

## 日本エネルギー法研究所 2018年度第1回特別研究講座 講演録

- I 日 時 : 2018年6月12日(火) 14:00~16:00
- II 場 所 : スタンダード会議室五反田ソニー通り店 6B会議室  
東京都品川区東五反田2-3-5 五反田中央ビル
- III 講 師 : 東啓綜合法律事務所 弁護士・ニューヨーク州弁護士 村尾 治亮 氏
- IV 演 題 : 「ビッグデータに関わる法的問題」
- V 内 容 :

### ◇開講挨拶

日本エネルギー法研究所理事長の野村でございます。

2018年度第1回特別研究講座の開会にあたりまして、ひとこと皆様方にご挨拶を申し上げます。

皆様ご多用中のところ、本講座にご出席くださりまして誠にありがとうございます。また、平素は当研究所の活動に対しまして、格別のご高配を賜り、この場をお借りして厚く御礼を申し上げます。

本日は東啓綜合法律事務所でも弁護士としてご活躍されていらっしゃいます、村尾治亮先生を講師にお迎えして「ビッグデータに関わる法的問題」というテーマでご講演をいただきます。

村尾先生は東京大学法学部をご卒業後、弁護士を務められる傍ら、ニューヨーク大学のロースクールを修了され、国内法だけでなく海外の法律にも深い造詣をお持ちでおられます。現在は、大阪大学知的財産センター招へい教授、法とコンピュータ学会理事を務められるなど多岐に渡ってご活躍をされております。法とコンピュータ学会は現在私が理事長を務めておりますが、シンポジウムの企画等について様々ご指導いただいているところでございます。

また、これも個人的なことですが、ソフトウェアの著作権登録の指定機関になっておりますソフトウェア情報センターという組織がございます、こちらも私が理事長を務めております。登録業務の他に知的財産権、特にソフトウェアについての研究を幅広く行っておりますけれども、こちらでも様々、村尾先生からはご指導をいただいているところでございます。

さて、EUにおきましては先月5月25日に一般データ保護規則（General Data Protection Regulation: GDPR）が発効しまして、ビッグデータに関する関心が非常に高まってきております。

もちろんこれはEUだけの問題ではなくて、日本でも同様でございます。情報技術の改革が目覚ましく進む現在、企業の競争力の源泉は、データ、その分析方法、これらを活用した製品やビジネスモデルと移行しつつありますけれども、これはエネルギーの分野においても

例外ではございません。

本日のご講演では、こうした状況の下におけるビッグデータの法的保護とビジネスにおける留意点等につきまして村尾先生から貴重なお話が伺えるものと存じます。

最後になりますが、本日のご講演が皆様にとって有意義なものとなることを祈念いたしまして、簡単ではございますが、開会の挨拶に代えさせていただきます。

どうぞよろしくお願いいたします。

## ◇講演

村尾です。今日はどうぞよろしくお願いいたします。

野村先生もこちらにいらっしゃることを先日伺いまして、それ以来緊張しておりますけれども、有意義な時間に出来ればと思っております。

### 1. 総論

#### 【スライド2<sup>1</sup>】

それで早速ですが、まずビッグデータとは何かということです。ビッグデータの定義らしい定義はあまりないのですが、よく言われるのは Volume が多い、大量である、それから, Variety, 多様なデータである, Velocity, 高速にたくさんデータが集まってくる, Value, 価値があると。元々はリレーショナルデータベース等で取り扱うことができないような大量のデータをシステム分野の辺りがビッグデータと言っていたらしいのですがけれども、それが一般的な用語で使われるようになってきている状況かと思います。

こうした状況というのは、情報処理・ネットワークの高度化、IoT等で色々なデジタルデータが溜まってくる、スマートフォンやタブレット等で利用者がどんどんデータを入力する、そうした環境下で起こってきた事象だと思えます。

総務省はビッグデータを類型化して、例えば、国や地方公共団体が提供するオープンデータ、それから産業データ、これは企業のノウハウをデジタル化するもの、構造化したデータや、Machine to Machine から吐き出されるストリーミングデータ、刻一刻と出てくるデータのことで、また個人のパーソナルデータと、このような類型があるとしております。

こういったデータを利活用することによって経済成長への期待がされているということです。AIもビッグデータがないと、ディープラーニングすることはできないですから、データをAI等に活かすことで、経済成長につなげることが期待されています。

---

<sup>1</sup> スライド番号は当日配布資料の右下に記載。

### 【スライド3】

次に活用事例についてですが、様々な例があると思います。まず典型的ですが、ウェブでのターゲット広告配信、Facebook等が自分が持つデータや広告主が持つデータを利用して、ユーザー毎にそのユーザーに最適な広告を発信すると、それからタクシーの需要予測、これは最近の日経ビジネスに載っていた例ですが、NTTドコモがスマートフォンからユーザーの位置情報を取得して、人数と人の位置や動き、どの時点にどれぐらいいるのかというデータをタクシー会社に提供する。タクシーの過去の運行実績データや、気象情報等の情報も駆使してタクシーの需要予測をします。これにより、新人の運転手の一日の売り上げが5,000円もアップしたということが記事に書かれていました。

それから、アメリカの運送業者であるUPSでは、保有する配送車に取り付けたセンサーで速度、燃費、走行距離、停止回数、エンジンの状態等を監視することで得られたデータをコスト削減に活かしている、また同じくアメリカのSanta Clara市では犯罪が発生する可能性が高い場所や時間帯を予測することで、治安を改善するというに使ったりしていると。電力関係で申し上げますと、火力の最経済運用システムに東芝が使っているという例が報告されています。

### 【スライド4】

ビッグデータは色々活用に期待はあるのですが、逆にビッグデータの副作用ということも最近指摘されています。

慶應義塾大学の教授である山本龍彦先生は著書「おそろしいビッグデータ」の中で、ビッグデータ社会では、自分がデータで予測されて類型化した中で決めつけられてしまうので、本当の自分が顧みられなくなってしまうのではないかと懸念されています。

色々な例を挙げられているのですが、例えばTargetというアメリカの小売店では、特定の年齢層の女性で、臭いがしないスキンローションを使って特定のサプリメントを飲み、大きいバックを買う顧客は妊娠している可能性が高いと予測して、当てはまるお客さまに対してベビー用品のクーポン券を送ったと。そうしたところ、高校生の家にそういったものが送られてしまって、父親は激怒してTargetに抗議したのですが、実際には娘が妊娠していたということがその後判明したということがあったようです。これは、ある意味プライバシーが侵害されてしまうという状況になるのではないのかということです。

それから、大学在学中に就職活動をしたが失敗をしてしまい、その後にファーストフード店でアルバイトをして、また数年後に就職活動を始めた。そうすると、最近ではどういう人を採用したらよいかということにもAIが使われるようになってきているので、そういったデータが集められて、就職に失敗してファーストフード店でアルバイトしている人は職務遂行能力が低いのではないかとAIに勝手に判断されてしまって、すべての会社で不採用になってしまうことがあり得るのではないかと。

実際、中国ではアリババグループのアリペイというところがビッグデータに基づいて個人の信用力を査定するサービスを開始しているようで、それには支払いの記録だとか学歴だとか資産状況だとか交友関係等を基にして、融資するかどうかを決めるというようなことがあるようです。それだけではなくて、住居を賃貸借するかどうかを判断するとか、外国ビザの取得、裁判の証拠等にそのデータが利用されることが中国では起こっていると言われてます。

またアメリカでは、罪を犯して量刑を決める時にこういうタイプの人間はもう1回犯罪を起こすリスクが高いから、これぐらいの刑が望ましいのではないかとというように量刑を決めるために利用されることも行われ始めているようで、黒人の再犯リスクは白人よりも高く見積もられてしまうことがあって問題ではないかと指摘がされているようです。

スライドで挙げましたのは、うわべだけの相関関係、本当にそういう相関関係があるか分からないのにデータ上は相関関係があるように見えてしまうというものです。プールで溺れた人間とニコラス・ケイジの出演作品の数というのは、データ上は相関関係があるらしいのです。多分どう考えても関係がないと思うのですが、数字上は何かちょうど連動しているように見えて、いかにも相関関係があるように見えるということが起きることがある。あるいはデータが本当に何かの事実をきちんと示しているのか分からないというデータへの過小・過剰代表の問題、それから既存バイアスの反映というのは、今既にあるデータを利用して、AIが何かを推論するとなると、既存のバイアスが反映されてしまうのではないかと、そうしたAIによるアルゴリズムが絶対のものとして扱われてしまうのではないかと、そういったことで人がどんどん差別されるようになるのではないかとということが危惧されています。

