今日の場合、これは行為規制をもっていたと、ご意見をいただければと思っています。

○林委員　わかりました。私の思いでは、7項の機器に着目した規定のあり方自体が当時の被害状況に基づいたものなので、もう時代に合わないのかなという認識をもっています。そこからひっくり返すのではないという前提でも、全体のセキュリティとしては、切れ目のないセキュリティをすべきだと思っていますので、トータルで立法事実に応えることを考えていきたいと思っています。

○岡村委員長　ありがとうございます。時代に即してというのは非常に貴重なご指摘であると受けとめさせていただきました。

では、引き続きまして、宮島委員、よろしく願いいたします。

○宮島委員　ありがとうございます。私自身は、普段、知財のこういった具体例を扱っていませんので、多少ふわっとした意見とご質問になると思いますけれども。

1つは、営業秘密も含めて、知財に関しましては、十分な保護と十分な有効利用というところのはざまに議論がいつているので、保護をするというような部分は守りつつも、それが有効利用を妨げるようなことがあってはいけないのではないかと思います。

あと、今の「ともに」という部分に関しては、私も印象としては、まさに時代の変化に対応するという意味で条文の変更をするべきではないかと思うのですが、こういった法制度は、どうしても具体例が積み上がった後に法制度をいじるということになるしかないのかなと思いつながらも、もしも今後の技術の発展などが多少先行きがみえるような部分があれば、たった今できた機械とか、たった今できた方式に限らず、少し幅広に考えるような文言を考えられるのであれば、難しいかもしれませんが、常に後手後手にならない

ような法改正ができれば良いなと思います。

その上で、私は今のさまざまな中で思いましたのは、現実の状況が変わって、意識は同じだけれども、単に方式や扱いが変わったものに関しては、時代に合ったというところで改正していけば良いのだと思いますが、改正したことで情報のルーツを妨げそうなものの中には、今ご指摘があった検討事項1の、データを全部対象にしてしまうと行き過ぎではないかというのがあり得ると思っています。

それから、もう1つは、この中で、「より慎重な処理を」と書かれている部分に関しては、データの流通との関係において指摘があるところだと思います。

お伺いは、ほかの部分で、事務局としてご提示いただきながらも、データの利活用の活用の部分としては、もしかしたらひっかかるかなと思う部分があれば、教えていただければと思います。

○諸永室長 我々も、今日の1つ目のご紹介の部分もそうですが、データの利活用が前提となっていると思っていますので、その部分は阻害したくないと思っていますし、そのようなルールづくりをしたいと思っています。

そして、今、宮島委員からご指摘いただいた点ですが、我々が思っているのは、まさにその1つ目のところと、情報提供というところが、そのバランスの部分があると思いますし、もう1つ、トレーサビリティの部分に関して、外す、外さないというところは、今日も個人情報が含まれるかというところがありますので、その部分はどちらに触れるか、正直、我々も見極められていない部分がございますので、ご検討いただければと思っています。

○岡村委員長 ありがとうございます。

次の池村委員のプレゼンテーションの時間もございますので、最後に、この論点に関しましては大水委員からのご質問をいただいて、それで次に移りたいと思います。

では、大水委員、よろしくお願いいたします。

○大水委員 2点ございます。

まず、BSA様からコメントをいただきたいと思います。アクティベーションモデルというのは、CD-ROMのモデルの次に出てきたダウンロード・アクティベーションという形なのですが、最近、サブスクリプションといいますか、そもそもデータ自体をクラウドでやってしまうという傾向もございまして、そういった流れの中で案件が減ってきているのかなとかんぐったりもしてみたのですが、将来的な流れとしてはどのようにお

