

AIアドバイザーリーボード勉強会（第1回） 議事抄録

日時：令和3年7月19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）：総務部総務担当 三瀬課長、Data & Intelligence事業部ソリューション担当 今村課長代理、品質保証部企画担当 中野課長、事業戦略室調査企画部調査担当 奥村課長、技術開発本部 鈴木シニアエキスパート

プログラム

時刻	アジェンダ	時間	発表者
16:00 - 16:05	趣旨説明、本日のプログラム	5分	技術開発本部 鈴木
16:05 - 16:10	座長より開会のご挨拶、出席者の自己紹介	5分	東京大学 森川博之 先生
16:10 - 16:50	講演 AIビジネス・スマートシティビジネスのリスクマネジメントー欧米の法・倫理の動向と日本の現況	40分	三部裕幸 先生 ・ 渥美坂井法律事務所・外国法共同事業 パートナー弁護士 ・ 大阪大学社会技術共創研究センター 招聘教授
16:50 - 17:05	NTTデータのガバナンスとプロジェクトガバナンスの紹介	15分	総務部総務担当 三瀬 品質保証部企画担当 中野
17:05 - 17:15	NTTデータのデータガバナンスの紹介	10分	Data&Intelligence事業部 今村
17:15 - 17:55	質疑応答・意見交換	40分	ファシリテーター： 東京大学 森川博之 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アドバイザーリ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、および、所属部署から聴講参加者の紹介が行われた。

(3) 講演：AIビジネス・スマートシティビジネスのリスクマネジメント——欧米の法・倫理の動向と日本の現況

専門委員である三部先生から「AIビジネス・スマートシティビジネスのリスクマネジメント——欧米の法・倫理の動向と日本の現況」と題して、講演をいただいた。

最初にAIビジネスのポイントに関する解説が行われた。AIの特徴として、帰納的であり結果の予測が難しいこと、人間の判断能力を超えることもできるようになったこと、それでいながら人類の歴史や価値観は学習・理解できないことがある。そのため、AIは現行法が想定していないことや現行法の背景をなす価値観に合わないことを起こすことがある。このことを念頭に置いて、次の3つのポイントに基づいて考えていく必要があるとのことだった。

A. 「米欧の新たなルール・法律づくりの動きに対応する」

EUは今年の4月にリスクベース・アプローチに基づいた本格的なAI規則案を公開した。その違反にはEU域外の企業であっても巨額の制裁金が課されるおそれがある。また、アメリカも2019年頃からAIを国防に関わるものと位置付けて様々なAI政策を推進してきた。さらに、バイデン政権成立後、バイデン大統領がAIのルールが必要だと明言するなどしてその動きが加速されており、AIの法制度づくりに向けてEUとも協調姿勢を取りつつある。

これに対して、日本ではまだAIの法制度づくりの動きは見られないが、コーポレートガバナンスやJ-SOXなど欧米に追随してできた法律・規定は多々あり、遅かれ早かれAI法制についても欧米に追随しての法制化が見込まれるとの説明を受けた。AIを使ったビジネスをするのであれば、欧米のAI法制度づくりの動向を把握して備えておく必要がある。

B. 「現行の規制対策をする(遵守する、技術的に回避する、または規制緩和を求める)」

AI商品・サービスを提供する場合、その企画の時点から、関わる法律が何か、その法律に抵触しないかを調べた上で、抵触しそうな法律の対策(守るか、技術的に回避するか、規制緩和を求める)を打つ必要がある。それを怠ると、開始したビジネスがすぐに止まってしまうこともあることが指摘された。

実際、英国サウスウェールズ警察が採用した犯罪防止のための顔認証システムが裁判で違法とされ利用停止になったケースが紹介された。また、国立国際臨床医療研

究センターがAIを使って開発した「糖尿病リスク予想ツール」が、医療機器の法律に違反するおそれがあると指摘されて、同センターのホームページでの公開後わずか1日で停止（2か月後に再開）されたケースなども紹介された。国の機関でもこうしたことが起きたので、民間でも十分な注意が必要である。

C. 「ステークホルダーを意識する」

AIを利用したビジネスの場合、ステークホルダーが広がりがちである。そして、良い技術だからといって常に全ての関係者から受け入れられるとは限らない。

日本ではリクナビ事例が多くのステークホルダー（株主、監督官庁、学生・大学、マスコミなど）の利害に影響したため、個人情報保護法違反に加え職業安定法違反を理由とした行政処分も下り、他の法律との関係でも論点が生じた。また、業界団体、自治体、地方議会の議員などから受け入れられず、AIビジネスがストップしたり開始できなかつたりした事例も起きている。誰がステークホルダーとなり、どういう局面でどういうステークホルダーにどのように使うのかがポイントになる。

