Ⅰ－２－２　講演会　AI 法規制のない日本で必要となる企業の自主的対策 ---4 つのリスクと海外の現状を踏まえて何をすべきか

講師：渥美坂井法律事務所・外国法共同事業　パートナー弁護士
大阪大学招聘教授（社会技術共創研究センター）
三部　裕幸

開催日　：2024 年 4 月 4 日
開催場所　：JBMIA 会議室（第 1、第 2 会議室）＋Zoom 開催
参加者　：75 名
記　：坂津 務*

１．はじめに

2024 年 3 月 6 日に開催された第 1 回目の講演では、欧州・アメリカ・中国の AI 法規制動向が講演内容であった。第 2 回目となる今回は、第 1 回目に解説していただいた国際情勢を踏まえた上で、AI に携わる企業が生き残るための 4 つのリスク対応策についてお話しいただいた。（第 1 回目の講演の内容については、Ⅰ―２―１を参照のこと。）

２．講演内容

2.1. 明確に後れを取った日本の現状

第 1 回目の講演のおさらいとして、欧州・アメリカ・中国の AI 法規制動向に対して明確に後れを取った日本の現状を確認しておく。アメリカ、中国の AI 関連投資規模を考えると生成 AI の基本開発に巨額投資するのは現実的ではない。日本独自の AI の勝ち筋を見出し、そこに資源を集中することが大切である。また、アメリカや EU は国民・国家・企業を守るため 2019 年から法制化を検討してきた。日本は一部の AI 開発者の心情に引きずられ、規制化されるとよくないという先入観があったので、ガイドラインや業界団体ルールなど法的強制力のないソフトローの方向に向かった。そのため、AI 法規制の点で西側諸国と比べて日本は大きく出遅れる事となってしまった。

2.2. AI 法規制のない日本における 4 つのリスク

ソフトロー偏重の独自路線をとった日本では以下の 4 つのリスクが生じる。

- 悪意あるものから攻撃を受けるリスク
- 何が許され許されないかの羅針盤がないリスク
- 現行法が障害となるリスク
- 海外との関連でのリスク

これらのリスクに見舞われた企業をソフトローは全く守ってくれない。国が本腰をあげるまでに時間がかかると考えられるため、企業は自主防衛策が急務となる。4 つのリスクについて具体的な事例を紹介しながら解説する。

* 技術調査専門委員会委員

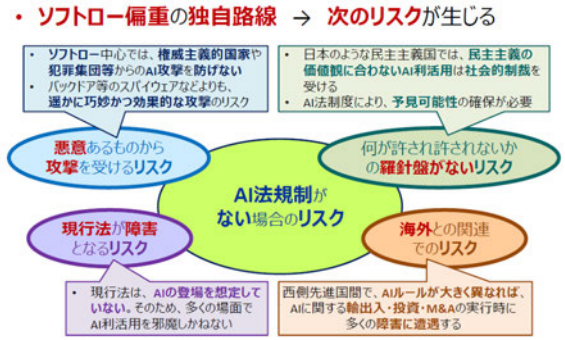

Fig.1 AI 法規制のない日本における 4 つのリスク

2.2.1. 悪意あるものから攻撃を受けるリスク

ソフトロー中心では権威主義的国家や犯罪集団などからの AI 攻撃を防ぐことができない。AI を使った攻撃も防げないし、また AI に対する攻撃も防げない。スパイウェアなどよりもはるかに巧妙かつ効果的な攻撃を受けるリスクがあると考えられている。6 つの事例を挙げるが、アメリカ大統領令ではこれらのリスクに取り組むことを既に命じている。

- 国家や企業の重要な財産・知的財産が盗まれる、消される、操作される
- 絶対に攻撃されてはならない設備にサイバー攻撃を受ける（原発、防衛施設など）
- 危険性の高い兵器が開発され安全保障の脅威となる
- 偽情報の被害が続発する（人権侵害、選挙操作など）
- 詐欺集団による広域的・効率的詐欺が発生する
- バイオセキュリティを侵害する（生物テロなど）

これらのリスクに対して、日本ではほとんど対策が立っていない。偽情報の被害の一部に対して検討されているだけである。日本のソフトローでは太刀打ちできるわけがない。

2.2.2. 何が許され許されないかの羅針盤がないリスク

法律がないから罰せられることがないかというとそうではない。日本のような民主主義国では民主主義の価値観に合わない AI 利活用は社会的制裁を受ける。そのような事例は国内外で多数発生している。本当は AI の法制度を作った方が何をやってよくて何をやったらだめかという事がはっきりするので、予見可能性を確保することができるが、今のところ日本の中にはそのような法制度がない。AI 法がない中で強く社会的制裁を受けた事例を 3 つ紹介する。

