

## AIアドバイザーボード勉強会（第2回） 議事抄録

日時：2021年10月11日（月）16時～18時

場所：Zoom

出席者（専門委員）：森川座長、石川委員、三部委員、奈良委員、成原委員

出席者（NTTデータ）：総務部知的財産室 佐藤課長、松浦主任、セキュリティ技術部情報セキュリティ推進室 加納課長、由本主任、Data & Intelligence事業部ソリューション担当 今村課長代理、技術開発本部 鈴木シニアエキスパート（聴講者は省略）

### プログラム

時刻	アジェンダ	時間	発表者
15:50～15:55	趣旨説明、本日のプログラム	5分	技術開発本部 鈴木
15:55～16:00	座長より開会のご挨拶、当社出席者の自己紹介	5分	東京大学 森川先生
16:00～16:45	講演 AIと人権：プライバシーと差別に関する問題を中心に	45分	九州大学 成原先生
16:45～16:55	知的財産室におけるAI/データ利用ビジネスへの取組み	10分	知的財産室 佐藤課長
16:55～17:05	NTTデータにおけるセキュリティの取組み	10分	情報セキュリティ推進室 加納課長
17:05～17:55	質疑応答・意見交換	50分	ファシリテーター： 東京大学 森川先生
17:55～18:00	クロージング・集合写真撮影	5分	全員

### 議事概要

#### （1）趣旨説明・本日のプログラム

事務局を代表してNTTデータの鈴木シニアエキスパートから、AIアドバイザーボード勉強会の位置づけと開催趣旨の説明、および本日のプログラムの紹介があった。

#### （2）座長挨拶・出席者の自己紹介

座長の森川先生から本日の勉強会開催に向けた挨拶が行われた。

続いて、NTTデータの出席者から自己紹介が行われた。

(3) 講演：AIと人権：プライバシーと差別に関する問題を中心に

専門委員である成原先生から「AIと人権：プライバシーと差別に関する問題を中心に」と題して、講演をいただいた。

最初にビッグデータ・AIの利用に伴い、プライバシー侵害やマイノリティの人々に不公平な判断が行われる「AIによる差別」が問題として認識されるようになってきたことの事例として、入居審査AIに関する記事を示され、本件はAIに詳しい専門家らの中から懸念の声が示されていることが紹介された。具体的に考えられる懸念の例としてAIの予測結果について判断の理由が明確にされない透明性の問題、および、審査の公平性を担保するために国籍など不当な差別につながりかねない情報をデータとして入力・使用することの妥当性といった問題を挙げられた。一方で従来から例えば留学生は審査に通りにくいといった事例もあり、人間による審査でも透明性や公平性を欠くのではないかという疑問もある。これらのことから、本当に「AIによる問題」が新しい問題ということが言えるのか、むしろAIはこれまで見えにくかった差別を可視化することで、私たちの社会に対して差別にどう対処するかを迫っている面があるといった指摘があった。

次に、倫理と法の関係について身近な例を挙げて紹介され、倫理と法は重なっている側面と重なっていない側面があり、これを意識することが、企業が法の遵守、あるいはプラスして倫理への配慮を考えていく上での参考になることが指摘された。加えて、法の遵守や倫理面から自主規制を作って守ること自体は重要だが、それ自体が目的ではなく、それらが目指している目的は何かを意識して自分たちが守るべきルールや運用の在り方を絶えず見直していく必要があることを述べられた。

続いて、AIが扱うデータの観点から、プライバシーと個人情報保護法に関連する問題についての紹介があった。まず、プライバシーについて、これは法律で明文化されたものではなく、元々はマスメディアによって私的領域が脅かされることから個人の私的領域を守るために生み出されてきた権利であること、そして、情報化の進展で自分に関する情報が大量に収集され、それが知らない間に使われるようになったことで、自分に関する情報をいつ／どこまで／どのように他者に提供するのか選択する自己情報コントロール権の必要性が説かれるようになってきたが、その内容については法律家や学者の間でもコンセンサスが確立していないなど現状の紹介があった。これを踏まえて、個人情報保護法を守ればプライバシーが守れるわけではなく、プライバシーの範囲が技術や時代の変化とともに変わり得るものであることを意識することの必要性を指摘された。この考え方はAI倫理につ