考えでしょうか。

○水越 ありがとうございます。もちろん、私どもの会員企業もクラウドサービスには非常に力を入れているところでございます。そうはいいまして、プログラムについては、スピードですとかいろいろなニーズ、規模、管理を含めまして、ダウンロードをしてインストールをするというのも非常に大きなニーズがありますので、ビジネスがどちらかだけになっていて、それが被害状況に影響を与えているというのは、ちょっと別問題ではないかと思えます。両方とも重要なビジネスモデルであって、オークション等においては、そこでお金を得たいという人が活躍をしているという状況ではないかと思っております。

○大水委員 一般的にみると、大手のかなり高いソフトウェアの会社様は、どちらかというサブスクリプションに移行しつつあるという認識がございましたものですから、質問させていただきました。

それから、先ほどから問題になっています映像とプログラムとデータという関係のところなのですけれども、今、保護をされている対象というのは、もともとそのコンテンツ自体に価値があるとそれなりのコンセンサスができていた音楽であったり、映画であったり、ソフトウェアプログラムであったりというものに対するということでございまして、データ一般となりますと、果たしてデータの中にそもそも本当に価値が今あるのか。あるいは、私個人の見解では、実はデータの多くは、それを外からアクセスをして何らかの処理をすることによって価値を見出されるタイプのものが多いのではないかと。内在する価値ではなくて、むしろそれを処理する側が価値を付加しているというような面も結構あるのではないかと。

そういったものに関して、広く、内在的な価値があるものと同等のアプローチをするのが適切かどうかというところについては、慎重に事例を考えながら検討しなければいけないのではないかなという違和感をもっております。

○岡村委員長 最後の点のご意見ということですね。

○大水委員 はい。

○岡村委員長 それでは、その点にも関連しますので、次の議題の「技術的な営業秘密の保護の在り方について」に移りたいと思います。

まずは、事務局から資料の説明をお願いいたします。

○諸永室長 岡村委員長、ありがとうございます。

それでは、資料7、そして参考資料1に基づきましてご説明させていただきたいと思

ます。

まず、参考資料1の14ページ目を御覧いただきながら、資料7をみていただければと思います。

ここで議論したいところは、現行法において、営業秘密に関しまして、それが実際に第三者なりに不正に取得されて、そして、それを使って物がつくられているであろうという状況のもとにおいて、それを使用したのか、使用していないのかといったところの立証を、推定を働かせるというものがございます。とったことが明らかで、それを使えばつくれる物をつくり続けていて、そして、使用に関しては民事訴訟が前提でありますけれども、民事訴訟において外からはとられた側の営業秘密と、とった側の営業秘密もありますので、外からは使用行為に関して立証することは困難です。そこで、昨年1月1日に施行されています法改正において、営業秘密を使った物の生産ということに関しましては、推定を働かせるという規定が既にごございます。

その中に、さらに政令として、その他情報という文言があり、こちらの方を定めていくのかということをご検討いただきたいと思います。

そして、資料7に関しまして、その生産というのを入れたときの観点などもご説明しながら、今回の具体的な事例に入っていきたいと思います。

まず、資料7の1ページ目の1. 前提でございますが、当時、立証責任は公平に配分するという観点から、そして、2つ目のポツの部分が大きいと思いますが、民事訴訟を起こす際に、被告側が外から侵害したというのを立証するのは非常に困難であるというところが大前提だと思っています。一方で、逆に、訴えられた側が反証していくことが容易かどうか、この辺も観点として必要とされております。

もう1つ、最後のポツでございますが、濫訴の防止ということで、これは本当に侵害していないにもかかわらず、このような規定を使って営業秘密などをみせろといった形での訴訟などが起きないようにといったところも含めてのご議論ではございます。そのような営業秘密は、例えば取得までは明らかで、その取得においては民事訴訟も行われている上で、さらに、その使用の部分まで裁判の中で白黒をつけて、そして損害賠償であるとか差止めを行うのかということも重要な観点だと思っています。

そして、原告側の立証事項として、生産方法とその他ですが、その他というところにおいても、「政令で定める」と書かれている部分が2ヵ所ございます。政令で定める技術上の営業秘密という観点と、当該技術を使用したことが明らかな行為として政令で定める行為、

