

デジタル社会・新産業創出調査特別委員会会議記録

デジタル社会・新産業創出調査特別委員会委員長 高橋 こうすけ

- 1 日時
令和6年8月7日（水曜日）
午前10時1分開会、午前11時30分散会
- 2 場所
第2委員会室
- 3 出席委員
高橋こうすけ委員長、畠山茂副委員長、名須川晋委員、柳村一委員、千葉秀幸委員、
神崎浩之委員、臼澤勉委員、菅原亮太委員、佐々木朋和委員、飯澤匡委員、
田中辰也委員
- 4 欠席委員
なし
- 5 事務局職員
正部家担当書記、藤澤担当書記
- 6 説明のため出席した者
森・濱田松本法律事務所 弁護士 岡田 淳 氏
- 7 一般傍聴者
なし
- 8 会議に付した事件
(1) 調査
生成A I の課題と法規制化
(2) その他
次回の委員会運営等について
- 9 議事の内容

○高橋こうすけ委員長 ただいまからデジタル社会・新産業創出調査特別委員会を開会いたします。

これより本日の会議を開きます。本日は、お手元に配付しております日程のとおり、生成A I の課題と法規制化について調査を行いたいと思います。

本日は参考人として、森・濱田松本法律事務所、弁護士の岡田淳様をお招きしておりますので、御紹介いたします。

岡田様の御略歴につきましては、お手元に配付している資料のとおりでございます。

本日は、生成A I の課題と法規制化と題しましてお話しいただくこととなっております。

岡田様におかれましては、御多忙のところ、このたびの御講演をお引き受けいただき、

改めて感謝を申し上げます。

これからお話をいただくことといたしますが、後ほど岡田様を交えての質疑、意見交換の時間を設けておりますので、御了承願いたいと思います。

それでは、岡田様、よろしく願いいたします。

○岡田淳参考人 本日はこのような場にお招きをいただきまして、誠にありがとうございます。なかなかこういった形で都道府県議会に招かれてお話しするという事はないので、私にとっても大変貴重な機会でございます。

きょうは、いろいろ資料を用意していますけれども、そこまで細かく逐一お話しするというよりも、概要を説明して、メリハリをつけポイントを絞ってお話ししたいと思っています。そのため、全てを理解する必要は全くなくて、疑問があればいつでもお気軽に御連絡いただければお答えさせていただきますので、どうぞよろしくお願い致します。

早速ですが、導入として、日本のAIガバナンスをめぐる全体像という大きな話からしていこうと思います。御案内のとおり、2022年11月にOpenAI社がChatGPTの提供を開始して、その衝撃はすごくて、いわゆる大規模言語モデル、LLMに代表される基盤モデルのAIの進化、社会実装が急速に進んでいるということ、日本だけでなく、社会全体に衝撃を与えたところであります。

私もいろいろ関与させていただいていますが、政府での動きも急速に進んでいて、去年、そしてことしに至るまで、矢継ぎ早にいろいろな政策が打たれていますので、まずはその全体像をお話ししたいと思います。

2023年の2月に、自由民主党において、AIの進化と実装に関するプロジェクトチームが設置されました。私もワーキンググループのメンバーです。その後、4月にAIホワイトペーパーというものを公表しました。5月に内閣府でAI戦略会議が設置されまして、こちら私もメンバーなのですが、座長は東京大学の松尾教授で、AI研究の第一人者です。設置後、暫定的な論点整理というものを公表しました。5月に設置して、2週間ぐらいでこの論点整理を公表したということになります。

去年、いわゆるG7の広島AIサミットがあって、日本がその議長国ということで、グローバルにいろいろな政策のすり合わせ、ガイダンスをつくっていかうということで、岸田首相が、広島AIプロセスというものも始められました。

6月になると、生成AIとプライバシーの問題が論点になり、個人情報保護委員会が、OpenAI社と利用事業者に対して注意喚起を公表しました。OpenAI社のやっていることが違法だと言ったわけではないのですが、こういうことを守ってくださいということを知った形になります。

個人情報やプライバシーのほかに、著作権の問題もございます。AIで世界中の著作物を学習させるとか、あるいはアウトプットしてみたら既存の著作物に似たようなものが出てきたという話はよくあると思います。特に日本新聞協会などのコンテンツホルダーが非常に懸念しておりまして、無断でどんどんAIに学習されてしまうことで、クリエイター

は今後どうなるのか、そういった懸念もあります。文部科学省の文化審議会において7月から、A Iと著作権に関する検討を開始しました。私はメンバーではありませんが、有識者としてヒアリングに対応させていただきました。

その後、10月に、A Iと著作権の問題に関連して、著作権以外の知的財産との関係も非常に重要だということで、内閣府において、A I時代の知的財産権検討会が設置されました。私もメンバーを務めています。

先ほど5月からG 7の広島A Iサミットの話が動いていたという話をしましたが、広島A Iプロセスが一つ成果を見せまして、広島A Iプロセスに関するG 7の首脳声明を発出しました。

2024年の2月に、A Iセーフティ・インスティテュート、いわゆるA I S Iを政府の中に設置しております。厳密に言うと、政府の中でもI P A、独立行政法人情報処理推進機構という団体の下に設置しております。

3月に、文化審議会のA Iと著作権の検討を開始しました。これが一応の成果を見せまして、A Iと著作権に関する考え方というものを3月にファイナライズをして公表しています。

また、4月に、A I事業者ガイドラインというものを公表しております。

5月には、先ほどの内閣府のA I時代の知的財産権検討会、これも成果を見せまして、中間取りまとめを公表しました。

先月あたりから動いていることとしまして、ヨーロッパにおいて包括的、横断的なA I法が整備されることに伴い、日本で同じ道をとらないにせよ、規制をしないで本当にいいのかと議論になっており、その規制の可否や程度について議論する、A I制度研究会が設置されました。第1回の会合が先週の金曜日に首相官邸で開かれまして、私も参加しました。岸田総理も同席されて、第1回が開かれました。