#### 【スライド5】

こうしたデータによるプロファイリングの法規制の動向ですが、GDPRの中にはプロファイリングについて、中止請求権というのが認められています。あるいは、自動処理のみに基づいて重要な決定を下されない権利が個人に認められているということがあります。公正・透明性というのは、自動処理のみに基づく決定を行っていることや、その決定のロジックに関する意味のある情報、その処理の重大性及びデータ主体に及ぼす帰結をデータ主体に告知する必要があるというようなことがヨーロッパでは主張されるようになっており、GDPRの中に規定があります。

アメリカでもFTC2016年報告書ではそういったことについて懸念を示しておりまして、2つ目の項目ですが、消費者レポート、インターネットで集めるデータなんかも消費者レポートに当たると言われていますが、それを利用する時に不利益がないか、そういったデータに基づいて金融、保険、雇用、住宅またはその他の一定の便益について利用を拒否する場合には、消費者に対して不利益通知を提供しなければいけないとされています。これはAIに基づいて不利益な判断をした場合に、そういった理由を説明しなければいけないということ

を言っているわけです。

日本はまだこういった規制はありません。放送番組の放送受信データについては、そういったことをしてはいけないというガイドラインはあるのですが、一般的にはないという状況です。

#### 【スライド6】

それから、最近の法規制の動向としましてはデータポータビリティですね、自分のデータが様々な事業者を持たれているわけですが、データを他の事業者に移したいということを認める動きがあると。これはGDPRの中にあります、日本でも現在検討中です。

それから Data residency law, データローカライゼーションとも言われますが、どこかの国の人のデータは、その国の中のサーバーに置いておかなければいけないと、そういった規制をし始めている国もあるようです。

これは1つには個人情報保護という側面もありますが、別の側面では国民監視のツールになっているという国もあるのです。ロシアなんかは、自国の国民のデータは皆、自国の中のサーバーに置かなければ駄目だとし、その理由は国民を保護するためだと主張していますが、国民のデータを全て監視するためではないかと言われてます。

TPPの中には、データを自分の国に置かなければいけないことには、原則的にはいけないという条項があります。これが13条2項でしょうか。「いずれの締約国も、自国の領域において事業遂行するための条件として、対象者に対し、当該領域においてコンピュータ関連設備を利用し、又は設置することを要求してはならない」ということで一応例外もありますが、原則としてTPPはそうしたことは禁止されております。

## 2. ソースの保護

#### 【スライド8】

それで今までのところは前提なのですが、まずビッグデータに関して法的保護を考える時に視点がいくつかあるかなと思っています。1つはビッグデータの元になるデータのソースについての保護の関係です。

始めに、プライバシー権の問題があります。

プライバシー権は、古典的には1人で放っておいてもらう権利です。これは有名人の私生活をイエロージャーナリズムが暴露するということが1890年代ぐらいに起きて、カメラが私生活に介入して私生活を公にさらすということに対して、1人で放っておいてもらう権利だということで、ハーバード・ビジネス・ロー・レビューでウォーレン・ブランダイスが発表したというところに起源があります。これを受けて、当時アメリカのニューヨークで様々な印刷物に自分の顔写真が掲載されたという女性が裁判を起こしましたが、裁判所はこの権利を認めなかったということがありまして、最初にニューヨークでこういったプライバシー、

1人で放っておいてもらう権利というのが立法されたという経緯があります。

その後これが4分類説というように①私生活の侵入，②私事の公開，③誤認を生ずる表現，④私事の営利利用に関して，プライバシーの権利があると学説上は言われました。

日本でプライバシーの権利が最初に裁判で認められたのは、「宴のあと事件」です。政治家と料亭のおかみの男女関係について，三島由紀夫が小説化し，プライバシー権侵害が問題となり，東京地裁はプライバシー侵害を認めました。この時，①公表された事柄が私生活上の事実または私生活の事実らしく受け取られるおそれのある事柄であること，②一般人の感受性を基準として当該私人の立場になった場合公開を欲しないであろうと認められる事柄であること，③一般の人々に未だ知られてない事柄であること，が侵害の要件とされ，基本的に1人で放っておいてもらう権利と同じような内容です。

最高裁ではその後，「ノンフィクション逆転事件」で，過去の有罪判決に関することが出版物に実名で記載されたことについて，時が経過して一般市民としても生活することができ，前科の公表を受忍しなければならない，という性質のものではないとし，プライバシー侵害を認めました。

このように過去にはプライバシー権は，1人で放っておいてもらう権利という点が軸でしたが，近時は情報コントロール権，つまり自分の情報をコントロールする権利だと言われてきています。

#### 【スライド9】

その経緯については，IT化が進展してきたことが背景にあります。

1960年代に電子計算機の利用が拡大して，個人の情報が不当に使われるのではないかと世界的に懸念されるようになりました。

1970年にアメリカで初めて「Fair Credit Reporting Act」が成立，西ドイツでもヘッセン州で個人情報保護法が成立し，個人の情報を保護しようという動きが国際的に進んできました。1973年にはスウェーデンでデータ保護法が立法されまして，我が国では1976年に政府が「電子計算機処理データの保護管理準則」を制定しました。

その後，1980年にOECDで理事会勧告がありまして，この時には，ヨーロッパではできるだけ個人で情報をコントロールする権利を認めるべきであるという議論がされていましたが，アメリカでは情報をどのようにスムーズに流通させるかという議論がされる等，国ごとに個人情報の保護がバラバラに立法されていました。そのため，統一的な法制が必要となり，OECDの8原則が話し合われて決められました。その後，日本では先に行政機関における個人情報保護の議論が進み，2000年代になって個人情報保護法が成立しました。

#### 【スライド10】

スライドにあるのが「OECD 8原則」で，収集制限の原則や，データ内容の原則などありまして，これらは現在でも参考とされ，この8原則を前提に個人情報を保護すべきであ

ると各国で考えられました。日本でも裁判でこれを引用して、不法行為を認めた事件が過去にあります。

#### 【スライド 11】

2015年に個人情報保護法が改正されました。この改正の背景は、個人情報保護法が作られたものの、過剰反応があるのではないかと考えられたからです。例えば、JR福知山線の列車事故においては、被害者の搬送先病院が個人情報保護法違反を恐れて、被害者の家族にも安否確認を拒んだことがありました。一方、個人情報漏えい事故の多発や、デジタル化・ネットワーク化の爆発的な発達によって、プライバシーへの不安が増大してきました。このようにデータをどのように利用し、また守るかという2つの観点から、法改正が必要になったということです。

個人情報保護法の体系は、まず法律があって、それから基本方針、施行令、施行規則、ガイドラインがあります。これらをすべて細かく見ないと詳しいことはなかなか理解できないような法体系になっています。

#### 【スライド 12】

プライバシー権と個人情報保護法とがどのような関係にあるのかという点について説明します。プライバシー権とは、基本的には国家等の公権力との関係では人権になり、私人間では人格権の一種とされて、侵害された場合は差止請求や損害賠償請求ができます。

個人情報保護法は、個人情報を適正に取扱うためのルールを定める事前規制です。そういう意味ではプライバシーを守るために、全体としての取扱いを定めたルールと言えます。したがって、プライバシー権を保護することと完全にイコールではなくて、保護される権利は必ずしもプライバシー権とは限りません。行政規制であり、事前規制でもあります。個人情報保護法違反になると必ずしもプライバシー権の侵害になるわけではありません。

#### 【スライド 13】

個人情報保護法の規制対象を図にしてみました。個人情報取扱事業者に当たると規制の対象になります。あるいは匿名加工情報取扱事業者になります。個人情報データベース等を事業の用に供している者、あるいは匿名加工情報データベース等を事業の用に供している者ということで、個人情報を取得したとしてもデータベース化していなければ、基本的にはこの取扱事業者には当たりませんので、規制の対象ではありません。データベース化して利用している場合には、生存している特定の個人を識別可能な情報として利用している場合に個人情報として保護されます。

個人情報のうち、個人データベースを構成しているものが、個人データとして保護されます。それがさらに6か月以上保持されると、保有個人データとなって新たにそれに関する規制の対象となるということです。要配慮個人情報には、特別な規制があります。これらを匿名加工すると匿名加工情報として、また様々な規制がありまして、それについては、後程