この2点が、これは恐らくパラレルになると思いますが、セットでご議論いただきたいと思っています。

具体的に、2ページ目でございますが、本日、この後、池村委員からプレゼンテーションもいただきますけれども、これは法律をつくった際にもこのような事例があるというご意見、そして、施行に向けてというところでさまざまなご意見をいただく中で、いただいたご意見をまとめたものでございます。

まず1つ目が、①化学分析方法でございます。これは、例えば血液の成分などを分析して、疾患の可能性を検査で明らかにしていくような技術が、営業秘密を使ったサービスとしてあるのではないかとのご指摘でございます。

そして、②画像分析方法ですが、これも2つ例を書かせていただきました。例えば、画像を撮って生体認識をする。それから、よく使われているのが、実際の工場のラインなどでの最後の検品でも使われている。この部分に関しましても、特許を取得するというよりも、営業秘密としてノウハウで守っている部分が現状多いと伺っております。

そして、その他として、ちょっとフォントを落とした形で書かせていただいた部分は、こういうものもあるのではないかなということで、ご意見としては、委員の方々などからいただいている部分でございますが、実際に現状のニーズとして強くいわれている部分は、①、②の部分でございます。

そして、このような部分に関しまして、3ページ目の3. 検討の視点ですが、今、2つの例を挙げておりますけれども、それも含めて今回ご議論いただきたいと思っている部分が、さらに、「その他政令」として追加していくものとして何がふさわしいのかをご議論いただきたいと思います。

その際の視点や留意点に関しまして、繰り返しになりますけれども、原告の立証困難性が存在すること、そして、訴えられた被告側の反証容易性が認められること、そして、実際の盗まれた技術と被告が行っている行為との関連性があること、このような3つの視点が大それたと思っております。実際に条文があっても使われないということがないようにということで、とられて使用している端緒のようなところが実際に明らかなのかということも、冒頭申し上げましたけれども、不正な取得にとどまらず市場の行為まで立証することが重要なという、差止め請求や損害賠償請求の必要性を考慮いただければと思っております。

そして、具体的なイメージとして、化学分析方法、画像分析方法、そして、ここに案1、

案2と書いております。これは今日ご議論いただくために、何も案がないと議論しにくいかなということがございましたので、書かせていただきました。

例えば、案1は、「当該化学分析方法を使用しなければ実施することができない役務の提供」というように、かなり立証する側が証拠などをそろえなければいけないというものでございます。

案2は、真反対で、「当該化学分析方法を使用して実施することができる役務の提供」ということで、両方とも極端過ぎるかなとは思っていますが、この間ぐらいのところでは何かいい文言などがあればということも含めて、アドバイスやご意見をいただければと思っています。

そして、ここに、①、②がふさわしいのかとか、さらに③、④として何か追加のものがあれば、ご意見をいただきたいと思います。

そして、先ほどからのニーズ調査ではございませんが、今日もこの場でもニーズをいただきつつ、さらに委員の方々にご協力いただきながら、今後のニーズなども調べていきたいと思っています。

以上でございます。

○岡村委員長　　ありがとうございました。

続きまして、今の説明に関連して、池村委員にプレゼンテーションをお願いしております。

では、諸永室長、ご紹介をお願いいたします。

○諸永室長　　ありがとうございます。池村委員の方からご説明いただきますけれども、もともと法律をつくる段階から、味の素さんの方からはさまざまなご意見をいただきまして、その中で、今回、具体的なイメージも含めてご紹介いただく形でお願いしております。

それでは、池村委員、よろしく願いいたします。

○池村委員　　経団連の知的財産委員会企画部会の委員をやっております池村と申します。ご依頼がございましたので、説明をさせていただきます。

これは当社の疾患を検査・評価するサービスとして、アミノインデックス®という名前でサービスをもう既に行っている技術です。この技術の概要と、諸永室長からお話がございました不競法に関してどのような観点で議論の参考にできるかということで、説明をさせていただきます。