日本のリクナビ事例は記憶に新しい。リクナビは就活生が就職用に使う Web サイトであるが、そこでリクナビ側が取得した就活生の情報をアルゴリズムで分析し、就活生が内定を辞退する確率を算出して就活先企業に提供するサービスを実施した。個人情報保護法に加え労働法にも違反している事案だが、行政指導される以前からマスコミ･SNS･大学などから強く非難され、主な顧客である大学からも締め出され、大株主が株を売り出し、就職先企業にも行政指導が及ぶこととなり迷惑をかけた。その結果業界全体から背を向けられることとなり、大きな損害となってしまった。

カナダのトロントのスマートシティ事例は、Google の子会社が計画したスマートシティで AI を活用したサービスがプライバシー侵害ではないかとメディア・住民が批判した事例である。市民団体が訴訟を提起し、トロント市も疑問を述べる報告書を公表した。市民の反対でスマートシティ計画は頓挫してしまい、大きな損害を負う事となった。

イギリスの英国警察事例は、犯罪予防のために自動顔認証システムを導入し約 50 万の顔画像撮影を実施した事例である。市民活動により提訴され違法と判断された。欧州人権条約やデータ保護法、平等法の違反が理由だが、システムを納入した企業の将来の大きな収益が消えてしまった。AI 法が制定されていれば AI 企業はそれほど損害を受けなかったと思われる。

2.2.3. 現行法が障害となるリスク

今までいろんな事業者を代理してきているが、様々な業域をカバーする法律が存在している。しかしながら、それらの法律は AI の登場を想定していない。そのため多くの場面で AI 利活用を邪魔しかねない。個人情報保護法や知的財産法などは関連する法律として一般的に議論されやすいが、その他にも例えば介護、労

働、健康医療、防災災害対策など、それぞれの分野で現行法がいろいろと関わってくる。

介護施設での AI カメラの事例は、トイレや浴場にカメラやセンサーを設置して、AI によって介護施設の働き方改革や介護される人がどのような状況になったら介護が必要かという事を明確にするという狙いがあった。しかしながら、個人情報保護法だけでなくカメラで撮るという事は高齢者保護の法律に反してしまう。私が担当した事案では、厚生労働省へ確認した後、技術を組み直して問題をクリアすることができた。もし改善しないで運用していたら違法行為となっていた。

そのほか、労働分野における職業安定法、健康医療分野における医師法や薬機法（旧薬事法）、防災災害対策における消防法や災害対策基本法など、例示し切れないほど様々な法律が関わってくるので、それらを含めて対策を考えていく必要がある。

2.2.4. 海外との関連でのリスク

AI 法規制の点で西側諸国と比べて日本は大きく出遅れる事となってしまってガラパゴス化している。そのため、西側先進国と AI ルールが大きく異なり、AI に関する輸出入・投資・M&A の実行時に多くの障害に遭遇する。

2.3. 不祥事が起き危機に進むと企業はどうなる？

様々なタイプの危機管理を担当してきた経験から、不祥事を起こした企業がどういうことになるのかという事を紹介する。

まず、AI 関連で不祥事を起こすと、AI 関連業務だけが止まるだけでなく、様々な対応を迫られるので通常業務がストップする。例えば、まず、マスコミが次々と報道するというのが典型的である。国民への状況説明や記者会見が当然必要になる。被害者がいれば謝罪対応や賠償が必要である。監督官庁が報告を求めたり、指導・命令が出されたりする。株主や顧客・取引先への状況説明や質疑応答が要求される。これらのことに対応しながら、同時並行で事実確認・原因分析、再発防止策の策定、訴訟対応を進めなければいけない。そうすると関連する部門は本来の業務がほとんど止まり、収益が得られなくて非常に大変な状況になるという事が起こる。

それと同時に、資金ショートと資金調達難の悪循環のスパイラルによって経営危機になりやすくなる。評判や信用が悪化すると、売上げが下がるだけでなく、状況説明や謝罪のため営業活動もストップし、更に利益が減って資金ショートをもたらす。一方、株価下落につながると市場で資金調達も難しくなり。こうなると銀行借入もしにくく、株式の発行による資金調達も出来なくなり経営危機になりやすい。大企業でも大きなダメージである。