現在進行形でいろいろなことがまだまだ動いております。本当に急速に政府の中でも議論が進んできたというのが実態であります。

先ほどいろいろお話をした議論の一つの出発点である、去年5月のA I戦略会議で、2週間で作ったという暫定的な論点整理から一部を抜粋しております。こちら、リスクへの対応にフォーカスして抜粋していますが、もちろんA I戦略会議はリスク対応だけではなくて、基本的には政府も、与党の自由民主党も割とA Iに対してフレンドリーといえますか、どうやってイノベーションを促進していくか、それによってきちんと経済を潤していく、そういうところも含めて見えています。この暫定的な論点整理というのは、ほかにどうやったらA Iを開発しやすくなる環境が整備できるのか、A Iを利活用しやすくなるのか、いろいろなことを書いています。きょうは私が呼ばれたということで、法律家の視点から、主に法的なリスクも含めたリスクについてお話するということが、私自身の一つの役割だと思っています。

どういう方向性で整理がされているのかというと、まず、一番下のところで八つほど大

きなリスクを挙げています。機密情報、個人情報、犯罪の巧妙化、容易化、偽情報、誤情報などを挙げています。よくフェイクニュースなどが問題になっています。サイバー攻撃も、AIによってより巧妙化しています。逆に、AIによって防衛もしやすくなっている部分もあるかもしれません。教育現場での扱いや、先ほど言った著作権侵害、あるいはより広い社会的なリスクという意味では、AIにどんどん仕事を奪われてしまって失業者がふえるのではないかとというリスクがあります。こちらについては、日本だと少子高齢化が進んでいるので、海外のほうが問題意識が強い気がするのですが、日本でも、特に生成AIによって、知的労働者の仕事がどんどん奪われるようになっていくのではないかと、生成AIの特徴として挙げられています。

こういったリスクに対応して、どういう制度が必要であるか、去年の5月に議論されました。基本的な方向性として、一旦は既存の法制度やガイドラインを前提に、どこまで対応できるのかをもう少し深掘りして検討しましょう。もしそれでいけるのだったらいいし、それでいけない可能性があるのだったら、もう少し諸外国の状況なども参考に対応をさらに検討しようということで、一旦整理されました。そのため、当面は既存の法制度やガイドラインのもとで何ができるかということを検討しました。例えば、ガイドラインのようなものを新しく更新したり、先ほどの著作権法についての考え方についても、既存の著作権法のもとでどう整理されるのか、検討してきた状況になります。

先に進める前に、一般の事業者、民間事業者に限らず、皆さんのようにAIを利用される利用者側からみた主な法的リスクについて、お話ししたいと思います。

いろいろな議論がありますが、この縦軸が対象となる 이슈 です。著作権の話、個人情報の話、機密情報の話、そのほかいろいろ、いわゆるハルシネーションと呼ばれているようなことです。私もそうなのですが、自分についてAIで検索すると、でたらめな情報をもっともらしく出てきます。そういったことの名誉、信用毀損、不適切な内容等も含めて、縦軸に取っています。

右側の横軸は、一つ目と二つ目が、どういう情報を入力して、どういう情報が出力されるかをあらわしています。入力段階、学習段階では、まずファインチューニング、追加学習のようなことをします。こういう本格的な学習入力の段階になってきて、一般の利用者であれば関係ないのかもしれませんが、ある程度本格的に活用しようとする、こういう問題が出てきます。

その上で整理をすると、例えば入力、学習段階でいうと、既存のクリエイターがつくったコンテンツや著作物を学習用データとして入力する場合にどういう問題があるのか。日本の著作権法は、AIによって学習させることは自由にできるような条文が整備をされています。ただし無制限ではありません。アウトプットで既存のコンテンツと似たようなものが出てくると、それは著作権侵害になる可能性はそれなりにあるわけです。そのため、そういったリスクというのは、入力の段階でそのようなアウトプットを誘発するように入力をしてしまうと、アウトプットのところで問題になってきますので、そのあたりは気を

つけなければなりません。

あとは、いろいろな世の中にあふれているコンテンツ、例えば有料の会員でないと入れないコンテンツになると、利用規約がしっかりしています。著作権法に違反していなくても、利用規約に違反してしまうと、それは問題になるので、一定の学習入力に制約があります。

そのため、今の著作権法というのは、AI学習にはフレンドリーなのですが、限界もありますし、事業者としては、ChatGPT、Geminiなども含めて、普通に使っていれば著作権侵害となるような生成物というのは出てきにくい技術的なガードレールはありますので、過度に心配する必要はありません。ユーザーとしては不用意に、少なくとも著作権の入っているコンテンツ、著作権の対象になっているコンテンツをプロンプトに入れたり、あるいは著作権侵害を誘発するようなプロンプトを入れたりすることは避けるよう一定の社内ルールを導入して、一定の歯どめをかけながら使っているというのが現状になっています。

個人情報については、一般論として個人データを本人の同意なく入力すると、個人情報保護法上のいわゆる第三者提供、目的外利用に該当する可能性があります。

ただし、実際問題としては、去年の6月、個人情報保護委員会から注意喚起が出まして、それを見てみると、例えばプロンプトに入力する場合でも、一定の場合には可能という整理になっております。基本的には事業者がOpenAI社、マイクロソフト社のAzureやGeminiを使うとき、それらの利用契約には、勝手にAI事業者が学習データには使わないという条項があるものがほとんどです。そのため、学習用データとして利用されないように担保されていて、あくまで通知、公表されている利用目的の範囲で使っていれば、個人情報保護法上の問題は基本的にないと整理することが、一般的な考え方であると思っております。そういう意味では、この辺は一定のリスクはありますが、普通に使っていれば一応セーフであるという余地は十分あると考えております。

そうはいつでも、多くの事業者では、あまり不用意に何でもかんでも個人情報を入力されると、アウトプットの観点からは問題なので、社内ルールで一定の制約を課しているのが実情です。

第三者から秘密保持義務を課されているような機密情報を使用すると、契約上の守秘義務違反になる可能性があります。また、自社の機密情報を入力すると、本来秘密として法律上保護されるはずのものが保護を受けられなくなる可能性がある一方で、これは理論的に確立しているわけではないのですが、セキュリティーがしっかりしていて、学習用データとして用いられないようなAIのプロンプトとして入れる限りであれば、守秘義務違反にはならないという整理ができるのという考え方もあります。直ちにアウトというわけではなくて、いろいろな理論構成でやりようはある場合もあると思っております。事業者としては、あるいは利用者としては、何でもかんでも機密情報を突っ込んでしまうと、それは大きな問題なので、普通機密情報は、全く機密情報を入れないようにしている事業者もあ