説明したいと思います。

【スライド 14】

簡単に改正法の概要を説明します。スライドに記載したように個人情報には、15～18条、35条といった規制があります。また、個人データに関する規制には19～26条のような規制があります。

【スライド 15】

まず、個人情報とは生存する個人に関する情報であって、①特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）や、②個人識別符号が含まれるものです。

したがって、これら識別照合性・容易照合性があると個人情報になります。これは個々の事業者で相対的に決まります。例えば、自分の名前がメールアドレスに載っていれば、それで個人情報になるかもしれませんが、記号か何かで構成されているメールアドレスは、それ自体では誰のものか分かりませんので、個人情報には当たらないかもしれません。ただ、特定の事業者が自分の手元のリストと照合することで、誰なのか判別できるときは、そのメールアドレスは個人情報に当たります。つまり、個々の事業者ごとに相対的に決せられることになります。

②の個人識別符号については、1号と2号がありまして、1号は、身体の一部の特徴を電子計算機のために変換した符号や、DNAや顔の骨格といったものが該当します。2号は、旅券番号や基礎年金番号等が該当します。

【スライド 16】

個人情報の利用目的はできるだけ特定しなければいけません。目的については原則として、制約は定められていません。できるだけ特定しなければいけないので、例えば第三者提供するというときには、第三者提供すると書いておかないと第三者提供することができません。利用目的は、原則としてどのような目的でもよいのですが、他の法律で例えば禁止されていることや、公序良俗に違反するものを目的とすることは当然できません。例えば割賦販売法等で信用情報の利用は、購入者の支払能力の調査目的にしか使用してはならないとなっていますので、別の目的で使ってはいけなくなります。

それから、取得した個人情報を利用するときには、利用目的の範囲内で使用しなければなりません。ただ、法令や人の生命・身体・財産の保護の必要性がある場合等の例外はあります。

また、利用目的は、本人に通知するか公表しなければならず、事前に公表しておくか取得後速やかに本人通知または公表しなければいけません。申込書やアンケートに個人情報を記載させたり、ユーザー入力画面に個人情報を入力させたりする場合は、あらかじめ本人に明示しなければいけません。つまり、直接紙などに記載させたり、インターネットの入力画面



で入力させたりするときには、きちんと利用目的を明示しなければなりません。そのあとで利用目的を公表することはできないのが原則です。そして、不正に個人情報を取得することは禁止されています。

#### 【スライド 17】

これまで個人情報について説明しましたが、次に個人情報がデータベース化されて個人情報データベースを構成する個人情報、つまり個人データについて説明します。

コンピュータにより検索できるように体系的に構成したものや、容易に検索できるように体系的に構成したものが個人情報データベースになります。容易に検索できるように体系的に構成したものですので、例えば取得した個人情報が時系列に並んでいても、容易に検索できるように構成されていないので、そのような情報をたくさん所持していても、個人情報データベースを持っていることにはならず、個人データには該当しません。あくまで容易に検索できるように、体系的に構成したものです。

それから、個人データは6か月以上持っているると保有個人データになって別の規制がかかります。

#### 【スライド 18】

個人データについては安全に管理しなければいけません。基本方針を策定して個人データの取り扱いに関する規律を整備する、組織的安全管理措置をとる、人的安全管理措置、つまり従業員の教育をする、物理的安全管理措置をとる、技術的安全性管理措置をとる等、こういったことをしなければいけないということです。それから、個人データに関しては従業員や委託先の監督をきちんとしなければいけません。また、第三者提供をする時には、本人の事前の同意かオプトアウトが必要ということです。データの内容の正確性の確保や、不要時の消去の努力義務というものもあります。

#### 【スライド 19】

これを6か月以上持っているると、保有個人データになります。保有個人データに関する義務としては、開示・訂正・利用停止等の請求手続きについて、本人が知ることができる状態におく義務、本人から開示・訂正・利用停止等の請求があった場合には、これに応じる義務があります。改正前の個人情報保護法の時は、こういった請求権は個人にはないと立法時は議論したのですが、裁判所がそれを認めるような判決を徐々に出し始め、EUが認める方向になり、日本も認めるということになった経緯があります。

#### 【スライド 20】

このように法律上は、個人から請求を受けた場合には、保有個人データについて開示や訂正等を行わなければいけません。しかし、これはやや驚いたのですが、つい最近の日経ビジネスの記事なのですけれども、個人情報保護法の手続きに従って、日経ビジネスの記者が個人情報の開示請求をしたらしいのです。そうすると、日本の大手はことごとく様々な理由をつ

けて拒んだということです。Google 等は認めて出してきたらしいのですけれども、楽天も Yahoo!JAPAN も、そういったものには応じていません、そういうことはできませんと断りました。その後記者が「実は取材なのですが」と言うと、間違っていましたと言ってきたということで、驚くべき対応だと思います。この記者の方が分析していることには、おそらく日本の企業は様々な部門で情報をバラバラに集めて、それを統合的に管理するというのを今までずっとしていなかったと。個人情報保護法が改正されて、本当はこういう開示請求等に応じなければならなくなったのに、システムが追いついていないのではないかと指摘しているのですが、それにしてもこういう法律ができたなら、普通は社内のルールを決めるべきなのではないかと思います。

#### 【スライド21】

次はこういった個人データを第三者に提供する時のルールです。原則としては本人の同意が必要です。例外としてレジュメ記載のような場合がありますが、それに当たらない場合には、要配慮個人情報は除きますが、オプトアウトという手段があります。オプトアウトというのは、後で本人からデータを提供しないでくださいと言われたら停止する手続きです。②のところですが、以下の5項目をホームページに掲載する等、本人が容易に知ることができるような状態にすることが必要です。第三者提供を利用目的にしていること、提供される個人データの項目、提供の方法、本人の求めに応じて提供を停止すること、本人の求めを受け付ける方法。それを個人情報保護委員会に届出をしておけば、事前に同意を得ていなくても第三者提供をすることができるという手続きなのです。すごく緩いのです。

最初の同意にしても、どれくらいきちんとした同意がとられるのかということ、本当は非常に問題だと思います。ガイドラインでは、こういったところに提供されるのかということ、本人に分かるようにして、そうした情報を開示した上で同意を取れとされているのですが、この同意も非常に曖昧で、利用規約等を非常に長く書いてそのどこかにあたっているからと第三者提供の事前同意があるとされる場合があると思いますが、問題が起こる可能性があると思います。

それから、第三者提供の場合には本人から同意を取るか、オプトアウトという手続きを残しておくかということなのですが、提供先が第三者に当たらないような場合には、第三者提供に当たらないので、他の事業体にデータを提供することができる場合があります。1つが委託の場合ですね。それから事業の承継の場合、そして共同利用の場合です。他の会社と共同利用するために始めから取得したデータですということであれば、一緒に利用する会社が使うのは自由だということで、改めての同意やオプトアウトは必要ないということです。共同利用は、共同利用すること、共同利用されるデータの項目、共同利用する者の範囲、利用する者の利用目的、管理責任者の氏名・名称を、あらかじめ本人に通知または本人が容易に知りうる状態におく必要があると言われていています。

ですから、他の会社と何か情報を共有するというときには、やり方としてはこの共同利用を使うか、委託を使うか、あるいはきちんと同意をとるか、オプトアウトの方法でとるか、このうちのどれが一番ふさわしいかを考えて使うということになります。

【スライド 22】

第三者に提供するとなった場合には、個人情報保護委員会に対して、届出や公表が必要です。第三者から個人のデータを受領する場合にも、こうした記録をきちんと取る必要があります。ベネッセの事件で、名簿屋が様々なところに情報を売ったり、買われたりということがあったのですが、情報がどのように流れているのかについてきちんと記録をとらせる目的で設けられた規定です。

例えば、第三者から個人データを受領するには、どこから取得するのかという確認をして、記録を取るという義務があるのですが、ガイドラインでは次のようなケースで確認記録の義務がないとしています。1つは本人による提供と整理できる場合。それから本人に代わって提供しているという場合、本人側の提供と言える場合、個人データには該当しないという場合。こういった場合には、確認や記録を取る必要はないということになります。

【スライド 23】

今までは国内の事業者に対する第三者提供だったのですが、外国にある第三者に対しては、その国がきちんと個人情報を保護している国かどうか分からないので、また別の規制があります。外国にある第三者の個人データの提供は、以下の場合を除いて本人の同意が必要です。同意が必要なので、オプトアウト方式や、委託、事業承継、共同利用ということでの提供はできません。