いても同様であり、ある時期までは単に倫理的な要請に過ぎなかったとしても、その後の技術の発展などにより単に倫理的な要請だけに留まらず、法的に保護されるべき権利・利益として認められるようになるということがあり得ると指摘された。また、個人情報保護法に関しては、AIによるプロファイリングにより些末なデータからでも病歴や信条などのセンシティブ情報の推測ができるようになってきたことなどを踏まえ、海外では規制の動きがあること、日本でも新卒向けの就職情報サイトによる内定辞退率の提供問題などを受けて昨年に個人情報保護法が改正され、クッキーなど個人関連情報の第三者提供が制限されたほか、違法または不当な行為を助長・誘発するおそれがある方法により個人情報を利用することが禁じられたことが紹介された。

また、AIに関する差別の問題は、データのバイアスが原因とされるが、AI自体が差別を生み出しているというよりも、人間がこれまで生み出してきた差別の構造をAIがデータから学習することを通じて、AIが差別的な判断を反復再生産しているというのが実情に近いのではないかという指摘があった。そのため、企業としても単にAIによる差別を防止するだけではなく、そこから明らかになった従来のビジネスや社会における不公平な慣行や差別につながりかねないような慣行を見直していく必要があることを述べられた。

講演の最後に、まとめとして、人権が尊重されるビッグデータ・AI社会の実現に向けて、企業も主体的に立法に先駆けて、自主規制やガバナンスを構築していく必要があること、その際には法令や自主規制、標準を単に遵守するのではなく、それらを遵守すべき目的、例えばプライバシーや平等、公平性、個人の尊厳など目的とする様々な価値を意識して、自ら主体的にルールを形成し、運用していくことが重要であることが指摘された。

#### (4) 講演：知的財産室におけるAI/データ利用ビジネスへの取組み

NTTデータの佐藤課長から知的財産室の取組み紹介が行われた。AIやデータを用いるビジネスや当該ビジネスでのPoC (Proof of Concept：実証実験) において、事業展開・促進を見据えた成果物の権利整理をどうするかなど、実際に現場から挙がってくる相談へ適切に対応するための体制面での整備や対応実績、AI/データ利用ビジネスに関する情報配信、教育・啓発等の活動状況の紹介があった。その具体例として、1)PoCに関する契約相談についての法務室との連携整備、2)AI生成物(学習済パラメータ等)やデータの権利帰属と使用条件について定めた契約書雛形の整備、3)クローリング技術を利用する際の法的留意点の周知、4)経産省ガイドライン(AI編、データ編)のポイントまとめ資料や「AI/データ

利用ビジネス事例集」の作成・展開、5)プロジェクト向け研修の実施、の5点の事例が紹介された。

(5) 講演：NTTデータにおけるセキュリティの取組み

NTTデータ情報セキュリティ推進室の加納課長から、NTTデータにおける情報セキュリティガバナンス体制や個人情報保護の取組みの紹介が行われた。これまで取り組んできたビジネス向けのセキュリティと自社のセキュリティの2つに加えて、今後は第三の極としてAIのセキュリティが加わってくることを念頭に、「人間中心のAI社会原則」のうち、セキュリティの観点からは「プライバシー確保の原則」と「セキュリティ確保の原則」を考えていく必要があること、匿名加工データもAI技術を考慮すると個人データに戻ってしまう可能性があることに想像力を働かせながら、システムの開発・設計・運用を進めていく必要があることが述べられた。