れば、そうはいつでもやはり一定の機密情報を入れないと業務のDX、効率化にはならないということで、機密情報のレベル分けをして、このレベルまでは入れていいけれども、このレベルでカテゴリ化されたものは入れてはだめというように制限している事業者もいらっしゃいます。

そのように、いろいろなリスクがあって、注意すべきことはありつつも、法律上はそれなりにどの分野においても、今の法律の考え方で手当てができないわけではありません。基本的には各事業者で一定の社内ルール等を設けながら、できるだけテクノロジーを使えるところは使って、イノベーション、DXの流れを起こしていこうという形で、うまくバランスをとりながら、使っているのだと思っております。

今お話ししたのが著作権、個人情報保護法、個別法の話なのですが、よりAIを使う、あるいは開発、提供するに当たって、より包括的で横断的な規制があるのかどうかを示したのがここからのスライドになっています。

先ほど、ことしの4月にAI事業者ガイドラインというものができたとお話ししたのですが、これについて少しお話ししたいと思います。もともと、先ほど言ったような著作権法、個人情報保護法など、そういった個別の法律は別として、AIについて包括的に、横断的に規制する法律があったのかと言われると、日本ではありません。しかし、法律ではありませんが、ガイドラインが一応ございます。実は以前から、数年前から日本ではガイドラインがありまして、細かいものを挙げるとたくさんあるのですが、主要なものとしてはこの三つです。いわゆるAI開発ガイドライン、AI利活用ガイドライン、こちらは総務省がつくったものです。AIGバナンス・ガイドライン、これは経済産業省がつくったものです。最初の二つが、ハイレベルなことを書いていて、最後の一つが実践に落とし込むような、そういうものが対象になっております。もともとこういう三つの大きなガイドラインがあったのですが、いずれも法律ではなくて、いわゆるソフトローという、守らなくても何のサンクションもないし、守る義務も法律上はありませんが、一応ガイダンスということであったわけです。

これまでつくられていたガイドラインは、いわゆる生成AI以前のAIを対象にしている、生成AIの発展を踏まえたものではありません。三つあって、どれを見ればいいのかわかりにくかったので、この三つのガイドラインを統合し、アップデートしつつ、生成AIの発展も踏まえて作り直そうと、去年あたりから作成の作業を進めております。去年の12月に案が公表されまして、パブリックコメントを1月、2月とやっていて、4月に最終的なガイドラインが公表されました。分量がすごく多くて、本編と別添で300ページぐらいあるのですが、全体の位置づけだけ少し御説明をしようと思います。

このAI事業者ガイドラインというのは、WHYとWHATとHOW、その三つの観点で構成されています。WHYというのは、一番ハイレベルの基本理念のところですね。それこそサステナビリティ、ダイバーシティなど、すごく抽象的なレベルの話です。

WHATは、WHYより抽象度が低いのですが、HOWに比べると抽象度が高い、そう

いう指針のレベルであります。安全性、プライバシー、公平性、透明性、そういったレベルの話です。

HOWというのは、それをさらに具体的に落とし込んでいくとどうなるか、そういう観点の話になっていきます。

このガイドラインには、本編と別添がありまして、特に別添が長く、本編ではこのWHYとWHAT、別添でHOWの部分の規定をしています。やはりHOWというのは具体的な話で長くなるので、別添がHOWの話をしているということになります。

このWHY、WHAT、HOW、この軸があるのと、もう一つは主体ごとに整理をしているということで、AI開発者、AI研究者、AI利用者のレイヤーに分けて主体別の話をしております。

この主体ごとに分けていることについて、解説が9ページのスライドにあります。開発者というのはAIシステムを開発する、典型的にはOpenAI社やグーグル社、あるいはそこまでのレベルではなくても、中規模のシステム開発も含まれます。ほかにもいろいろあるのですが、決して事業者の数が多いわけではないですよ。開発者とはデータ前処理学習から開発をしていく段階まで関与している主体になります。

次に、AI提供者です。これは日本企業でも多いのですが、AIシステムをアプリケーションや既存のシステムに組み込んで、サービスとして利用者に提供していくような事業者です。

一番多いのはAI利用者です。AIシステム、AIサービスを利用する事業者。これは、もう日本企業、日本の事業者でもかなりの割合を占めると思います。一番多いのは利用者で、次に多いのは提供者で、一番少ないのが開発者になるかと思います。こういう形で主体を分けて整理をしているということも、このガイドラインの特徴になっています。

先ほどWHYとWHATとHOWということで申し上げましたが、このスライドではWHYとWHATを整理しています。ディグニティと、さっき言ったダイバーシティ、サステナビリティなど、こういう抽象的なレベルの話になります。

やはり有名なのはWHATですね。先ほど言いましたけれども、安全性、プライバシー保護、セキュリティ確保、透明性、公平性、アカウントビリティ、人間中心、このあたりをメインに、もう少し細かくガイドラインを見ていただくと整理をしています。

繰り返しになりますが、法的に拘束力があるわけではなくて、守っても守らなくてもいいのですが、そうはいつでも基本的な観点というのはこのガイドラインで網羅されているので、自分の立場に応じて、一通り見ていただければと思います。基本的にAIというのは、AI以外もそうなのですが、法律を守っていればいいというわけではなくて、レピュテーションリスクがあるので、不適切な使い方をすると、法律に違反していなくてもすぐにネットなどで炎上して、撤回に追い込まれるようなことが結構あるので、こういう観点を意識するためにも、すごく参考になる書類だと思っています。

また、大きな話になってしまいますが、今申し上げたように、基本的には日本でAIを

包括的、横断的に規制する法律は今の段階ではありません。今申し上げたような事業者ガイドラインのような、いわゆるソフトローを進化させることで対応させていくというのが日本の方向性になっています。少なくとも当面は、ソフトローを中心にしていくということが日本政府のスタンスです。それは少子高齢化を含めた社会課題がいろいろある中で、AIのようなイノベーションを積極的に活用していくことにとっても価値や重きを置いている日本のスタンスに即していると思います。