まず、①として外国にある第三者が個人情報保護委員会の規則で定める基準に適合する体制を整備している場合です。このような場合には提供できます。規則でどのように言っているかという、提供を受けるものにおける個人データの取扱いについて、適切かつ合理的な方法により、個人情報保護法の趣旨に沿った措置の実施が確保されていることと、個人データの提供を受ける者が、個人情報の取扱いに係る国際的な枠組みに基づく認定を受けていること。この認定というのは、アジア太平洋経済協力（APEC）の越境プライバシールール（CBPR）のシステム認証等がこれに当たると言われています。②外国にある第三者が、個人情報保護委員会が認めた国に所在する場合と言うのですが、まだ認められている国はありません。あるいは、③個人情報保護法 23 条 1 項の例外事由に当たる場合です。こういった場合に当たらなければ、本人の同意をきちんと取らなければいけません。

日本の個人情報保護法の場合は、外国にある第三者ということなので、例えば自分の国の外国の支店等に情報を送る時には、この規制の対象にはなりません。ですので、例えば外国の企業であるけれども、日本に支店があるとするとその支店は日本にあるので、自国の本社には、外国にある第三者への提供の制限はかからずに、一般の第三者提供で情報を送るこ

とができます。外国法人においては同じ法人だとできるのです。法人単位というのが日本の考え方です。

それに比べてGDPRの場合は、EUの域外に出すかどうかということが問題となっているので、同じ法人でもEUの域外に出す場合には、特別な規制がかかるということで、考え方が少し違います。日本は同じ法人だったら外国でも送れるのですが、GDPRの場合は域外かどうか、同じ法人でも域外であれば厳しい規制になるということです。

#### 【スライド24】

アメリカは国外移転については、基本的には一般的な規制はないということです。EUのGDPRでは、域外移転については様々ある規制や行為要件のどれかを満たさなければいけません。例えば、欧州委員会から充分性認定を受けた国であれば、そこには移転できるということで、日本は今充分性認定を受ける交渉中であると聞いています。私の聞いている話では、EUの方から例えば警察等から情報を出せと言われた時に、それに対してどの程度情報を出すことを拒否することができるのかといったことを聞かれているそうです。

それから、企業グループ内で個人データをこうやって保護しますという拘束的企業準則を策定して、それを監督当局の承認を受けると。このようにすれば、自分のグループ内であれば、外国にあるグループでもデータを移転することができます。欧州委員会が策定した標準契約条項という雛形を使って個別契約で1回1回これを利用して移転する。あるいは業界団体が作成した行動規範を承認してもらった場合は、それに従う限りはその業界団体でそれを使うことができます。それからデータ保護認証を企業単位で受ける等ですね。そういったものがなければ、個人から同意をきちんと取ると。自由意思、特定性、十分な理解、明確性、必要な外形を充たす同意を得る等、同意についても要件が非常に厳しく定められています。こういったものに当たらないのに域外移転をしてしまうと、最高2000万ユーロの制裁金、あるいは全世界年間売上高の4%という、莫大な制裁金を課される可能性があるということです。

#### 【スライド25】

次ですが、また日本法に戻りまして要配慮個人情報です。こういった情報については、取得について原則として事前に本人から同意をとる必要があります。人種、信条、社会的身分等、昔は機微情報と言われていたようなセンシティブ情報です。推知情報、例えば宗教に関する書籍をたくさん買っているとその人の宗教が大体推測できるわけですが、それはガイドライン的には要配慮個人情報には当たりません。

ですので、先程のプロファイリングの禁止については、GDPRでは様々配慮されていますけれども、日本の場合は、たとえ分かったとしても要配慮個人情報には当たらないとされており、あまり検討はされていない状況です。

こういった要配慮個人情報に当たると、取得するには本人の事前の同意が必要になり、第

三者提供についてオプトアウトは認められず、本人の事前の同意が必要となります。

【スライド 26】

ビッグデータとして、個人の情報、パーソナルデータを動かそうとすると、先程から説明したように1人ひとりから同意を得たり、オプトアウトだと事後的に自分の情報を流さないでくださいという問合せに対応しなければいけないので大変です。そうすると、匿名加工情報というのに加工して流通させた方が容易に使いやすいということになると思います。

匿名加工情報というのは、個人情報加工して、特定の個人を識別できず個人情報を復元できないようにしたものです。図になりますが、こうした情報にした場合にどんな義務があるかということです。個人情報取扱事業者としては適正に加工するだとか、加工方法を漏えいしてはいけない、作成時にはきちんと公表しなければいけない等の義務があります。匿名加工情報取扱事業者は、識別行為をしてはいけない、安全管理措置を取らなければいけない等の復元させない、匿名加工情報を元に戻さないという観点から義務が定められているわけです。

【スライド 27】

匿名加工情報をどのように作るのかということで、ここが一番多分難しいところなのですが、こうすれば絶対匿名加工情報になるという方法はないのです。一般的にはということを示されているものはありますが、実際にどうするのかというのは非常に難しい問題です。

ガイドラインで言われているのは、特定の個人を識別することができる記述等の一部を削除する、個人識別符号の全部を削除・置換する、個人情報と他の情報とを連結する符号（ID）を削除・置換する、特異な記述、例えば年齢 116 歳なんていう記載があると大体分かってしまうので、削除・置換する、その他適切な措置と、そういったものが必要となります。データ加工についての粒度は個別に検討する必要があるということで、実際それでよいのかどうかは個別具体的に判断しなければならないこととなります。

よく匿名加工情報と一緒に、どうやって個人情報を扱うのかを議論する時に出てくるのが統計情報です。統計情報についてどのように定義されているかですが、これも多分ガイドラインの定義だと思いますが、複数人の情報から共通要素に係る項目を抽出して同じ分類ごとに集計して得られるデータであり、集団の傾向又は性質などを数量的に把握するもの、そうした統計的なデータにしてしまうことで、一人ひとりのデータでは無くしてしまう方法もあります。

私が携わった案件で、個人情報保護法の改正よりもしばらく前に、薬局からのレセプト情報が欲しいという海外のデータ分析会社がありまして、薬局は非常に高いお金を払ってくれるので、出したがっていたのですけれども、レセプト情報、すなわちどんな薬を処方されているかという情報は非常に怖いわけです。それで、統計情報程度に留めなければならないのではないとか、様々議論をしたのですけれども、データ分析会社側は詳しくれば詳しいほ

どありがたい、薬のMRが病院に行ってこの薬を使ってくださいと売り込む際には個別の情報が必要だ、非常に機微な情報が欲しいと言われて困ったことがありました。

【スライド 28】

では、具体的にその匿名加工とはどのようにするのかを少し見てみたいと思います。スライドの資料は、下の方に書いてありますけれども、「パーソナルデータの利活用促進と消費者の信頼性確保の両立に向けて」という個人情報保護委員会事務局が作成した資料の中で、電力利用情報に関して匿名加工をどのようにするのかということを書いている資料があったので、ここで抜き出してきました。

電力利用データとしては、個人属性情報と履歴情報があります。個人属性情報としては、契約者のIDとか氏名、電話番号、性別、生年月日、職種、住所、住居区分、竣工年等のデータがあります。また、履歴情報として、いつこれだけの電気を使用しましたということや、推定使用家電等も記載されています。

このデータをどうやって匿名加工情報にするかですが、まず1つひとつの項目を見ていくわけですね。契約者IDはこのIDを起点として個人の特定に繋がる可能性があるため、これは全部削除するか仮のIDに置き換える。氏名もこれは特定できるので全部削除する。電話番号も削除する。性別、住所、生年月日も組み合わせると個人が特定できるかもしれないので、削除した方が望ましいという感じですね。ただ、場合によっては、他の生年月日や住所等の加工で対応する場合には、男女は残してもよいのではないかとということで、今回はどうもここは加工しないという選択をしたようです。生年月日については、年代の20代、30代といった区分はどうだろうかとされています。職種については、少ない職種についてはその他に置き換えて丸めるとか、住所については、地区単位よりも細かい情報は削除したらどうかとされており、丸めた結果がこういう結果になっています。そして、どのように丸められているかという続きを申し上げますと、住居については何平米未満とか、竣工年は何年から何年という丸め方をしています。家族構成も少し丸めるとか、履歴情報についても、日時を今回は加工しないとしています。電力使用量については、特異な使用量だけを少し変えるというようなことをしています。こういった丸め方をすればよいのではないかと一例になります。