次に、AIに関する最新の技術として、連合学習について利用における法律面の注意点の解説があった。連合学習は、個人情報を誰かに開示することなく、各社がAIの学習済みモデルだけを統合することによって、その成果を各社が利用できるようにする技術である。連合学習についてはいくつかの法的論点があり、たとえば、統合した学習済みモデルが個人情報に該当するのかが論点になっている。イギリスの個人情報保護当局や欧州の著名な技術系研究機関の見解（学習済みモデルが個人情報に該当する場合があるとする）、そして日本の個人情報保護委員会も「特定の個人との対応関係が排斥されている」と言えなければ個人情報に当たらないとは限らないという見解を本年（2021年）6月末に示したことが紹介された。連合学習を使えば安心ということではなく、確実に個人との対応関係が切れているかどうかを、ケース・バイ・ケースで検討する必要がある。

最後に、企業におけるAIガバナンス推進体制に関して、三部先生の企業への助言経験や総務省の委員としての海外調査などをもとにした提案があった。既存組織を利用し時間と人手をかけないAIガバナンスと、そのためのリテラシ教育の重要性が述べられた。

（4）講演：NTTデータのガバナンスとプロジェクトガバナンスの紹介

NTTデータの三瀬課長からNTTデータのコーポレートガバナンス体制について紹介が行われた。続いて中野課長から、所属の品質保証部の業務内容の紹介の後に、NTTデータの情報

システム開発におけるプロジェクトリスクマネジメント体制について、コーポレートガバナンス体制との関係と共に説明があった。

【補足】紹介に使われた図はサステナビリティレポートの「Governance編」にも掲載されている (<https://www.nttdata.com/jp/ja/sustainability/report/>)

(5) 講演：NTTデータのデータガバナンスの紹介

NTTデータの今村課長代理から「NTTデータのデータガバナンスの紹介」と題して所属のData&Intelligence事業部におけるAIやデータ活用ビジネスの紹介、および、DMBOK (Data Management Body of Knowledge) に基づいたお客様に向けたデータガバナンスサービスの紹介が行われた。

(6) 質疑応答・意見交換

座長の森川先生のリモートにより、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。

【森川座長】

AI利用における制度的なことを検討するにあたり、自動運転や医療、ヘルスケアなど人間が関わるところは重くなる。例えば、製造業での異常検知といったものであれば、そこまでは重くならないといった考え方で良いのか。

【三部委員】

製造業だから制度の検討が不要、とはならない。単に工場内での異常検知をするAIが法的に問題ないことが多いのはそのとおりだが、「製造業」全般についての法律は多い。あくまで一例だが、たとえば、鉄道や公共施設のインフラに関係するAIとなると、鉄道会社や施設関係者が守るべき法律があるので、そのインフラに関わるAIを開発・利活用する際には注意が必要だ。その意味で、現行法を検討するプロセスを設けることが大切になる。

【森川座長】

AIでステークホルダーが増えるというご指摘をいただいたが、その理由を考えると、AIに対するある種の「気持ち悪さ」に起因するのではないか。ご紹介いただいたAI利用によ

る問題事例は、それまではAIを使っていなくても似たようなことをアナログや表計算ソフトで人がやっていたかもしれず、それがAI利用になって問題が大きくなったのであれば、「説明可能なAI」が出来ることで軽減されていくのではないかと考えるが、先生のお考えをお伺いしたい。

【三部委員】

「AIでステークホルダーが増える」原因は、AIが「気持ち悪い」からではない。「AIでステークホルダーが増える」のは、人間にできないことがAIにできるがために、法律に違反したり法律で守られた権利を損なったりする場合があるからだ。リクナビ事例では、人間にはできない精度の高いサービスをAIが実現した。だからこそ、学生が法律上持っている権利を侵害し、また、他の法律にも違反して監督官庁や大学、株主なども深い利害を持つようになった。

このような事態を「説明可能なAI」で軽減できるかということ、できる場合もあるかもしれないが、そうではないケースが多い。リクナビ事例では、個人の辞退率データを第三者に提供するビジネスを認めてよいかどうかの社会合意がない。また、先程述べたとおり多くの法的問題もある。したがって、AIを「説明可能」であれば問題を解決できるわけではなく、個別事例ごとに、社会受容性や法的問題の検討が必須となる。

なお、よくある誤解として、「何故、AIだけを特別扱いするのか」というものがある。しかし、実際は逆で、法律はAIを特別扱い「できない」。すなわち、法律は何にでも平等に適用されるため、AIにも適用されるが、その法律はAIを想定していないので、AIビジネスが違法になるケースやうまく進められないケースが生じる。だからこそ、「遵守する、技術的に回避する、または規制緩和を求める」という対策を、AIビジネスの企画段階から取る必要がある。さもなくば、ビジネス後戻りのリスクを抱えることになる。