他方で、ハードローをつくったほうがいいのではないかという議論が少なからず進んでいるというのも事実です。特にヨーロッパにおいては、AI法というものが8月1日に発効されました。実際施行されていくのはこれからになっています。アメリカでは、ハードローに消極的な発想なのですが、例えば安全保障、いわゆるデュアルユースと呼ばれるような、軍事利用もできるようなAIを中心に、企業は一定の自主的なコミットメントというのを求めています。さらに、いわゆる国防生産法に基づいて、本当に危険なものについては一定の規制をするというような議論も着実に進んでいます。また、中国はいち早く法律をつくって、導入しております。

そういう意味では、もちろんソフトローも大事なのですが、法的拘束力を持ったハードローを導入、あるいは検討する方向に進展しつつあるのではないかと思います。

これは、本当にいろいろな議論があるところですが、一つの方向性として、日本でも、提供者、利用者については、ソフトローがあれば十分ではないかという議論も根強いのですが、特に高リスクなAI開発者については、確実なリスク対応が必要になるのではないかと、こういった議論が強くなってきております。

自由民主党でAIの進化と実装に関するプロジェクトチームのワーキンググループ有志による提言に私も入っているのですが、いわゆる責任あるAI推進基本法というような、これは仮称ですけども、そういったものの素案をたたき台として議論の俎上にのりました。これは、まさにハイリスクなAI開発者について、一定のハードルを設ける必要があるのではないかということの問題提起したことになります。

誤解のないように申し上げますと、自由民主党はAIを何でもかんでも規制しようとしているわけではなくて、むしろすごくイノベーションを推進しようという、AIフレンドリーな日本を打ち出そうとしてきましたし、これからもそうだと思います。規制一辺倒ということではなくて、基本的にはイノベーション重視で、ソフトロー重視という路線は全然変わっていないのですが、全く野放しでいいのかという疑問は残ります。といいますのも、必要最小限の規制というのはあってもいいのではないかというのが、いわゆる責任あるAI推進基本法の議論の文脈であります。

そのため、この素案の中身もそんなに厳しい規制を入れるというイメージではなくて、対象もすごく絞っています。あくまで、社会的影響が大きいフロンティアモデルを対象にしております。やはり主として想定されているのは、海外の大規模なAI事業者、皆様が知っているような、そういうところに絞っています。あとは義務の範囲でもあれこれ個別

に言うということではなくて、どちらかというともっと大きな体制を遵守しなさいとか、あるいは一定の報告をしなさいとか、遵守すべき体制の中身も、政府があれこれ決めるというのも技術の進歩のスピードに追いつかないだろうということで、民間を交えて、政府と民間が協調しながら、民間の実践にも委ねていくようなモデルが、基本的には想定されている素案になっております。法律案のようなかっちりしたものでもないし、国会に提出されているわけでもないのですが、その一步手前の素案として、たたき台としての位置づけで提案をしています。

これをベースに、自由民主党ではことしのホワイトペーパーというのをつくっておりますし、さらにことしの6月に政府の統合イノベーション戦略というところでも、そういった考えを踏まえつつ、AI戦略会議の中でAI制度研究会を設けて、制度のあり方の検討に着手するという方針が示されました。

これを踏まえて、先ほども申し上げましたが、AI戦略会議の下にAI制度研究会を設置したというのが直近の動きになっております。7月19日に設置しまして、先週首相官邸で第1回会合を開催して、今後議論を進めて、本当にタイトなのですが、秋頃に中間取りまとめにて方向性を決めていく予定なのではないかと考えています。

このスライドのダイアグラムにあります。先ほど言った開発者、提供者、利用者、そしてプロバイダー、こちらは新しく出てきた概念なのですが、このあたりの主体を縦軸で分けていて、横軸で影響度、リスクで分けています。先ほどもお話ししましたが、AI開発者で、影響の高い、リスクの高いモデルを開発するこの①の部分の開発者について、今、主に議論が進んでいます。これもいろいろな考え方があるので、もちろんEU、ヨーロッパのような方向性を志向しないということはコンセンサスが得られていると思うのですが、他方で必要最小限の規制とはいっても、その必要最小限のハードローすら要らないのではないかという意見もそれなりにあり、やはり人によって意見が異なりますので、多様な成功例の意見を集約していく必要があります。この結論がどういう方向になるのか、ハードローを入れていこうという方向になるのか、やめましょうという方向になるのか、報道が先行していますけれども、今完全に決まっているわけではなくて、まさにこれから議論が進んで、方向性を決めていくことになると思います。

これが日本の方向性です。参考までにヨーロッパの状況についてもスライドを入れています。御案内のとおり、ヨーロッパではAI法というのが数年前から議論されていまして、ここ1年ぐらいでようやく制定され、発効したという形になっています。

ヨーロッパのAI法には、二つ軸がありまして、一つは用途に応じた規制です。ユースケースということで許容できないような用途なのか、ハイリスクな用途なのか、リスク限定的な用途なのか、あるいは大してリスクがない用途なのかという、この四つに分けて規制の強度を変えているというのが一つの軸になります。

もう一つの軸が、やはり最近の生成AIに対応した軸でありまして、生成AIの汎用モデルというのはいろいろな用途があり得えます。これがなかなか予測できません。そのた

め、従来型のA Iだと、あえて用途ごとに分けて規制していけばワークするのですが、汎用モデルのもととなるLLMをつくるような話ではなくて、どのように用途が化けていくかわからないので、用途ごとの規制というのはなかなかなじみにくいです。用途ごとの規制とは別に、汎用A Iについての透明性も含めた規制というのを入れています。汎用A Iの中でも、一般的な汎用A Iと、より高度なリスク、システムック・リスクを伴う高度なリスクの汎用A Iに分けて規律を設けています。

もともと2021年にこのA I法案ができていたのですが、当時は生成A Iがそこまで注目されていなくて、この汎用A Iに関する規定はなかったのですが、この議論の中で生成A Iがあつという間に世の中を席卷して、この汎用A Iについての条項が途中から入って制定されました。この二段構えの規制になっています。