まず、アミノインデックス®は、そもそも生体内のアミノ酸を分析して、疾患の可能性、

リスクを評価するというサービスです。前提ですけれども、皆さんご承知のように、人間の体の血液中にアミノ酸がぐるぐる回っている、その前提としましては、体の20%はたんぱく質でできていて、たんぱく質はアミノ酸からできているということがございます。

アミノ酸はどのくらいあるのかというと、ざっくりいうと、20種類のアミノ酸が体の中にあります。それがあある割合で存在しているのですが、各アミノ酸によってその量は違います。ただ、同じ人でみても、例えば朝一番であるとか、食事の影響を受けるのですが、ある時間でみると大体一定の割合で存在しているということがわかっております。

これではがんという疾患をみているのですが、ある疾患状態になるとそのバランスが崩れるということがわかってきております。この図はみづらいなのですが、先ほどアミノ酸ごとにいろいろな量の比率があると言いましたが、これを全部ならして、健常人のバランスを、この真ん中の丸にしています。一方で、こちらの折れ線となっている図は膵臓がんの患者さんで、ステージⅡBというのは早期です。それから、全ステージ——かなり悪くなっている方も含めてみると、このきれいな丸であったものが、こういうでこぼこになってくる。でこぼこになってくるのが、早期のがんの状態から出てきて、膵臓がんであればこのような一定の形に、これはいろいろな患者さんの平均値ですので、ぴったりこの形になるというわけではありませんけれども、これに近い形になってくる。

それらが、胃がんとか肺がんとかほかのがん種においてもそれぞれ特徴的な形になってくる。実際ががん患者さんの血液を分析することによってこういうことがわかってきました。それが具体的には、大量の臨床データを蓄積して、それを解析することで、多変量解析という、今でいうAIにこのデータを食わせて、それで学習させて、学習済みモデルが出てきたというのと同じような考え方で良いかと思うのですが、これは一つのアルゴリズムになります。算式ですね。

その算式でみると、健常人では大体こういう分布になって、がん患者ではこうなります。これは模式的にあらわしたものですので、これほどきれいになるかというのはいろいろあるのですが、こういう違いが出てくると。そうしますと、がんであるかどうかわからない患者さんの血液を分析したときに、どっちに近いのですかということで、そのリスクを評価するという方法です。

具体的には、これはアミノインデックス®・キャンサー・スクリーニング (AICS®) という名前でサービスを行っているのですが、男性についてはこの5種類のがん、女性に

についてはこの6種類のがんについて、1回の採血で各がん種のリスクの評価がなされまして、A、B、Cというリスクとして評価されます。

具体的に、この技術の流れとしては、最初に健康診断とか、病院に行って検査を受けるというような場で、まず、採血をします。そして、その採血で血漿と血清との分離をして、その血清部分のアミノ酸の分析をして、その分析したものをデータとして取り込んで、先ほどアルゴリズムといいましたけれども、既に大量のデータから処理されて得られているアルゴリズムに入れ込むことによって評価される。その評価をもって検査結果として本人に通知される。こういう流れでのサービスになっております。

不競法の観点で少しまとめてみましたが、5条の2のところに、「技術上の秘密を取得した者の……」と書いてございますけれども、ここの推定規定のところ、立証責任の転換で規定されているのが、諸永室長からご説明がありましたように、物の生産方法と別途政令で定める技術ということになっていますが、ここが今までまだ具体的なものが出ていないということで、ここに当てはめてみたのですけれども、政令で定める技術の例として、「血液中のアミノ酸組成の分析により疾患である可能性を評価する技術」としております。

そして、当該技術を使用したことが明らかな行為として、「被告が採血により幾つかの疾患の可能性を評価する検査サービスの提供を開始」。というと、どんな技術でやったのだろうということになって、疑わしいのではないかということになるかと考えております。