【スライド 29】

さらに、最近三菱総研が出した調査報告書「スマートメーターのデータ活用の促進等に関する調査」の中でも同じように、電力利用情報をどのように匿名加工すればよいか議論されています。

この中では、住所は番地以下を削除すればよいのではないかとされておりまして、先程の個人情報保護委員会よりも緩やかな考え方をしています。また、契約のアンペアは3区分にする、氏名、電話番号、設備情報等の属性情報は削除するとしています。消費電力量につ

いては、30分消費電力量を提供することを原則として可とするとしています。そして、データを提供するまでの時間については、情報を取得してから匿名加工情報として提供するまで1ヶ月以上を確保すると言っています。この報告書の記載では、期間を十分に確保しなければ、万一個人が特定された場合に、利用者に対してアクセスされる可能性が高まるので、1ヶ月ぐらいは置いた方がよいのではないかということでしたが、もちろん安全を考えた方が望ましいですけれども、タイムリーな情報提供が有用な場合もあるでしょうから、絶対に1ヶ月置かなければならないのかどうかについては、個人的には少し疑問を感じます。

#### 【スライド30】

それから、関連するかもしれない規定として、電気事業法の23条で一般送配電事業者は次に掲げる行為をしてはいけないという規定があります。先程の三菱総研の報告書に記載があったものですが、「託送供給及び電力量調整供給の業務に関して知り得た他の電気を供給する事業を営む者及び電気の利用者に関する情報を特定の目的のために使ってはいけない」というものです。

電気の利用者に関する情報を使ってはいけないということで、個人情報保護法をクリアしてもこの問題があるのではないかという指摘がありました。この規定の趣旨ですが、これは託送分野における公正な電力取引のための規定で、おそらく個人情報保護の規定ではないと思います。そうすると個人から同意を取ったとしても駄目なのかもしれません。そこまでの議論は、調べましたがよく分かりませんでした。つまり、個人情報保護の利用者を保護するための規定、利用者のプライバシーを保護するための規定であれば、利用者から同意を取ればよいという話になりますが、そうではなくて、公正な託送分野の電力取引のためということになると、利用者から同意を取ることは公正な託送分野の電力取引とはあまり関係はないということになると思います。ここは研究が必要かもしれないです。

#### 【スライド31】

細かい個人情報保護法の話がようやく終わりに近づきつつあるのですが、最近プライバシーバイデザインという議論がよくされます。技術の設計思想の中にプライバシーの考え方を埋め込むもので、もともとその製品の使用上プライバシーがきちんと配慮されるように製品を作るということが言われています。

そのように製品を作ればプライバシー保護の観点からはよいですけれども、本来自由であるべき人の判断がデザインにより規定されてしまう、あるいは制約されてしまうという側面もごさいます。デザインにより本来自由であるべき個人の判断を事実上決定してしまうというのはいかなるものかという批判もあるところです。

#### 【スライド32】

次に、Suica事件になります。個人情報の関係でどうしても触れておかなければならない事件です。この事件では、JR東日本が保有していたSuicaの利用データ、SuicaのID番

号、利用者の氏名、電話番号、生年月日、性別、乗降駅名、利用日時、それから鉄道利用額、物販情報等につきまして、これらを日立製作所に提供して分析してもらうことで、JR東日本はどのようにより良い駅を作ればよいかという検討に活かそうとしていたようです。日立製作所に提供する際には、情報はレジメに書いてあるように加工されていました。当時はまだ、匿名加工情報という概念がないと言いますか、そういう言葉がない法改正前でしたが、利用者の氏名等を削除し、また生年月日については「日」を抜いて、生年月までの表示にするとともに、SuicaのID番号も変換してデータを提供したという状況だったのですが、個人のプライバシーの侵害に当たるのではないかという批判が非常に多く出てしまい、JR東日本の計画は中止になったということです。

そして、この事件をきっかけに、データの利活用をよりやりやすくする必要があるのではないかという議論がなされ、その中で匿名加工情報にすればデータのやり取りをしてもよいということを法律で設けたらよいのではないかということになり、改正法ではそうした規定が設けられたわけです。しかしながら、結局のところ、利用者の言いようのない不安感のようなものに対して、どう対応するかという問題が残ります。法律を守っていればよいのかというと多分そうではなく、法律を守っていても何か気味が悪い等の感覚を持たれてしまうとおかしいのではないかといった批判が起きるようになってしまうということです。おそらく、プライバシーがどのように侵害されているのか、よく分からないために不気味なのだろうと思われま

一方、GoogleやFacebook等は、おそらく個人情報をかなりの場面で使っているのだと思われま

すが、おそらくは無料サービスとして自分たちも利益を受けているからまあよいと、またTポイントカードのようなものも、おそらくかなりの個人情報を使っているのだと思われま

すが、利用者としてはポイントを提供してもらっているからよいという、そういった感覚があるのだと思われま

す。ただ、Suicaのようなものでやられると、よく分からないまま勝手に自分の情報を利用されたという感覚が何となくあるのだろうと思われま

す。やはり、利用者に対して事前にどのようにきちんと説明しておくかというのが、非常に大事になってくると思いま

す。Tポイントのようにポイント等のサービスを提供することができれば望ましいのですが、そうでないときはきちんと事前によく説明してやらないと、何か不気味だといったような雰囲気

が盛り上がってしまい、炎上してしまう可能性があるということだと思いま

す。

#### 【スライド33】

その次のスライドには、最近のFacebookの事例について掲載しております。

経緯としては、2013年にケンブリッジ大学の教授がクイズアプリを利用してFacebookのユーザーのデータを集めています。そのアプリは利用条件の中で、当時のFacebookのポリシーに沿うような形式で、ユーザー本人とその友達のいくつかのデータを第三者に提供する



ということが明示されていたということでもあります。

その後、この教授がこのユーザーとその友達の個人情報約 5000 万人分を、選挙コンサルティングの会社であるケンブリッジ・アナリティカという会社に売却しました。アプリの利用条件で第三者提供の同意を取っていると、形式的にはそういうことになっています。

そして、ケンブリッジ・アナリティカという会社は、このデータを機械学習させて、それを基に分析したユーザーの趣味や嗜好から、個々の Facebook ユーザーの政治的傾向を予測して、トランプ氏への投票を促すための政治広告を配信したのではないかということが疑われた事例です。今年の 3 月 17 日に、このケンブリッジ・アナリティカの内部告発がニューヨーク・タイムスやガーディアンにより報道され、2 日後には Facebook の株価が 9% 近く急落し、時価総額としては 370 億ドルが喪失しております。その後、ザッカーバーグが公聴会で証言したと、このような流れとなっております。

これも形式的に言えば、アプリの利用条件において第三者提供の同意について書いてあるわけで、それに利用者が同意して使っているのだからその情報が使われて何が悪いのかと、形式論で言えばそのようになります。こうした同意がどこまで及ぶのかという法律的な問題も本当はあるのだらうと思うのですが、仮に同意があるとしても、法を守っていれば何をやってもよいのかという問題はどうしても付き纏うと思われまます。ですので、こういった個人のプライバシーに関わることについて、特にインフラのような社会からしっかりした対応が求められている会社が行う際には、きちんと丁寧に説明をしながら行う必要があるのだらうと思います。

#### 【スライド 34】

これまで取り上げた内容では、ビッグデータのソースとして個人情報の問題となっていたのですが、これからは別の観点として著作物についてお話しします。Google ブックサーチの事件では、アメリカの図書館にある本が全てデジタルスキャンされたということで、ソースが著作物だったことに問題があったわけです。

日本の現行の著作権法では 47 条の 7 で、そういったデータマイニングのようなことを非常にやりやすくするような規定があります。そして、今年の法改正により、さらにやりやすくなりました。条文の言葉尻の問題のように私は思いますが、よりやりやすくなるということです。日本の著作権法 47 条の 7、あるいは改正法の 30 条の 4 の特殊性としては、営利企業もデータマイニングのために、自由に著作物を利用してもよいというところにあると思われまます。

#### 【スライド 35】

スライドにはアメリカとイギリスだけしか書いていませんが、諸外国を見ると、基本的には営利企業が自由にデータマイニングをできるという規定にはなっていません。イギリスは 2014 年の立法で、そうしたデータマイニングをできるようにする規定を入れたのですが、た

だ、条文を見てみますと、

(1) The making of a copy of a work by a person who has lawful access to the work does not infringe copyright in the work provided that-

(a) the copy is made in order that a person who has lawful access to the work may carry out a computational analysis of anything recorded in the work for the sole purpose of research for a noncommercial purpose, ...