【鈴木シニアエキスパート】

EUのAI法案のスケジュールの見通しをどのようにお考えか、お伺いしたい。メディアの報道ではGDPRと同様に4年ぐらいは法案の審議にかかるのではないかとあったが、世の中の動向からすると、もっと早く進むのではないかとという雰囲気も感じる。実際、どのようになりそうか。

【三部委員】

EUのAI規則案について、EUは、次のとおり法制化することを目指している。

- ・ 2022年後半には、AI規則案が法制化されて効力を生じるシナリオがあり得る
- ・ 法制化されると、事業者向けに施行するための移行期間に入り、その期間で具体的な基準が作られる
- ・ そして、最速で2024年後半に事業者向けに完全施行される

このように、2022年後半にはEUのAIビジネスにおいて、確定したAI規則の影響が生じる可能性がある。その中で、AIビジネスが今回のAI規則案やその基礎をなすEUの価値観・方向性に反すると、AIビジネスが後戻りするリスクがある。したがって、そうならないように、今からAIビジネスを構築・検討し、AIビジネスの中に先取りしておくことが肝要だ。AIの価値観・方向性は明確なので、先取りすることは困難ではない。

【奈良委員】

三部先生にお伺いしたいことが2点ある。1つ目はAIガバナンスを構築するにあたって、最初の準備段階で社内原則を作ることを挙げておられたが、どれくらいのものであればいいのか。今日のお話しの中でOMB通達の10原則を紹介されていたが、こういったものを出すべきなのか、それとも何か企業に特化した原則が必要なのか。もう1つはAIガバナンス体制について先生からご紹介いただいた案と本日のNTTデータさんから紹介があったガバナンス体制の親和性をどうお考えなのか、少しアレンジすれば出来そうなものなのかどうか。

【三部委員】

1点目の社内原則については、既に当社はAI指針を定めているので、この具体化をどのように進めるかが課題になる。これはOMB通達の10原則の内容で済むことではない。

もう1点の体制については、本日ご紹介いただいた当社の体制と親和的になるように検討する必要がある。これまでに担当した顧客企業では、私が提案したAIガバナンス体制を採用して頂いており、とてもうまくいっている。うまくいっている理由は、スペシャルな体制を目指さないからだ。できるだけ簡潔で単純な体制を構築すれば、ほぼ全て、その中に包含できる。当社でも、既存の体制と適合するように構築できると確信している。

【成原委員】

1点だけAIを利用する主体とリスクの関係についてお伺いしたい。

ご講演の中で紹介いただいたとおり、EUのAI規制案では、例えば顔認証技術について、法執行機関による顔認証技術の利用は許容されないリスクということで原則禁止されているのに対して、民間部門については禁止ではないものの高リスクということで厳格な規制が課されている。このことは、同じAI技術でも利用する主体によってリスクが異なるという示唆なのではないかと思う。

また、顔認識技術について、アメリカでは昨年のブラック・ライブズ・マター運動がきっかけに主要企業が顔認証技術の警察等への提供を停止することを公表して反響があったのに対し、日本は顔認証技術に強みを持つ大手企業が提供を続けている。このことは人権意識がアメリカ企業の方が進んでいて、日本の企業は遅れているという見方もできるかもしれないが、別の視点からはアメリカでは顔認証技術で現実に黒人などマイノリティーに対する差別が生じる恐れが高いのに対して、日本で顔認証技術により人種差別が生じる恐れがアメリカと同じくらいあるのかといえば疑問の余地もあり、国ごとの文化や社会状況の相違を踏まえた対応の違いとも理解することができるのではないかと思う。

これらの話からも、同じAI技術でも、誰が利用するのか、NTTデータさんの立場から見ると、誰に納入するのかによってリスク評価の在り方が変わってくる側面があると思う。その辺りについて、三部先生はどのようにお考えになっているのか。NTTデータさんとしても、納入先が公的機関なのか民間企業なのか、あるいは、どの国の企業だったりするのかによって、リスク評価やリスク管理の在り方を変えていらっしゃるのかお伺いしたい。

【三部委員】

おっしゃるとおりである。講演中に述べたとおり、誰がステークホルダーとなり、どういう局面でどういうステークホルダーにどのように使うのかがポイントになる。それによって、検討すべき論点や対策が全く異なってくるからだ。

この点について補足すると、「主体」のみならず、AIの影響を受ける者の違いも重要だ。リクナビ事例に限られず既に事例が生まれている。例えば、AIを活用したライドシェアひとつとっても、AIの利活用でタクシー利用が効率化されている地域では受け入れられやすい場合がある。しかし、観光地近くでライドシェア構想を実現しようとしたある事例では、タクシー業界から猛反発を受けて構想が撤回に追い込まれている。同じタクシー業界でも、