これは先ほどの絵ですけれども、実際、被告がサービスを始めて、採血をしましたと。そして、その結果を返却して、そのサービスをやっていますという、ここはわかるのですが、では、具体的にどのような技術を用いてこのサービスとしているのかというのは、ブラックボックスですので、原告の立証が困難であるということかと思えます。

それから、被告が独自技術を使用したと主張する被告の反証の容易性というものもあります。

この技術の一番大事なところは、大量の患者さん、そして健常人のデータに基づいたインデックス、アルゴリズムなのですが、この技術の確立には、大量の患者さん、健常人から血液データを取得して、それで分析するという、そういう長年の研究開発が必要で、原告技術と被告行為との関連性の疑いがここでもたれるということになります。

仮に、アミノ酸分析を実施してやっているということが被告の行為としてわかれば、原告の営業秘密がとられたのではないかという疑いがそこでもたれるのではないかと。

そして、これは差止めする必要があるのかどうかということですが、結局、こういうサ

ービスを提供されることによって、もともと技術をもっていた原告の機会損失ということになりますので、差止め請求、そして損害賠償請求が必要だと考えております。

説明は以上です。

○岡村委員長 大変ありがとうございました。

それでは、事務局からの先ほどのご説明と今のプレゼンテーションに対しまして、どの点からでも構いませんので、ご意見、ご質問がございましたら、よろしくお願ひいたします。

では、野口委員、お願ひいたします。

○野口委員 単なる確認ですが、資料7の1ページで、その他の技術についてで、「被告による違法な取得行為があったこと」というのが要件ですので、例えば、今の池村様の最後のスライドでも、当然、こういう長期間の研究開発が必要であろうものについて、被告がこの行為を始めたということに加えて、当然、被告による違法な取得があったということをあわせて立証が転換されるという理解でよろしいですね。そこの確認だけです。

○諸永室長 はい、そうです。

○岡村委員長 それでは、長澤委員、お願ひいたします。

○長澤委員 データのことが先ほどから話題になっているので一言話します。私は実は今日プレゼンをお断りしています。理由は、私が何が守るべきものかを大勢の前で話してしまうと、ハッキングのリスクが高くなるからです。

ほとんどのデータは営業秘密で守れる可能性が高いと思っています。ただ、そうでないデータも事実上存在すると思っており、大水委員がいわれたように、何かのプログラムと一緒に使わないと有効性が出ないものもあれば、実はデータ単独で有効性が出るものもあり、データそのものを盗みたくなる場合があります。そのようなデータは当然、それ単独でビジネス上有益であることは間違いないのですけれども、これはデータそのものはある意味非公知とは言えない場合もあるので、秘密管理性や非公知性がなかなかうたえないものが存在しています。このようなデータについてはこのオプションが使えば良いと思います。

ただ、一方、相澤委員がおっしゃったように、広げ過ぎると大変なことになるということも非常によく理解できます。それに関しては何をもって不正とするかによって、かなり制限をかけてもらうしかないと思いますが、明らかに、相当量のデータになりますけれども、そのデータそのものがあるビジネス的な価値を生み出すものがあります。

それから、第2条7項の話がさっきから出ていますけれども、「何々とともに」というのが同じ記録媒体とか同じときに送信されるというのは、逆にむしろまれになっているのではないかと思っています。恐らく皆さんがメールを出すときに、パスワードを添付書類につけて、そのメールに張りつける人はいませんよね。それと同じで、別の手段でユーザーに通知するのが今は普通であろうと思っています。

ですので、「ともに」というのがそこまで広く解釈できるのであれば良いのですが、「一緒についてないじゃないか」という議論を呼ぶのであれば、特許を書いている私だと、恐らく一番広く書くと「関連つけられた状態で」と書くと思います。関連は広すぎるということになると、今度は「リンクされた状態で」などという言葉を使うと思ういます。いずれにしても、この文言はかなり慎重に記載してほしいと思います。最低限、「同時に」もしくは「同じ媒体に」とは読まれないようにする工夫は必要かと思っています。