(6) 質疑応答・意見交換

座長の森川先生のリファレンスにより、講演に対する質疑応答・意見交換が行われた。主な論点は以下のとおり。

【鈴木シニアエキスパート】

プライバシーのお話の中で「自己情報コントロール権」について、まだコンセンサスが得られていないということだったが、今後、こういった方向になりそうか、見通しをお伺いしたい。

【成原委員】

学界や判例でも理解が分かれているところであるが、最近、ITの発展を踏まえ懐疑的な見方が有力になりつつある。ITの発展により個人情報が日常的に収集、利用されるようになっている中で、個人情報の完全なコントロールを求めることは非現実的になっているともいえる。こういった現状を踏まえ、個人情報の完全なコントロールを求めるよりも、個人情報の取扱いによって、本人に不利益が生じないように個人情報を保護することの方が重要ではないかという見方が、専門家や学者の間でも有力になっている。

**【森川座長】**

三部先生のご見解をお伺いしたい。

**【三部委員】**

以前申し上げたとおり、AIビジネスの幅広いステークホルダーに配慮しつつ、AIビジネスが現行法や社会通念に反しないようにするため、会社としてガバナンスを構築していく必要がある。成原先生のお話もこの視点から参考になると考える。

成原先生には、プライバシーの概念を明確化する方向で議論をした方が良いかについてお伺いしたい。何がプライバシーに当たるかについて、判例では一定程度示されているが明確ではない。

**【成原委員】**

裁判所、あるいは研究者の役割として、そういったプライバシーの内容を、できるだけ明確化していくことが期待されるというのはご指摘のとおりである。プライバシーという権利自体が、アメリカでも日本でも明文上の根拠を持つものではなく、解釈によって導かれてきた新しい権利である。もともと倫理と法の間にあるような権利で、プライバシー侵害があるかどうかについて、裁判官も、一般人に「この情報についてプライバシーを守ってほしい」という期待があるかどうかを1つの手がかりにして判断していると思われる。したがって、社会の意識の変化により、プライバシーの保護範囲が左右せざるを得ない面がある。おそらく今後も技術やメディアの発展に伴って、プライバシーの在り方は変化していかざるを得ないところがあり、企業としても常にプライバシー・ガバナンスの在り方を見直していく必要がある。

**【三部委員】**

ご回答を受けて2点述べたい。1つはプライバシーが法的・倫理的に問題となるケースを企業が適切に認識する必要があることである。“プライバシー”という概念で議論されるケースは、一般の方が認識するよりもだいぶ広い。もう1点は、成原先生のおっしゃるとおり、プライバシーの外縁を明確化し切れない点である。そのため、個別のAIビジネスごとの技術、使われる場面、ステークホルダーへの影響を考えるプロセスが必要である。これらプライバシーの課題を含め、法的・倫理的に求められる対策を、御社の個別AIビジネス事例

を通じてお伝えしていきたい。

**【森川座長】**

ありがとうございます。他、いかがでしょうか。

**【松浦主任】**

最初の質問の回答の中で、今の学説上でも、個人に不利益が生じない場合には、個人情報保護法上の規制をかけないほうがよいのではないかといった話が出てきているということ伺った上での質問になるが、実際にその部分がどれぐらい実現できるのか、法律上は落とし込まれる可能性があるのかを伺いたい。そこができれば、技術の進展に大きく貢献できそうだが、一方で保護とのバランス、その方針が見えているのかどうか。