特に去年大きな修正があつて、去年の12月に議会と理事会などが暫定合意をして、その後議会、理事会の承認を得て、先月官報に掲載をされ、8月1日になって発効しました。例によって、ヨーロッパは違反のときのサンクション、罰金あるいは制裁金が非常に大きいので話題になっています。全世界の売上高の7%が上限になっております。

これから段階的に適用が開始されていきます。ハイリスク、許容できないリスク、汎用A I、いろいろな規制があります。順次施行されていくということで、原則的な施行日は2年後の2026年8月となっていますが、2025年2月から施行される規制もあるので、2025年から2027年あたりにかけて適用開始されていく形になっています。

ここまですべての大きなガバナンスの話でありまして、ここから後半になります。著作権の話やプライバシーについて、生成A Iとの関係ですごく注目されているので、少しお話しします。

まず、著作権の話ですが、いろいろなレイヤーの議論がありまして、先ほどもA Iの入力の話と出力の話、学習、入力の話と出力、利用の話があると申しあげました。著作権の話もそれに対応して、厳密には三つ、大きな柱があります。この左の二つは、一番左が開発、学習をして入力していく段階、真ん中がアウトプットをして、それを利用していく段階、それぞれについて別の議論があります。

入力、開発、学習の段階では、世の中にあるいろいろなコンテンツ、著作権で保護されるようなコンテンツを無断でA Iに学習させていいのか、あるいはプロンプトに入れていいのか、そういう問題があります。ここについて、日本では著作権法第30条の4という、有名な条文がありまして、これによって情報解析がかなり自由に、クリエイターの許諾なく自由にできるというようなたてつけになっています。もともとは、一応A I等も想定してつくってはいたのですが、ここまで生成A Iで無断学習が進んでいくというのも、著作権法を制定したときにはあまり意識していなくて、それが今急速に無断学習し放題のような状況になっているので、非常にコンテンツホルダーが危機感を持っており、法第30条の4を改正すべきではないかとかということも含めて懸念を表明しております。そういう声もあつて文化審議会で議論が進んできました。これが去年からことしにかけての流れに

なっています。

あともう一つは、アウトプットの段階です。生成利用段階、これは例えばユーザー側で著作物について認識をしていなくても、A I モデルがコンテンツを学習してしまっていて、結果としてアウトプットがその学習したコンテンツと似たようなものが出てしまうと、基本的に著作権法的にはアウトになります。アウトになりますが、これも実はいろいろな議論があったので、議論を整理したほうがいいということで、去年から文化審議会で論点整理を行ってきました。

文化審議会で7月ぐらいから議論が始まりまして、私も有識者ヒアリングに呼ばれておりましたが、議論が注目を集めました。ことしの3月ぐらいにファイナライズをしたのですが、特に後半、いろいろな議論がヒートアップをしまして、この検討会の委員の間でもかなりかんかんがくがくの議論もありました。また、2万5,000件ぐらいパブリックコメントがありました。そうはいつでも、パブリックコメントだって字数制限があるので、本当にいろいろ書きたい会社というのは、字数制限のことを考えると、合計すると1社で10通出しているところもあるので、2万5,000件という数字を直ちにうのみにはできないのですが、それでも2万5,000件というのは結構な数字でありまして、それだけ社会的な注目の高さがうかがえます。

そのいろいろな議論の結果、3月に公表されたのが、A I と著作権に関する考え方についてというもので、それをまとめたスライドがこちらになります。一番注目されたのはこの一番下の(5)の各論点という、いろいろな著作権法の解釈について具体的な考え方が示されています。

一番盛り上がったのがやはり開発、学習段階ですね。先ほどの3本の柱の一番左側なのですが、A I が無断で膨大なデータを学習してしまって、こんなことが本当に許されるのか、法第30条の4で原則許されるのですが、歯どめが必要ではないかという議論であります。本当にモデルを1からつくるような場面でもそうですし、追加学習していくような場面や、あまりなじみがないかもしれませんが、RAGというような技術もあって、これは一定のデータベースをつかって、そのプロンプトを補助してあげるような位置づけの技術でして、モデルをいじることなく、できるだけ意図に沿うような適切なアウトプットが出るように工夫していくような技術です。そういうのも含めて、法第30条の4の限界をどこまで認めていくのかという議論がされました。

あまりテクニカルな話をするつもりはありませんが、法第30条の4というのはどんな条文になっているかと言いますと、平たく言うと、同条の第2項で情報解析というのがありますが、これはまさにA I の情報解析を含んでおり、情報解析の場合には、必要と認められる限度において利用できます。ただし、著作権者の利益を不当に害することとなる場合にはこの限りでない。そういう構成になっています。

なぜ著作権で保護されるコンテンツを無断で学習することが許されるかということですが、基本的な発想というのは、A I で解析をしていくというのは、人間がその著作物やコ

コンテンツを見て楽しむわけではないですよ。あくまでいろいろ分析をして、そのままそれをアウトプットとして出すわけではなく、そこから学習をします。例えばOpenAI社のChatGPTであれば、ある文字やある単語があったときに、次にどういう単語が来るのが一番確からしいかということを確認的に分析してアウトプットしているわけです。つまり、元のコンテンツを楽しむ、享受するような目的でないため、基本的には著作権者の利益は害されないというのが、法第30条の4の発想です。ただし、何でも無制限ではなくて、享受の前提が外れてくると、法第30条の4の対象外になります。また、場合によっては著作権者の利益を不当に害することがあり得るので、そういう場合にはアウトになるよう限定しています。この限定の部分がどうなっていくのか、どの範囲で認められるのか、非享受目的というところとただし書きになりますが、利益を不当に害することになる場合、この範囲を具体的に議論したことが一番のホットなトピックです。

結論については、すごく難解に書かれているので、きょうお話しはしませんが、結果について、どういうことを頭に置いて読めばいいのか、スライドに示しております。

まず、1点目ですが、法第30条の4のような権利制限規定というのは非常に柔軟で、人によっては日本にはこの著作権法のこの規定があるのだから、AI学習、機械学習パラダイスなのだというのですが、決して無制限ではないということをきちんと念頭に置いておく必要があります。だからこそ、各事業者でAIを使う場合には一定の社内のルールを決めて、その枠内でやっているわけなので、何でもかんでも許されるわけではありません。そこを理解しながら開発し、また利用する必要があります。