○岡村委員長　今の点は、パラメーターも営業秘密に当たるかどうかということも問題になり得ると思いますが、インプット・アウトプットについて、機械自体をリバースエンジニアリングされると、リバースエンジニアリングの前には結構脆弱かなと思いますので、営業秘密それ自体でどこまで守れるのかなという論点も付随してあり得るかとは思っています。

では、大水委員、お願いいたします。

○大水委員　2点ございます。

1点は、事務局の方に確認を念のためにさせていただきたいのですが、ここでいっている立証責任転換の話というのは、あくまでも営業秘密という前提のもとでの議論ということで、資料3で、営業秘密に加えて、データを保護するというお話のところまでは考えなくて良いということで、よろしいですか。

○諸永室長　5条の2の部分の、営業秘密であるものがさらに不正取得をされてという、先ほどの野口先生のご質問と同じで、その先にといった立証の部分だけでございます。

○大水委員　次は、池村委員にご教示いただきたいのですが、AIをというお話がございましたので念のためですけれども、ここで不正に取得される対象となる営業秘密というのは、AIの観点でいくと、学習用のデータセットなのか、それとも学習済みのモデルが盗まれるイメージなのか。そのあたりを明確に教えていただければと思います。

○池村委員　一般的には、学習済みモデルという理解をした方が良いとは思いますが、ただ、この場合にちょっと特殊なのは、薬の開発でいうと臨床試験でかなりの費用をかけてデータを取得すると。こちらの方も、がん患者さんから病院とかお医者さんをお願いを

して採血をして、それでデータを集めるということがございますので、健常人のデータであれば外せることもあるかとは思うのですけれども、努力して集めた患者さんのデータについては、保護の対象としたいとは考えております。

○岡村委員長　　よろしいですね。

では、相澤委員、よろしくお願いいたします。

○相澤委員　　刑事罰が課される条項につきましては、構成要件を不明確にするわけにはいかないのです、明確な限定は必要であると思います。もちろん、民事についても、不特定で良いというわけではありませんが、刑事については特に配慮が必要であると思います。

それから、分析方法については、特許も含めて、保護が不十分な状態にあります。この問題の解決には、立証方法をどうするかが重要です。立証について、立証責任の転換だけではなく、文書提出命令等を含めて、手続の改善を考えていく必要があります。

被告のみが証拠を有している場合に、知的財産権を保護するためには、方法の特許の場合も含めて、手続の改善を考えていかなければいけません。

その流れのなかで、立証責任の転換については、積極的に考えていただければと思います。

○岡村委員長　　ありがとうございました。

では、鈴木委員、よろしくお願いいたします。

○鈴木委員　　今相澤委員から出たところに関連してですが、池村さんに今日プレゼンいただきまして、資料8の8ページの不競法の推定規定に関する検討のところ伺いたいと思いましたが、例3で挙げられている「評価する検査サービスの提供開始」というときに、考えておられる差止めの行為の対象というのはどういうことになるのでしょうか。

○池村委員　　これは、疾患のリスク、可能性を評価する方法だととらえていますので、その方法を提供するサービスを差止めの対象としたいと考えています。

○鈴木委員　　ということは、サービス方法そのものということですか。

○池村委員　　そうですね。検査サービスということであれば、そのものと考えています。

○鈴木委員　　そうすると、もともと5条の2の本文で書かれているのが、「使用する行為により生ずる物の生産」と、「その他技術上の秘密を使用したことが明らかな行為として政令で定める行為」ということで、政令で定められるべき行為としては、「使用する行為により生ずる物の生産」行為と同等のものが定められるべきかと思いますが、今おっしゃった例で、方法自体を推定し、その方法の差止めを求められるということになるのだとすると、