**【成原委員】**

個人情報保護法では個人の権利利益を保護することが目的とされているので、個人に全く不利益を与えない、個人の権利侵害につながり得ないような個人情報の利用は、もしそのような利用があるとすれば、そもそも論でいうと、構わないといえる可能性もあるかと思う。問題なのは、現実には何が個人の権利利益の侵害につながり得るかというのは、あらかじめ予測することが難しいということである。例えば、些末なデータからセンシティブな情報が推測できてしまうかもしれないし、匿名加工情報にしたとしても、本当に技術的に完全に特定の個人が再び識別されるリスクがないかという点、完全にゼロとは言い難い。ある種のリスクの問題で、個人情報保護法についても、EUのAI規制案と同様に、最近はリスクベースの議論が重視されるようになってきていると思う。完全にリスクがない個人情報の利用は考えにくいと思うので、どこまで許容できるリスクなのかを考えながら解釈論や立法論を検討していく必要がある。立法論も含めて考えると、何が個人の権利利益にとって許容できないリスクになるのか／ならないのかという観点から、絶えず個人情報保護法の在り方を見直していく必要があるかと思う。日本の個人情報保護法は形式的、画一的なところがあったが、近年の改正で実質的な価値判断を伴う規定を盛り込む方向に変わってきている。企業による個人情報の取扱いが違法になるかは、形式的に条文に照らして判断できることが多かったが、今後は何が不当な行為を助長、誘発するのか、個人情報保護法の目的に照らして何が個人の権利利益にとってネガティブな影響をもたらすのかを、より実

質的に判断しなければならないことが増えていくように思う。

**【松浦主任】**

今までは形式的な部分で制限をかけてきたが、今後はより実質的な面も見られていくということだが、例えば形式的な面で正しい手続きを踏まずに取得した個人情報、実質的には誰の権利も侵害していなかったような場合は、どういった考え方になるか。

**【成原委員】**

法律の世界の一般的な考え方で、例えば刑法でも違法性阻却事由があり、形式上は法律に違反する犯罪に当たるような行為でも、正当防衛や緊急避難に当たる場合には違法性が阻却されて罰せられない。個人情報保護法においても、そういった考え方が成り立つ余地というのはあり得ると思う。難しいのは、個人情報保護法は何か具体的な権利侵害や不利益が生じる手前で、それが生じないようリスクの段階で予防するために、個人情報を広く保護しているという面がある。特に技術発展に伴って、そういったリスクが顕在化していくこともあるので、個人情報の利用が個人情報保護法に形式上違反していたが実質的にはリスクがないと事前に判断できるかという点、なかなか難しいと思う。何らかのリスクへの懸念が顕在化した場合には、仮に個人情報保護委員会が指導したり処分しなかったとしても、レピュテーションリスクの問題とも繋がるが、おそらくSNS等で専門家や一般市民から批判を受けたりして結局はサービスを停止せざるを得なくなる可能性もある。形式的には個人情報保護法に違反しているように見えるかもしれないが、実質的には法の趣旨に照らしてみると違法ではないということ、よほどしっかりした理屈で言うことができ、社会に対して説明できる自信があるならば、そういったことに挑戦してみる価値はあり得ると思うが、そのロジックが十分に説得力のあるものだと言えないのであれば、慎重に対応していく必要があると思う。実務家である三部先生にもご意見をお伺いしたい。

**【三部委員】**

実質的にリスクはないことを問題提起したいということであれば、理論武装した上で個人情報保護委員会に事前に相談・交渉する方法はある。受け入れられないケースもあるだろうが、選択肢としてはあり得る。

**【松浦主任】**

個人情報保護法を無視してやるということはないと思うが、議論の中でいろいろと気になった点があったので質問させていただいた。ありがとうございました。

**【森川座長】**

ありがとうございます。今村さんどうぞ。

**【今村課長代理】**

法律ではなく倫理まで語られるところに強い新鮮さと違和感があった。技術的に何でもできるようになって未知の世界に入り込む中で、誰かを知らない間に傷つけているかもしれないリスクがあることに気づくのが倫理の本質かと思う。新しい道德観という話で、教育が必要になるし、実際にそのデータを扱う我々自身が、非常に切迫した強い倫理観を持っていないと容易に踏み外すように思う。

リスクを認識してヘッジする具体的で実行可能な方法は何かを十分語る必要があると思っている。2つ必要なことがあると思っていて、1つは誰かが最初にやってくれるのを待ってその後に追随することが考えられるが、ビジネスをする上ではそうはいかないので、何とかクリアしないといけない。もう1つは、従業員に対して高い倫理観を持ってもらうために、倫理や道德の教育、あるいは我々で新しい人事をつくるという責任感を持って取り組むべきと思うが、2つとも未知の部分が多い。何か海外の先行事例があったらぜひ教えていただきたい。