また、文化審議会の考え方や位置づけについてですが、あくまで基本的に著作権法の解釈というのは、裁判所、司法が判断する領域ですので、もちろん文部科学省や文化審議会が言うことは非常に重要ではあるのですが、それ自体に法的拘束力があるわけではありません。そういう文書だという前提で、この考え方を読めばいいのではないかと思います。

あとは、結局議論がいろいろヒートアップしまして、多くの論点で断定的な結論というのは示されておられません。複数の見解を併記している論点も多いですし、規範が抽象的に示されていても、それを個別の事案に当てはめると、人によってニュアンスの違いが生じます。そういう意味では、この考え方が出たことで、全てが画一的に決まったという話ではなくて、まだまだ論点は残っているのだと、そのことも理解しておく必要はあると思います。

そのため、各論点に記載されたニュアンスを正確に把握しておく必要があります。ある意味、いろいろな考え方の妥協の産物として出された考え方なので、表現もかなり工夫されています。全体を正確によく読めば、その文章をようやく理解できるのですが、個別に切り取って見ると、ここはすごく経営者寄りのことを書いてあるとか、あるいはここはすごくAI事業者寄りのことを書いているなというように読めてしまうところもあります。全体としてすごく慎重な言い回しが長い文章で記載されているので、報道もそうなのですが、一部を切り取るとミスリーディングになってしまいます。正確に文脈を見て確認

するというのがすごく大事になります。そういう意味では難しい文章なのですが、そういうものだと思っておく必要があると思います。

もともこの検討が始まった経緯として、コンテンツホルダーが懸念を示したということもありますが、世の中の目線では、クリエイター対AI事業者の二項対立関係というイメージが関係しています。決してそんな対立関係はなくて、今はクリエイターもAIを使わないと本当にいいものが見つからない時代になっています。本当に人間の頭でやるべきこととAIに任せるようなことをうまく駆使してやっていく、これはクリエイター側にも求められます。AI事業者に有利とか、クリエイターに有利とか、そういう関係にはなくて、お互い建設的にコミュニケーションをとって高め合っていくことが求められると思います。そうでないと、日本のクリエイターもどんどん沈んでしまうだけのような気がしています。テクノロジーを使えるところは使って、クリエイターも発展していく、AI事業者も発展していくという、ウイン・ウインの関係をつくっていく必要があると思います。

こちらが、文化審議会の議論のときに私が有識者ヒアリングで申し上げたことです。基本的に文化審議会の議論というのは、著作権法の議論の解釈についてが主なものです。結構難しいのは、どれだけ著作権法の解釈を精緻にしたとしても、そもそもAI事業者として何を、どういうコンテンツを学習していたのか、どういう技術的なガードレールを引いているのかなど、そこが透明性を持った形で開示されないと、なかなか権利者としても権利行使のしようがありません。そのため、基本的に著作権の議論というのは、著作権法の解釈だけの議論では完結しなくて、AI事業者としてのAIガバナンスの問題、まさに冒頭で申し上げたAI事業者ガイドラインのような話になりますが、やはり著作権法だけでは解決しない問題があるので、そこは注意しておく必要があります。

これが著作権の話でしたが、そのほかの知的財産権の話もいろいろあって、営業秘密を学習用データとして使っていいのかという話や、商標について学習用データとして使っていいのか、こちらは基本使っていいということが答えなのですが、そういった話もあります。

最近結構多いのは、肖像権やパブリシティの絡みで、特に声優の声にそっくりな声はAIで使われてしまって、それを野放しにしているのかという結構センシティブな議論も出てきています。

あとは、特許の話で、AIで簡単に発明ができるようになっていくと、これまでと同じような技術水準のレベルで特許を認めてしまっているのかという話もあります。

また、著作権法も含めて、法律だけで解決できる問題ではなく、やはり技術の問題や、あるいは契約に基づく問題など総合的に考える必要があるという話です。

このあたりは、AI時代の知的財産権検討会で検討が進められて、既にことし、数カ月前に中間取りまとめを公表しております。

最後に、個人情報やプライバシーをめぐる議論になりますが、先ほど言いましたように、去年の6月に個人情報保護委員会が注意喚起をしております。繰り返しになりますけれど

も、OpenAI社がやっていることが違法だと言っているわけではなくて、こういうことに気をつけなさいと言っているわけなのですが、この注意喚起は二つから成っています、一つはOpenAI社のような開発者に対する注意喚起、もう一つは皆さんを含む利用事業者に対しての注意喚起です。

開発者であるOpenAI社に対しては、要配慮個人情報といって、人種、刑罰の前科、病歴、そういったものを取得するのは原則NGなので、それを含まないようにすることや、利用目的を日本語で通知、公表しなさいといったことが書かれていて、こちらは皆さんに直接は関係ないかと思います。

皆様に関係するのは、利用事業者に対する注意喚起でありまして、ここは利用目的を達成するために必要な範囲内で使ってくださいということと、個人データを含むプロンプトの入力を行うときには、AI提供事業者が機械学習にそのデータを利用しないことを十分に確認してくださいということです。最初のほうで申し上げましたが、プロンプトに個人データを入れることも、AI事業者がそれを学習用データに使わないということは契約で担保されていれば一応セーフだと読めるような注意喚起になっていて、そういう意味では実務的なバランスをとった注意喚起だと思っています。

他方で、一般的な事業者は個人情報を何でもかんでもプロンプトに入れることを許容しているということは基本的にあまりなくて、社内ルールで一定の制限を課しているというのが大半だと思っていますが、個人情報保護法にはこのように整理されております。

あとは、今、個人情報保護法改正に向けた議論が進んでおりまして、これは必ずしもAIと関係ありませんが、一応3年ごとに改正の検討をするというその節目の年でありまして、今ちょうど中間整理というものが出されました。来年に改正される予定なのですが、まだまだ方向性が正確に決まっていないところもあります。

私からは以上です。御清聴いただきましてありがとうございました。

○高橋こうすけ委員長 これより質疑、意見交換を行います。ただいまお話しいただきましたことに関し、質疑、御意見等がありましたらお願いいたします。

○菅原亮太委員 今後、日本もAI規制が法制化されるかもしれないという点について、アメリカではイノベーション重視、ヨーロッパは規制型というところで、日本のAI法体系としてはどちらに近いような形になるか、岡田様のお考えがあればお伺いしたいと思います。