とありまして、営利目的の分析のために使用してはならないとなっています。

### 3. 保有者の保護

#### 【スライド 37】

今まではソースの話をしていましたが、今度はデータの保有者の保護ということで、データ保有者をどのように保護するのかという点についてお話しします。

よく、データ・オーナーシップあるいはデータの所有権という言葉聞くことがあるのですが、データに対して所有権は発生しません。所有権は有体物に対するものであり、データは有体物ではないですから、所有権の対象にはなりません。では、こういった権利があるのでしょうか。

データベースの著作物と言うことができれば、そのデータのセットは著作権で保護できるかもしれません。また、営業秘密に当たれば営業秘密として保護できるかもしれません。その他には、データが排他的に自分しか使えない状態に事実としてあると、そういった状態をもってデータに対して自分に権利があると言うということも考えられます。勝手に盗まれたりしてしまうと、もうそれは取り返しがつかないということになるのではないかということです。

#### 【スライド 38】

順を追って見ていきますが、まずはデータベースの著作物です。条文では、「データベースでその情報の選択又は体系的な構成によつて創作性を有するものは、著作物として保護する」としておりまして、これに該当すれば、著作物としてデータベースが保護されることとなります。

#### 【スライド 39】

ただ、そういった著作物性が認められないデータベースはどうなるのでしょうか。

ヨーロッパにおいてはデータベースの権利が認められております。あまり有効に活用されていないとは聞いていますが、EU指令で認められております。一方、日本においては、翼システム事件という事件で、著作物ではないデータベースであっても、競合他社が勝手にそのデータベースをコピーして売ってしまうというようなことに対しては不法行為が成立するとした判決があります。データベース著作物ではないデータベースについて、著作物ではな

いが不法行為で保護したという事件になります。

【スライド 40】

ところが、平成 23 年に北朝鮮映画事件という最高裁の判決がありまして、この結果を踏まえますと、先程の翼システム事件のように、不法行為でデータベースを保護することができなくなるのではないかという議論がなされました。

北朝鮮映画事件がどういう事件だったかと言いますと、平成 15 年 12 月に放送局がニュース番組において北朝鮮の映画を著作権者の許諾なく 2 分 8 秒用いたことが、著作権侵害になるかが争われたものです。北朝鮮はそれまでベルヌ条約に加盟していなかったのですが、平成 15 年 4 月、この放送の 8 か月前にベルヌ条約に加盟していたのです。そして、ベルヌ条約に加盟すると、加盟国の著作物は日本でも保護しなければならなくなるので、北朝鮮の著作物として保護しなければならないのではないかが問題となったわけです。判決は著作権侵害を否定しました。平たく申上げると、北朝鮮がベルヌ条約に加盟したとしても、日本は北朝鮮を国として承認しておらず、国として認めていないところのものは著作権法のいう著作物とはならないと、そういった判決でした。

では、不法行為ではどうかということが次の論点となりました。先程のデータベースのように、著作物ではないが不法行為で保護されたという事例と同様に、北朝鮮の映画に対して著作権侵害は認められないが、不法行為で保護される可能性はあるのかが問題になったわけです。

【スライド 41】

著作権法は、著作物の利用について、一定の範囲の問題に対し、一定の要件の下に独占的な権利を認めています。そうすると、著作権法で保護されるようなものについて、著作権法が保護すると言っていないければ保護しないとしたわけです。要するに、著作権法において保護するような領域のものについて、著作権が保護をしないと認めていないものについては、保護をしないという判断を立法府はしていると考えられ、そのため保護はしない。よって、一般不法行為も成立しないと認めたわけです。

そうしますと、先程のデータベースの事例と関連して、著作物となるデータベースの著作権は保護されますが、著作物性が認められないデータベースは保護しないと立法府は判断しているのではないかということが問題となるわけです。

【スライド 42】

次に、北朝鮮映画事件の射程はどうかという点です。

最高裁では、判決を下すのは当然担当の裁判官ですが、担当の裁判所調査官という同じ裁判官の身分を持つ方が、事件に関することを一生懸命調査して、最高裁の裁判官に対してレポートを提出します。そういうものを参考にして最高裁の裁判官は判断するのですが、その調査官が最高裁判所判例解説を書いています。

それで、レジュメになりますが、この最高裁判所判例解説を書かれた山田裁判官は、著作権法の規律対象とする利益については、それを保護する、保護しないを含めて著作権法の制定により法定されており、もしこういった利益について、著作権法で保護されないとすれば、不法行為も成立しないとしました。

この後、著作権侵害とならないような行為について不法行為が成立するかどうかが争われた下級審の判決では、この北朝鮮映画事件判決を引用しています。例えば、被告書籍が原告作成映画のインタビュー部分を、著作権を侵害しない利用態様で引用することについて不法行為が成立しないとしたものがあります。これについては、まあそうかなと思います。2つ目の例は、国家試験対策講座のテキストに類似した別のテキストについて、著作権侵害にはならないとした上で、ほとんどデッドコピーだという場合に不法行為が成立するののかということ成立しないとったわけです。典型的なのが、5つ目に記載した星座盤のデッドコピーです。星座盤というものは、書こうと思っても同じようにしかなりようがない、全く違う星座盤ができるのは逆におかしいので、そういったものをデッドコピーしても不法行為にはならないとされました。そうすると、著作権法でデータベースの著作物については保護するといっているけれども、他のものは保護しないとしているのだとすると、そうしたデータベースを勝手にコピーしても不法行為は成立しないのではないかと心配がされているというわけです。

#### 【スライド43】

では、著作物として保護できないとしても、不正競争防止法で、例えば秘密情報としてデータベースを保護することができるのではないかと考えられます。データベースをきちんと秘密にしていれば、それが不正に取得され利用されている場合には、不正競争防止法違反になる可能性が出てきます。また、データベースを正当に誰かに提供した場合であっても、利用のされ方や開示が不正になされた場合には、不正競争防止法違反ということで保護できるのではないかと考えられるわけです。

#### 【スライド44】

そうすると、次は、データベースが営業秘密に当たるかどうかということが問題となってきます。営業秘密に当たるというためには、秘密管理性が認められる、有用性が認められる、非公知性が認められる、こうしたことが必要だとされています。

ビッグデータというのは、データを利活用しようとしているということで、基本的に流通させることをベースにしているわけです。一方、営業秘密は基本的には流通させないものです。厳密に言えば、きちんとNDA（秘密保持契約）を結んで管理している場合であれば、秘密管理性も認められるかもしれません。しかし、一般的な感覚からすると、営業秘密は基本的に自分のところで隠し持って、他者にできるだけ開示しない性質のものであり、ビッグデータをこれから利活用しようとする、データベースを他者に使わせて取引をしようという場合に、流通を前提とするならば、不正競争防止法2条6項の営業秘密の規定で本当に保護できるのだろうかという疑問が

提起されました。そうしたことから、今年の法改正がなされたわけです。

【スライド 45】

今年の5月30日に改正不正競争防止法が公布されました。こうしたデータの不正取得や使用に対する差止請求権等が規定されました。施行は公布の日から起算して1年6か月を超えない範囲内であるということで、具体的にいつからというのはまだ決まっていますが、こうした流通を前提とするデータについても保護しましょうという規定が改正で置かれました。

【スライド 46】

それがどういう規定かという、「限定提供データ」というものです。その限定提供データがどういうものかという、技術的管理性があり、限定的な外部提供性がある、有用性があるものと説明されているのですが、何となく分かるような分からないような文言です。改正不正競争防止法上の定義には、電磁的方法により相当量蓄積され、及び管理されている技術上又は営業上の情報と書いてあります。具体的には、ガイドラインでこういったものが保護されるかを明確化すると経済産業省は説明しております。法律で明確になっていないものを、ガイドラインで明確にすればそれでよいのかという原理的な問題があるようには思われますが、とにかく現在ガイドラインを作成しているところです。どういうものを保護しようとしているかという、技術的に管理されているもの、つまりIDやパスワードで管理されている、通信に専用回線が使われている、データを暗号化している、スクランブル化している等といったもので、限定的に外部提供されているものに限るとされています。つまり、誰にでもアクセス可能なものではないこととされているのです。