政令で定める範囲より少し広がる感じがするのですが、「物を生産する方法の発明」と「方法の発明」とは明確に裁判例でも区別されていますし、そのあたりはどのようにお考えでしょうか。

○池村委員　少し理解が追いついていないのですが、その他政令で定める行為、その行為の中に疾患を検査する方法と理解をしています。その方法を差止めること、イコール、サービスを差止めると理解をしているのですけれども。

○鈴木委員　そのあたりが、その生産方法の例1と例2で挙げられているものとは、ちょっと類型が違うような気がするのですが、質問させていただいたのですけれども。

○池村委員　もともと例1と例2でカバーされていないものを政令で定めていただきたいというのが、こちらから不競法の改正のときに申し入れたことでして、それで、「政令で定める」ということを一文入れていただきましたので、例1、例2ではカバーされていないと、もともとそう考えています。

○鈴木委員　政令では、法律で定められているところ以上のものは定められないため、政令で具体的にどこまで規定できるのか、方法そのものを規定することができるのかについてはちょっと疑義があるのかなと思っておりました。

○岡村委員長　ありがとうございます。今の点も参考に、また事務局の方でもご検討をお願いしたいと思います。

これはつけ足しで池村委員にお聞きしておきますと、これは解析センター内でされておられるだけで、外へプラントとして販売されている、検査システムを外販されていると、そういうことではないのですね。

○池村委員　現在のところはないのですが、ただ、今後、例えば、これを海外に展開するとなったときには、ライセンスをして他社さんにやっていただくとか、そういうことはあります。同様に国内でも、パッケージとしてそのサービスをどこかにライセンスするという事は将来はあり得るとは考えています。

○岡村委員長　ありがとうございます。

では。長澤委員、どうぞ。

○長澤委員　先の不競法改正時に味の素さんと弊社と帝人さんとで参加していたわけですが、そのときに、やはり生産方法だけではないということを産業界からかなり強く主張した経緯で、この書き方になったと私は理解しております、それが生産方法の枠を出ないということであれば、政策室に裏切られたかと（笑声）、ちょっと思ってしまう。冗

談ですけれども。

それから、もう1つ、細かい話ですけれども、資料5の11ページで、「電子透かしのようなものを外すことは、違法な行為や社会の混乱へとつながるおそれがあり、決して認められない」とあるのですが、実はビジネス上そういうニーズもありまして、例えば、非常に繊細なプロのカメラマンが撮った写真は、電子透かしがみえてしまうと使い物にならないとまでいわれる可能性がありますので、著作権者の了解をとって外すこともあり得ます。それは別に不正ではないと思っていますけれども、著作権者の了解をとって、「これは電子透かしを外してご提供いたします」ということもできるということを考慮していただければと思います。

○岡村委員長　ありがとうございます。

それでは、最後に、相澤委員、よろしく願いいたします。

○相澤委員　鈴木委員がおっしゃられたのですけれども、物と物の生産方法に関する現在の特許法のアナロジーを必ずしもここに持ち込む必要はないのではないかと思います。

○岡村委員長　ありがとうございます。

では、時間がまいりましたので、事務局から次回以降の予定についてご説明を願いたいと思います。

○諸永室長　本日も委員の皆様にはご議論いただきまして、ありがとうございます。そして、本日プレゼンテーションをいただきましたMONIC様、BSA様、ACCS様、そして池村先生、ありがとうございました。

次回以降のスケジュールでございますが、次回、第9回を3月17日、金曜日の10時から、そして、その次の第10回を3月29日、水曜日の15時からを予定しておりますので、よろしく願いいたします。

○岡村委員長　それでは、以上をもちまして、産業構造審議会知的財産分科会営業秘密の保護・活用に関する小委員会第8回会合を閉会させていただきます。本日は、長時間のご議論をありがとうございました。

——了——