○岡田淳参考人 まさにAI制度研究会でこれから議論をされていくところなので、その方向性がどうなるかというのは、確実には読めないところではあります。日本がヨーロッパ型を志向していくという可能性はかなり低いのではないかと、前提としては思っています。

ヨーロッパでは、個人情報の保護について2018年くらいから適用開始されたEU一般データ保護規則、いわゆるGDPRという非常に厳しい規制がありまして、それこそアメリカのグーグル社、フェイスブック社、メタ社など、いろいろなところが膨大な制裁金を課

されております。そのときは、世界から物すごく警戒されたのですが、結果的にはそれがグローバルに波及をしまして、GDPRに近いような法律が、タイやブラジルにもあります。アメリカでもGDPRを意識した連邦法の制定について、ずっと議論されています。

そういう意味で、ヨーロッパはGDPRをつくって、それがヨーロッパの企業のイノベーションに寄与したかはわかりませんが、少なくともGDPR的な考え方はグローバルに広がっていきました。これをいわゆるブリュッセル効果と呼んでいまして、そこにヨーロッパの人たちは結構味を占めていると思います。

ヨーロッパのAI法も、国内からすごく反対意見がありました。フランス、ドイツ、イタリアなどは、AIのスタートアップが出てきているような国なのですが、過剰な規制が自国のAI産業の育成の障害になることを懸念しておりました。最終的には法律になりましたが、最後まで紆余曲折があって、今後もどの程度運用を厳しくしていくかということも含めて、まだまだ議論があると思います。

ヨーロッパ以外の国々というのはそこを見極めていく状況で、少なくとも直ちにヨーロッパに追随しようという国はかなり少数派だと思いますし、日本も当面は追随しないと思います。

アメリカ型はどうかというと、そこは結構悩ましいところで、多分今志向しているのはアメリカに近いと思います。ハードローには慎重でありつつも、最低限のところについては一定の規制を入れるという観点で、アメリカに近い形を志向する可能性が高いと思います。ただし、アメリカはアメリカですごくデュアルユースというか、軍事的な観点や安全保障の観点をメインに置いているので、そこと全くイコールになるかということ、よくわかりません。

他方で、日本にもっと開発を誘致するためには、規制はせめてアメリカよりは緩くないとやっていけないのではないかという観点もあります。そういった点で、アメリカとは目線が違う部分もありますし、グローバルに誘致をしていくという意味では、規制を緩くしていけないといけないのではないかという産業政策的な観点、あとは日本のスタートアップにも育ててもらおうという観点もあります。

他方で、ある程度規制をしっかりさせて、安全性を担保したAIを武器に、世界で戦っていくことのメリットもあります。

○菅原亮太委員 OpenAI社が4月にアジア初の拠点を東京都に出したり、マイクロソフト社が我が国にもデータセンターを投資したいということで、日本は今まで規制が緩かったので、外国企業の投資がふえてきたと思います。今後もAI法によって、外国企業に対する規制が盛り込まれるか伺いたいです。規制をした場合、外国企業は日本に対してどういう態度をとるのか、お考えがあればぜひ伺いたいと思います。

○岡田淳参考人 一つの重要なポイントとして、外国の事業者に対するモニタリングというのがあります。まさにおっしゃっていただいているように、外国からたくさんいいAI企業に投資をしてもらおう、誘致をするということが非常に重要である一方で、きちんと外

国事業者をモニタリングしていく必要があるという意識も、経済安全保障的な観点を含めて重要です。

これは、例えばアメリカであれば、明確なハードローがなくても、自国の中にある企業なので、アメリカ政府が強く言えば、アメリカに本拠を置いている企業というのは、一定程度従わざるを得ません。ただし、これが日本だと、日本政府が法律のないところで何を言っても、しょせんアメリカの事業者というのは従わないのではないかという懸念があります。フェイスブック社も今いろいろと批判をされていますよね。アメリカの企業というのは、強制力のある法律かどうかということで、表面的には協力するように見せて、露骨に態度を変えてくるというところはあります。そのためアメリカ政府とは違って、日本政府としてアメリカ企業に対して及ぶような、そういう規制を設けていく必要があるのではないかと思います。これは、一つの規制推進派の重要な原動力になります。投資を誘致するということとは、また少し違うベクトルなので、そのバランスはすごく難しいところだと思っています。

○佐々木朋和委員 行政にも生成AI等の専門家とともに、それをリスクヘッジするアドバイザー等も必要ではないかと思いました。これから自治体などで生成AIを使っていく場合には、アドバイザーは必要なのでしょうか。また、法曹界ではこういった生成AIに詳しい先生方というのはどのぐらいいらっしゃるのでしょうか。

また、先ほど声優の方の声が生成AIでつくられることについて規制されていくのではないかという話がありましたが、それを突き詰めていくと、物まねタレントがやっていることなども、規制が及ぶのではないのでしょうか。こういった生成AIが進んでくると、肖像権、個人情報、あるいはそれぞれのパーソナリティーを守る考え方が明確になり、規制が厳しくしていくのか、先生の今後の予想をお聞かせください。

○岡田淳参考人 1点目については、まさに自治体でどうAIを利活用していくか。これは去年からそうですが、いろいろな自治体で取り組みがされています。私自身も去年の夏に、東京都が生成AI利活用ガイドラインをつくった際に、有識者のメンバーとして関与させていただきました。やはり内部のリソースである程度リーガルがしっかりしていれば、場合によっては外部アドバイザーというのは必須ではないのかもしれませんが、特に初期段階や、内部でAIの領域におけるリーガルの体制が整っていない場合には、法的なアドバイザー、弁護士など、相談体制を整えておくというのは、大事だと思います。どんどん技術も変わっていきますし、利用契約等もどんどん変わっていくので、そういう意味で常に最新の情報を持っているような弁護士に相談されるということは、とても意味のあることだと思います。

特に東京都の利活用ガイドラインは、具体例としてプロンプトの入力方法について、どのように業務の利活用促進になるのかが、かなり具体的に図表を用いて記載されているので、参考にしていただければと思っております。