**【成原委員】**

倫理においては、教育、企業であれば研修などが大事になってくると思う。倫理の場合には、社会の中でこういったことが倫理として求められている、期待されているというのは、六法などに明確に書かれているわけではなく、文化や地域、国、個人、さらには時代によっても変わってくるので捉え難いところがある。1つ視点として大事なものは、「自分が知らない間に人を傷つけているかもしれない」ことを意識しながらビジネスをするという視点、もう少し抽象化すれば、他者を個人として尊重することが基本的な姿勢として大事になってくるのではないかと思う。新卒向け就職情報サイトによる内定辞退率の提供事件は法令違反以前の問題として、学生のデータを分析して内定辞退の確率を算出して、学生に説明



せずに企業に販売することを就活生や世の中に公言して理解を得られると思いますかということ。法令に違反しているかどうか、コンプライアンスの観点から大事だが、それ以前の問題として、あるいはそれと並行して、自分がお客様の立場だったら、こういったことが密かに行われていたらどう思うかという視点に立つというのが大事なのかと思う。

**【今村課長代理】**

レピュテーション、あるいは、時流みたいなところもありそうで、今までの価値観であれば問題なかったが、今の若い人たちから見るとそうは映らないことがある。そういった価値観を掛け合わせる、あらゆる価値観から物事を見ることが大切なのだと思う。ありがとうございます。

**【森川座長】**

ありがとうございます。佐藤さんから手が上がりました。お願いします。

**【佐藤課長】**

先ほどの成原先生のお話で、AIによる差別をきっかけにして、可視化された従来のビジネスにおける差別的な行動やバイアスを見直して、より人権を尊重した公平なビジネスや社会の在り方を模索していく必要があるというのは、確かにそのとおりに思った。そういった中で私たちのような会社は、今まで以上により高い倫理観が求められる状況にあるというのを痛感した。

一方で倫理は法律ではなく道徳的なものであり、多様な価値観の中で企業として自主行動基準を作っていくようなときには、社会の考え方への対応など、どこまでやるべきか。人を個人として尊重したときに、これをやったときにどうするか、個別のところは非常に納得感があって理解できたが、一方でその考え方は、社会の考え方によって左右されることもあるように思われ、そういった中で企業の自主行動基準は、都度アップデートしていくものなのか、それともみだりに変えるものではなく大きな考え方でやっていくものなのか、その辺りのニュアンスをお伺いしたい。

**【成原委員】**

とても大事な質問である。まさに何が倫理かは、その社会の人々の意識に左右されるので、

世の中の人たちの意識を参照してお客様の立場に立って考えるのが大事であるが、人や文化、時代、社会によって価値観が違うので、どの価値観を参照したら良いのかが問われると思う。これは非常に難しい問題で、答えは1つに決まっていないと思うが、1つ言えるのは社内で多様な視点、例えば社内で自主規制や行動規範をつくる際に、できるだけダイバーシティを確保して議論することが大事になってくると思う。女性と男性の比率をできるだけ近づけて、いろいろな視点を入れるようにする、あるいは外国出身の方や障害を持っている方にも入ってもらう。仮に社内でそういった方の声を十分に確保できないのであれば、社外から有識者や当事者の方に入ってもらったり、ヒアリングすることが大事になる。AIのアルゴリズム設計による差別のリスクも指摘されていて、プログラム自体のバイアスによりシステムが差別をしてしまうことも考えられる。例えばニューヨーク大学のAI倫理の研究機関のレポートでは、意図せざる差別ということで、AI開発企業のエンジニアが男性だけで構成されている場合、女性の視点が欠けてしまい、無意識のうちに女性にとって不利なアルゴリズムの設計をしてしまう可能性もあるので、AI開発者の中でダイバーシティを確保すべきと言われている。EUの「信頼に値するAIのためのガイドライン」でも、開発者のダイバーシティが大事と言われている。AIに関するコードオブコンダクトや社内基準をつくる際にもダイバーシティを意識するということが大事になっている。