【スライド 47】

そしてどんな行為が禁止されているのかと言いますと、権限がない外部者が管理を侵害してデータを持ち出す。または、第三者提供禁止という条件で取得したデータを、不正の利益を図る目的または限定提供データ保有者に損害を与える目的で、その限定提供データの管理に係る任務に違反して使用、または第三者に開示する行為が違法とされています。

【スライド 45 に戻る】

スライド 45 の図ですが、保護対象となるデータがあって、これを不正に取得するのはもちろん駄目です。また、ライセンス契約等に基づいてデータを貰って使用している者の中でも、不正に利益を得る目的や、データ保有者に損害を加える目的で、その提供データの管理に係る任務に違反している場合は違法になります。これも定義は難しそうですが、ガイドラインで明確化されると言われています。

また、転得者になりますが、始めから不正な経緯を知って取得した者が使用・提供することも違法となります。始めは不正な経緯を知らずに取得したのだけれども、事後的に不正に取得されたデータであると知った場合には、与えられた権限内での提供や使用はしてもよいが、権限外の提供や使用は不正競争行為の対象になるとしています。これらについても、作成中のガイドライ

ンで要件を明確化するとしています。

【スライド 48】

あとは、正当な目的であれば不競法違反にならないように留意する、不正使用行為によって生じたものについては規制の対象とはしないとといったことも定められました。一方で、刑事罰は今回は見送りとなりました。基本的には契約違反のようなものが主に対象となりそうなので、刑事罰まで規定される必要は現時点ではないと判断されたようです。

#### 4. ビッグデータの取引

【スライド 50】

次は、ビッグデータの取引の側面です。これは、冒頭で野村先生からご紹介があったソフトウェア情報センターが様々な企業のIT担当者、知財担当者を招いて勉強会を実施した機会に、データ取引についてどう思いますかという質問を参加者に聞いた時に出てきた意見です。

規格争いのようなときには情報開示することに利益があるけれども、普通はあまりオープンにしたくない、情報セキュリティ担当の部門が管理しているが、書式を決めたらそれを形式的に全てに適用させようとするのであまり保護を考えていない、GDPR等どんどん新しくなるので訳がわからない、データを使わせてもらう立場としては、データへのアクセスは容易であって欲しい、個人情報のデータベースはセキュリティレベルを高くしてきたが、最近は株主もデータの利活用に関心があり対応に苦慮している、客は自分のデータだと主張するけれども、それを使ってデータの解析をしているベンダーとしてはどうなのか等、色々と錯綜してしまっていて、現在connected industry といって、データの利活用を推進しよう、データを流通させようとしているのですけれども、流通はあまりさせたくないという企業もかなり存在するという状況です。

【スライド 51】

経済産業省が作成した従来のガイドラインは、基本的にはデータの流通をできるだけさせようとするものでした。契約交渉にも応じないのは、独禁法違反になるかもしれないといった文言を記載してデータを流通させようとしていたのです。ただ、データを流通させることは当然のことなのだろうかという疑問も出されまして、今新たなガイドラインを作成中です。

【スライド 52】

データの取引をするときに、契約で何を決めなければならないのかを書いたのが、スライド52の図になります。結局、個々の取引でどういうことが重要なのか、何をやりたいのかということをしちんと考えて、契約を作成しなければならないということです。

提供事業者A社がデータを提供する側、受領事業者B社がデータを受け取って何かをやる側です。A社側ではデータの準備として、どんなデータを提供するのか、どんな保証をするのか、こうしたデータを利用したいという思いの他に、何かそれにより事業上の不利益を受けるのではないかという懸念があって、相手方をどうコントロールしたいかという話が出てくるわけです。

そして、B社側としても、契約をコントロールしたいので、データの利用目的だとか利用方法を取り決めるわけです。第三者に提供してもよいか否か、管理あるいは報告はどうするかといったことです。そして、そのデータを使って新しい派生データができた、例えばA Iがこのデータを利用して色々と学習したとします。その学習モデルをどうするのかということが、非常に大きな問題になるわけです。その学習モデルというのは、提供事業者A社のデータをベースにしているかもしれないけれども、解析したB社側のA Iのプログラムがあったからこそできたのかもしれないので、その派生データをどう今後使うのかは交渉の問題となります。それに対して、こうでなければいけないといったモデルは、現在は無い状況だと思います。

策定中のガイドラインでは、例えばデータを使った時のお金を何%か払わなければいけないというような取決めをされると言われています。言うのは簡単ですが、具体的にどうするのかというのはかなり難しいと思います。A Iで色々読み込ませる過程で、始めはA社のデータを使っているかもしれないけれども、全く別のデータも色々読み込ませるかもしれませんし、B社としてはこのような取決めは今後A社によりB社のビジネスに干渉されかねないと思うかもしれません。A社の側からすれば、自社が提供したデータを元にビジネスをされて儲けられているのは、何か納得がいかないところがあるかもしれません。結局、基本的にはビジネスの判断の問題として考えるしかないと思います。例えば色々なサービスを無料で受ける代わりに使わせるというのも1つの方法ですし、お金を分けるというのもそれで話がつくのであればあり得る選択だと思います。ここはその取引毎にどうするかを具体的に考えなければいけません。おそらくここが一番難しいところだと思います。

#### 【スライド53】

データの取引に関しては、更に独禁法の問題があります。GoogleやFacebook等がデータを独占しているのではないかということで、様々な検討がEUやOECDで行われており、日本でも議論されているところになります。ここでの議論の対象はデータの集積を伴う企業結合の審査です。製品市場の審査だけでなく、データの集積によるA I技術や商品市場への影響や、データ市場への影響も検討します。SNS等の無料サービスについても、無料だから全然考えないというのではなくて、商品の質、セキュリティレベル等について競争が行われている市場と考えられるだろうということです。

下の方にあるFacebook社/WhatsApp社欧州委員会決定というのは、Facebookの子会社とWhatsAppというメッセージングアプリを提供している会社とを合併させる時の審査についてのものです。様々な点が問題になったのですが、ここで取り上げているのはオンライン広告サービス市場に対してどういう影響があるかということで、この時の欧州委員会の決定では問題なしとしました。

なぜ、問題なしとしたかということ、広告提供を行ってないWhatsAppに広告を導入すると、「広告なし戦略」を変更することになり、ユーザーが離れる可能性があるからそんなことはしないだ

ろう、Facebookを代替する広告サービス事業者は十分に存在するから、この2社が合併してもそんなに市場に影響はないだろう、FacebookとWhatsAppのユーザーのプロフィール照合は技術的にハードルがあるとFacebookとWhatsAppの技術者が言っている、あるいは、ユーザーデータは、Facebookだけではなくて、Google、Apple、Amazon、twitter等その他の事業者も収集しており、FacebookとWhatsAppが合併してもたいしたことはないだろうと。そういうことで、市場に対して影響はそんなにないと判断したということです。

ただ、後日談がありまして、FacebookとWhatsAppのユーザーのプロフィール照合には、技術的ハードルがあると欧州委員会に説明したのに実際にはその後照合を行いました。その結果、罰金1億1000万ユーロを科されています。

#### 【スライド54】

次は、データ収集と利活用です。収集して使うこと自体は基本的には問題はありません。独禁法というのは人為的に独占したり排除したりすることを禁止しているので、データを収集して自分で利活用していること自体は基本的には問題がないわけです。

ただ、不当な収集というのは問題があります。特徴的なのは、例えば2つ目の項目ですが、プラットフォームに利用者がロックインされている場合、個人情報保護法等に照らして不当な行為により個人データを収集することにより競争秩序に悪影響を与える場合、つまり個人情報保護法を守っていたら集められないものを違反して集めることが、競争秩序に悪影響を与える場合に不当な収集になるとしています。

少し分かりにくいのですが、個人情報保護法違反の問題は個人情報保護法だけの問題で、競争法の問題は競争法だけの問題ではないかと思えるのですが、この問題はOECDで相当議論されていました。EUは個人情報のプライバシーの保護と競争法をリンクさせて考えようとしています。日本では別の問題ではないかと考えているようですが、ここではこのように述べています。

#### 【スライド55】

次は、収集されたデータへのアクセスです。誰にアクセスを認めるかは基本的には取引の自由ではあるけれども、以下のような場合については独禁法の問題となる可能性があると考えられています。従来競争事業者に当該データを開示していたのに、突然排除以外に合理的な理由が考えられないような不開示をした、競争者や顧客にデータをアクセスさせる義務があるのにそれを拒絶した等、こうしたいかにも不当なことを行った場合に、独禁法の問題になる可能性があるということです。