もし私でお役に立てることがあれば、いつでもおっしゃっていただければお手伝いさせ

ていただきますし、法律家の中でもこのAIは注目されているので、業務の一環としてやられている弁護士もふえてきていますので、私でなくても適切な方を入れていただければと思っています。

2点目の声優の話ですが、すごく重要なポイントを突いたコメントだと思っています。どんどん規制していくと、声の問題に限らず、AIで問題が起きた際に、それがAI特有の話なのか、それ以外にも関係する話だがAIで注目されるようになった話なのか、分けて考えないといけません。AIで問題になったので、規制を入れようとなると、場合によってはAI以外の、まさに物まねの話や、いろいろなところに波及してしまいう可能性があるのでは、一般的な規制として入れるのがいいのか、AIプロパーの規制として入れるのか、AIプロパーの規制として入れるのだったら、どこまでを守備範囲にするのが適切なのか、バランスを適切に考えないといけない話になってくると思います。

これは、ディープフェイクの話も同じで、AIではディープフェイクを発見しにくくなっているのでは、規制しないといけないという問題意識はすごくよくわかりますが、そのことを突き詰めていくと、パロディー作品等も含めて、どこまでが表現の自由で、どこからが偽情報として規制しないといけない領域か、そこにAI特有の問題がどこまであるのかというのはすごく重要な話です。それだけ難しい問題だからこそ、いろいろ議論しているけれども、まだ法規制について具体的な姿が見えてこないというのは、そのあたりに原因があると思っていますので、おっしゃっていただいたことというのは、一番本質的なところだと思っています。

○神崎浩之委員 6ページの個人データを本人の同意なく入力するという点について、これは、我々が普段使う際にも気をつけなければならないのでは。

○岡田淳参考人 普通の利用者としてどこまで自分事として関係あるかという質問かと思いますが、結構関係があります。皆さんAIに質問しますよね。質問指示がプロンプトになりますので、入力する際は気をつけなければなりません。実はもうこの時点で全部関係してくると、あと一番左のファインチューニングとかRAGですが、ファインチューニングというのはモデル自体をいじる話になるので、そこまで多くの事業者が関係するわけではありません。ただし、最近かなり多くの企業が既存のモデルをそのまま使うよりは、ある程度のカスタマイズをして、秘密情報とかも含めて入れています。より自分たちのニーズに合ったアウトプットを引き出すために、そのままではなくて、一定の加工を施して使いたいというニーズがあります。そのときに、ファインチューニングはモデルに手を加えるため、そこそ本格的な技術が必要なので、皆さんと接点はないかもしれません。いわゆるRAGと言われるようなものは、これはかなり浸透していて、モデル自体をいじるわけではありませんが、より自分たちの求めるアウトプットが出てきやすいようなデータセットを拡充して、プロンプトを補完してあげるという技術です。これは、今かなりの事業者が使っています。ファインチューニングまでいかななくても、RAGや、プロンプト入力は皆さんやっていますから、このあたりも含めていくと、もしかしたら自治体にも接点

はふえてくると思います。

繰り返しになりますが、リスクはふえている一方で、リスクへの対応について、やりようは十分にあるので、一定の技術的、または規則的な対応をしておけば、リスクを認識しつつ、活用できる方向になるというのが一般的な流れかと思います。

○**神崎浩之委員** 次に、9ページですが、提供者とは、具体的にどのような人を指しますか。開発者の開発したものを利用して、アプリをつくって売り込んでいるような人でしょうか。

○**岡田淳参考人** AI提供者というのはすごく広い概念で、今いろいろなソフトウェアサービスやシステムサービスというのは、売り文句としてAI活用をうたわないと時代おくれという風潮がありますよね。そういうのは、みんな提供者です。AI提供者というのは、すごく幅広いと思います。かなり多くの会社があります。

○**神崎浩之委員** 今例えばオリンピックでも誹謗中傷が話題になっております。それから、少し前は有名人が投資を勧める詐欺広告なども、本人に無許可で広告しているようなこともありました。このような問題に対して、政府の議論や、法曹界での動きについてお聞きしたいと思います。

○**岡田淳参考人** 非常に密接した関係するテーマだと思っていまして、やはり偽情報、誤情報、あとはまさに詐欺広告、そのようなものを含めて、情報の不適切なコンテンツの流通への対応をどうするのかというのは非常に重要な問題です。

これは、AIによって増幅されてきた側面でもありますが、AI特有の問題ではないというところもあります。今検討が進められているのは、総務省で、ワーキンググループの報告書を出したところですが、この偽情報、誤情報対策についての法的な手当てを含めた対応を提言しております。いわゆる情報プラットフォーム法というのがありまして、以前プロバイダー責任制限法と言われていたものの名称が変わったのですが、今回の報告書を踏まえて、早ければ来年にでも改正される可能性があると思っていまして、今後は総務省での議論が一番本丸かとは思っています。

ただ、これはAI特有の問題ではありません。やはり結構大きな問題意識としては、個別に情報の発信元をたたいていくというのは限界があります。フェイスブック社、グーグル社などのプラットフォーマーの側である程度きちんとやってもらわないといけないというのが大きな問題意識としてはあるので、プラットフォーマーへの義務づけも含めたところが基本的な部分だと思います。

○**高橋こうすけ委員長** ほかにありませんか。

〔「なし」と呼ぶ者あり〕

○**高橋こうすけ委員長** ほかにないようでありますので、本日の調査はこれをもって終了いたします。

岡田様、本日はお忙しいところ御説明いただきまして、誠にありがとうございました。

○**岡田淳参考人** ありがとうございました。(拍手)

○高橋こうすけ委員長 委員の皆様には、次回の委員会運営等について御相談がありますので、しばしお残り願います。

次に、9月に予定されております当委員会の調査事項についてであります。御意見等がありますか。

〔「なし」と呼ぶ者あり〕

○高橋こうすけ委員長 特に御意見等がなければ、当職に御一任願いたいと思いますが、これに御異議ありませんか。

〔「異議なし」と呼ぶ者あり〕

○高橋こうすけ委員長 御異議なしと認め、さよう決定いたしました。

以上をもって、本日の日程は全部終了いたしました。本日は、これをもって、散会いたします。