【佐藤課長】      ありがとうございます。

【森川座長】      ありがとうございました。奈良先生、お願いします。

【奈良委員】

AIによる差別について、成原先生のご講演にあった3つの原因を解決する手がかりとして、システムを提供する社内にダイバーシティを確保することが手がかりになり得るかをお伺いしたかったが、外国でそういった研究結果が示されていることで明確になった。過去に銀行で融資の担当をしていた時に、若い独身女性の住宅ローンの申し込みに対して上司は返せなくなるのではないかと指摘してきたが、担当者としてのその方の話しを聞いた上で見立てを説明して融資に繋がったことがあった。AIのシステムをデザインするのも人間であるし、そのAIのアウトプットを最終的に判断するのも人間なので、デザインと運用の場面で如何にしていろいろな状況や価値観を理解できるか、そのためにダイバーシティを確

保するのが有効かどうかをお伺いしようと思っていたが、そのとおりのお答えをいただいた。ダイバーシティの確保は、それ自体が企業価値を高めると言われているが、ダイバーシティを確保するきっかけがAIのリスクを下げるということであったとしてもアピールされたら良いと思う。

#### 【成原委員】

おっしゃった銀行のエピソードは大変に重要で示唆があると思う。先ほど講演の冒頭でも申し上げたように、人間が審査した場合でも偏見や差別が生じ得るが、奈良先生のエピソードは、人間がそのような偏見や差別を解消し、公平なビジネスを実現することができるということも示していると思う。

これまでに様々なAIが差別をしたということで炎上騒ぎになっているが、これもAIが悪いというよりは、これまでの人間の社会が、どうしても女性を差別してしまっていたり、マイノリティの人たちを差別してしまったりするような慣行を積み重ねてきたからこそ、従来のデータから学習したAIが差別をしてしまっているのです、まさにそうした旧来の社会やビジネスの在り方を見直すきっかけを、AIが与えてくれているのではないかと考えている。

#### 【奈良委員】

ありがとうございます。

もう1点、プライバシーのガバナンスについて、自主規制をしてガバナンスを構築していくことは、三部先生もおっしゃっていたとおりで、私も大いにそのとおりで思っている。

#### 【森川座長】

ありがとうございました。

まず、成原先生のお話を伺っていて法と倫理との間の線引きについて考えていた。倫理で嘘をついてはいけないというが、例えばポーカーのようなゲームをするときは嘘をついても問題ない。「嘘をついてはいけない」というルールがある社会はこのルールがない社会よりも優れていることは明らかであるが、ゲームでは何故、大きな問題にはなっていないのかといったことを考えてお話しをお伺いしていた。もう1つ考えていたのが、憲法・判例のところでの第21条の通信の秘密で、長い間議論が続いていたが、個人情報等が出てきたことによって少し解釈が変わる可能性があるのかどうかという点。解釈が変わっていく可能

性があるのか考えながら聞かせていただいた。

最後にNTTデータへのお願いが2つある。まず、今日は知財室と情報セキュリティ推進室からも御説明いただいたが、NTTデータは政府、業界、顧客、社会全体が大きな期待を抱いている会社だと思っているので、ぜひ模範を見せていただきたい。経産省がガイドラインをつくっているが、経産省でできるのだから、NTTデータでもできるはずで、ぜひ主導していただきたいと思っている。2つ目は、最後のところであった多様性の議論について、男性・女性の中でもいろいろなタイプがいてそれも多様性になるので、性別だけでなく、タイプというところまで踏み込んでいただいて多様性の確保をお願いしたいと思う。ありがとうございました。

#### (7) クロージング・写真撮影

最後に出席者全員でカメラをオンにして写真撮影が行われた。

— 了 —