#### 【スライド56】

それからデータアクセスに関連する他の不当な行為です。データの提供とその解析等を抱き合わせで販売する、義務付ける等で問題となる可能性があるということです。



## 5. 事例研究

### 【スライド58】

最後に事例研究です。

1つ目は、電力利用量情報を利用したいときに、テキストマイニングするために分析業者にデータを交付する場合、どのようなことに気をつける必要があるかということです。

電気事業法の問題はまず置いておいて、個人情報保護法だけの議論だとしますと、分析業者がまず何に当たるかということです。何に当たるかというのは、委託に当たるとすれば基本的にはそのまま個人情報を流してもよいけれども、委託先をきちんと監督しなければいけません。第三者提供の例外の場合で、委託、事業承継、あるいは共同事業の場合というのがあったと思いますけれども、国内の事業者へ委託する場合には、特に第三者提供の制限はかかりません。

そうでない場合には、匿名加工情報にして提供するということが考えられます。その匿名加工情報とする方法は、先程の例で挙げたようなことで、できるだけ丸めて匿名加工情報にして分析業者に交付すると。匿名加工情報にすれば、全く義務がないかといえ、そういうわけではなくて、復元してはいけない義務だとか、そういうのがあったというのも見えてきたかと思えます。

### 【スライド59】

次の事例2の方ですが、プラントの効率的な運転を図るためにデータ解析会社にプラントの運転データを解析してもらうことを検討しています。解析はデータ解析会社のAIで行います。データ解析会社から提供された契約書案を見たところ、運転データを解析することで得られたデータや知見は、当社と共有するものとし、当社もデータ解析会社も自由に利用することができる、とされています。データ解析会社としては、自分たちはAIを提供するので、成果物は共有として欲しい、とのことですが、当社としては運転データを元にしたデータを流用されるのは困ると思っています。どのように考えたら良いでしょうか。

ちょうど、スライド52の図で議論をした話と多分同じことだと思います。自分がデータを提供して、向こうのデータ解析会社はそのAIで解析した成果物を共有したいと言っていると。データの共有と言っても何だかよく分かりません。共有とは何かを本当はきちんと考えておかないといけません。要するに、お互いが自由に使えるというだけでなく、それぞれが第三者に自由に使えることができるのかということです。もし、相手の会社が第三者に対して使わせることまで認める、そういうことまで「共有」が含んでいるとすると、様々なところに出回ってしまうので、自分でコントロールできなくなってしまいます。ですので、それはたまったものではありません。ただし、おそらく受領事業者B社としては他の企業にどんどん提供したいのしょうから、他の第三者にも使わせる権限が欲しいということの意味しているのだらうと。そうすると、提供事業者A社では全然コントロールできません。自分は使えるかもしれませんが、それと同様に他の事業者にもどんどん使われてしまうことになります。

それが嫌ならB社と取引するのをやめるというのも1つの選択肢でしょう。ですが、このデー

タ解析会社がものすごく能力が高いところだとします。そうした場合に、B社がどうしてもその条件を譲らないので利用するのをやめると言うのか、それともB社の能力は高いから譲歩して利用すると言うのか、そこについてはぎりぎりのチキンレースになります。交渉でぎりぎりのところまで行った時に、対価を少し安くするとか、向こうが第三者に提供したら売上げの何%か自社にバックしてもらおうということで話がつくならそれはよいのですが、提供事業者Aの意図が、競合他社に使われたくないということであれば、お金を貰っても仕方ありません。

こういうところは現在、全然ルールがありません。もし収益分配するとしても何%とかいった業界慣行的なものも無いので、自分で考えないといけません。自分で考えるしかないのです、そこは難しいのですが、何がこの取引の目的かということから落とし込んで考えていくしかないと思います。

以上で終わります。ご清聴ありがとうございました。

## ◇質疑応答

### ○【司 会】

大変貴重なお話を、ありがとうございました。それでは、質疑応答に移りたいと思います。ご質問のある方は挙手をお願いいたします。

### ○【質問者A】

本日は新しいテーマについて多角的な分析をいただきどうもありがとうございました。

私がお尋ねしたいのは、少し細かいことなのかもしれませんが、スライド 45 で右下のところに事後的に知って権限内、権限外という部分がございます、権限外のところが違法になるという図解かと思いますが、この権限の中か外かというのは、結局最終的に取得した転得者とその前のこの図でいうところの取引相手Cですかね。その間の契約で定められた転得者側の権限の内か外かと、そういう意味に理解してよろしいでしょうか。

### ○【村 尾】

そういう意味のほうです。そうしないと分からないですよ。

### ○【質問者A】

元のデータの保有者との関係ではないということですよ。

### ○【村 尾】

そこはデータの取引の安全ということだと思います。

### ○【質問者A】

ありがとうございました。

○【司 会】

他の方はいかがでしょうか。

○【質問者B】

本日は貴重なご講演どうもありがとうございました。Suica 事件についてお伺いしたいのですが、恥ずかしながら詳しくは知らなくて、スライド 21 で提供先が「第三者」に該当しないとされる場合という中に、委託であればよいと。該当しないと書かれていたのですが、Suica 事件は委託では無かったのですか。何が問題になったのでしょうか。日立に J R が委託したということではないのでしょうか。

○【村 尾】

この問題は法律論では無いのです。こういうことを J R 東日本がやっているのが不気味だということで、もうそれで炎上してしまって、J R 東日本ができなくなったのです。目的がはっきり言ってよく分からないのです。今公表されている検証委員会の報告書によると、何のために今回のデータの提供を行ったかということは、利用者による駅の利用状況やその構成を把握し、地域や駅、沿線の活性化に資する様々な分野で活用することが期待され、利用者はもとより社会一般のための基盤となるという目的でといったことが書いてあります。何を言っているのかがよく分からないのです。もし本当に J R の中だけで使うために 1 回渡してそれで分析をして、分析したデータが戻ってくるということでしたら、多分委託なのだと思います。

しかし、報告書の記載はより目的が広いように思われます。日立でも関係会社が利用するつもりがあったのかもしれないと、そうするとその部分は委託では無くなってしまいます。その話は置いておくとして、法律論から言えば、委託なのでセーフという可能性も相当あって、それから個人情報にもそもそもならないのではないかと、これくらい匿名化していればというようなところだったけれど、当時からすると、そんなデータと言っても何か後で色々なものを組み合わせれば、個人が分かるのではないかとかそうした不気味さが先行してしまった事故というか事件です。

○【質問者B】

ありがとうございます。

○【司 会】

それでは時間の関係もございますので、あとお一方どなたか。

○【質問者C】

今日はありがとうございました。

今回のケースに当てはまるわけではないのですが、自治体等が持っているデータ、今回の個人情報は国等は対象から除くと、最初の方のスライドに記載がありましたけれど、自

自治体が持っているビッグデータ等、そういうものを例えば企業が何か新しいビジネスを生み出す時に自治体と協力して実施する時に法規制について気を付けなければならないことはありますか。今回の趣旨と合っているのか分からず、恐縮ではございますが。

○【村 尾】

まず、先程の国等を除くというところは、個人情報保護法の規制対象から国が除かれるということで、国が持っているデータを例えば企業が貰った際に、それがもし個人情報に当たっていれば、企業はそれが個人情報取扱事業者という状況であれば、個人情報保護法が適用されます。スライド 13 の図ですよ。国・地方公共団体・独立行政法人等は除くと書いてあって、これは個人情報保護法では規制されない。

それから、地方公共団体からデータを貰いましたといった時に、それがもし同じ個人情報だったら、それは企業としては個人情報として個人情報保護法を守って使わなければならない。貰ったものがオープンデータであれば、多分個人情報では無いのだと思いますけれど、もしそうではなく何かの契約で情報提供を受けたとしたら、それが個人情報であるとしたら個人情報として、企業として規制がかかってきます。

○【質問者C】

企業が受け取ること自体は可能なのでしょうか。

○【村 尾】

少なくとも委託の場合は受け取れるでしょうね。データを加工する等が求められるでしょうから。

○【質問者C】

ありがとうございました。

○【司 会】

よろしいでしょうか。それでは、本日の特別研究講座を終了とさせていただきます。本日はありがとうございました。

以 上