利害関係の違いによって反応が正反対になることがわかる。

AIビジネスを企画する際には、このような事実関係の違い、そしてそれがどのような論点の違いとなって現れるか、を検討するプロセスを設けることが大切だ。

【二科課長（品質保証部）：オンライン参加】

先生方がおっしゃられたとおりで、お客様や当社にとって経験がない業務領域に対して開発する場合のチェックは、今のプロジェクトガバナンスのシステム開発リスクのところでも色々やっている。AIのような新しい技術を採用し開発する場合についても、アドオンし、アジャストしていくようなイメージになるのではないかと考えている。

【石川委員】

今日のお話からすると、何でもしないとイケないくらいの大きな話だと思うが、実際に一步一步進めていくには、組織や意思決定から入っていく話もあるし、技術で足元を固めていく話もあると思うが、それはおそらくNTTデータさんが定型的なビジネスでこういった役割を持っているか次第になるのではないかと。

今日の三部先生のお話は、ベースの意思決定やリスク分析の話だったが、一方で、最初に出てきたものは結構、技術寄りの話だったので、NTTデータさんとしてのタイムライン、スケジュール感とか、例えば目の前にある話として、この半年で何をまとめるかというのは、何か議論されていたりするのかな。

【鈴木シニアエキスパート】

今年度は最初の年であり、4月のキックオフでいただいたコメントを受けて、私たちもリスクベース・アプローチで、既存のプロジェクトマネジメント体制に、AIリスクを管理していく仕組みを入れていくという考え方は、委員の先生方との打ち合わせでお話ししたとおりで、本日出席の社内の関係各所の皆さんにも同様の話をしている。

明確なスケジュール感は宣言しづらいところはあるが、来年の4月にはAIアドバイザーボードの総会があるので、そこで今年度の検討の成果を披露できるように仕上げていくのが、実際にこのAIガバナンスの取組みを推進している部署としての役割と考えている。

【三瀬課長】

GDPRが先例として何回か出てきたが、GDPRはヨーロッパがGAFANAなどにビジネスを侵食されていく中で、産業を守ろうという側面もあったと理解している。今回のAI法案に関して、いわゆる民主主義国家の中で、ここが進んでいるから自分のところをガードしないとイケないといった目線も含まれているのか、それとも最近の世界情勢において、民主主義国家vs権威主義国家みたいな形になっているので、今回は民主主義国家側が割と一丸となって取り組んでいこうということなのか。そのあたりの背景をお伺いできると、我々としても、これをどう捉えるかのヒントになるのでお願いしたい。

【三部委員】

ご質問にお答えする前に、GDPRに関して若干述べておきたい。

- GDPRの原型となるルールは、既に1990年代にEU法（データ保護指令）として制定され、それ以前も欧州の条約やEU加盟国法として存在していた。それは、歴史的背景、すなわちナチスによる個人情報管理がユダヤ人迫害の手段となったことなどへの反省によるものだ。GDPRはGAFANA対策のために突然できた法律ではない。
- GDPRが法制化されたのは、個人情報保護の重要性が高まったことに加え、データをEU域内で自由に使えるようにするためのEU統一ルールが必要だったからである。
- 統一ルールが求められているのは、実は米国でも同様である。事実、米国テック大手企業に、統一的な連邦法である個人情報保護法を切望する動きがある。それは、州ごとに個人情報保護法が異なるとビジネスがしづらいことが一因だ。

このようなGDPRと比べると、EUのAI規則案の背景には、GDPRと共通する面もあるが、異なる面もあるとわかる。

- 共通する面は、歴史的背景を持つ点である。EUでは、AIの倫理を大切にしなければならないという意識が強い。それは、AIの「倫理」が道徳ではなく、人間中心・プライバシー・公平性・透明性・安全性・アカウントビリティなどといった、EUの条約やEU加盟国の憲法・法律に現れている価値観だからだ。そして、その価値観は、長い歴史的背景を持っている。EUは、今回突然規則案を作ったのではなく、長い間大切にしてきた価値観をベースにEU統一ルールを作ろうとしたに過ぎない。
- 異なるのは、最近の国家体制の違いがもう一つの背景になっている点である。EUが大切にしてきた価値観は、米国や日本の憲法・法律でも共通して大切にされている。

そして、米国とEUが協調する動きを取っているのは間違いなく、これらの価値観を尊重する国々と、その価値観が尊重されない国家体制の国が対立軸にある。そのことが今回のAI規則案の背景になっているとみられる。ただ、対抗する陣営が特定の国に留まるのか、もう少し広い範囲になるのかは、今後見極めが必要である。

【三瀬課長】

弊社は今年度が中期経営計画の最終年度であり、次期中期経営計画策定に向けた動きもあるが、今後の更なる成長のためには、グローバルをどんどん拡大していくのは避けて通れず、その中でAIは重要なツールの1つになると考えているので、そのような動きも非常に重要だと考えていた。引き続き御指導いただければありがたいと思う。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 —