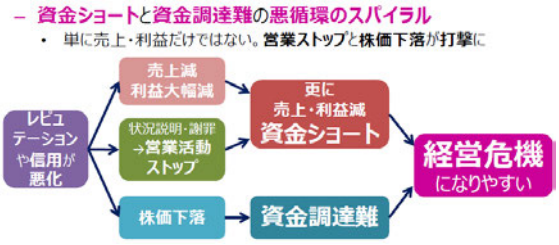

Fig.2 悪循環のスパイラル

役職員が文字通り疲弊するということもダメージが大きい。重労働・重圧が長時間継続し体調やメンタルを崩すケースがある。残業、徹夜、休日長期休暇返上などが常態化しやすいという事も起こる。

AI のケースではないが実例を見ると、通信教育会社の個人情報漏洩事例では、長期間にわたって株価が下落した。漏洩についての記者会見・謝罪の段階で下がった後、いったん持ち直したが、会員数の減少が決算短信で公表されると一気に下落して、3 分の 2 くらいまで落ちた。AI の場合だと国民が敏感なので株価下落の影響が大きく長期間続くであろう。

2.4. 企業の危機管理を行う弁護士としてのアドバイス

不祥事が発生すると損失が極めて大きくなる。弁護士費用だけで 2,000 万円～3,000 万円、ちょっと大きくなると 7,000 万円～8,000 万円はかかる。大きな不祥事の場合長期間の訴訟や巨額の逸失利益に苦しむ。

不祥事の原因ビジネスがストップするだけでなく通常のビジネスも出来なくなる。新人採用もストップするなど規模の縮小も余儀なくされるという事が起こる。

これらのような事態になってしまうことを考えると、不祥事になる前に資源を使う方が圧倒的にコストは安く済む。日本や世界の法律や動向に詳しい弁護士に事前に相談するための費用を用意する方がはるかに安く済む。

取引先・業務提携先・買収先などのリスクも対策が必要である。AI ビジネスはいろんな企業と結びついていかないとできないビジネスなので自社の体制整備だけでは不充分である。納入する大手企業のサービスに不備が見つかり連邦政府がその大手企業を締め出した事例もあった。海外との関係で輸出入・投資・M&A をする場合や国内案件でもリスクの検討が必要である。

2.5. AI に携わる日本企業の自主企業防衛策に向けた提言

AI 法規制の動きが見えない日本で企業が取り組むべきこととして下記 3 つを提言する。

- 事実を踏まえてリスクを分析する

アメリカ・EU・日本の AI 法務に詳しい法律専門家とディスカッションを開始しリスクを分析する。リスク炙り出しのプロセスが重要で多くの会社はこれができていない。

- AI 内部統制体制を確立する

EU の AI 規則やアメリカ大統領令を参考に体制を確立する。コンプライアンスなど既存の社内体制を応用することも可能である。安全保障に関するリスクを押さえながら、アメリカ・EU・日本の AI 法務に詳しい法律専門家との協議が必要である。

- AI に関する輸出入・投資・M&A の観点を掴む

海外とつながりのある企業では輸出入・投資・M&A に対する対策を講じることが重要となる。

2.5.1. 必要となる内部統制の項目

上記の 3 点の提案の中で、2 つ目の内部統制に関して詳しく述べる。EU が AI 法案を可決しているのでまずは EU について対策を立てるというのを優先課題とすればよい。4 つのリスク分類の内、許容できないリスクのある AI の懸念がある場合は早急に対応しないといけないが、その次のリスク順位である、ハイリスクのある AI に対する内部統制の概要として 7 項目が挙げられる。

- リスク管理システム

リスクを特定・分析・評価できるシステムを作り、リスク対策と残るリスクが許容範囲な設計となっているかを判定する。ゼロリスクを目指す必要はない

- データ・データガバナンス

学習用・検証用・試験用データセットについて、管理方法やデータの関連性・代表性・完全性に関して対策をとる

- 技術文書

AI の一般的な説明、開発プロセス、モニタリング・機能・制御・適合性の情報、市販後の評価、など事前に技術文書を作成する

- 記録保持

ログの記録機能を開発し、なにかあった時にトレースできるようにしておく、市販後のモニタリングができるようにしておく。

- 透明性・情報提供

動作の透明性が確保できるように設計する。使用上の指示をユーザーに明確に示すことが重要である。

- 人間による監視

人間が効果的に監視できるように設計することが重要である。

- 正確性、頑健性およびサイバーセキュリティ

適切なロバストネスが達成できているかを明確にする。使用上の指示で正確性の水準を示すことでよい。ゼロリスクにしなければならないという事ではない。一方、データポイズニング・敵対的サンプル・モデルの欠陥に関しては防止・制御しなければならないので対策を立てる必要がある。安全に関する一定の AI は第三者評価を受けないといけないが、それら以外のほとんどのハイリスク AI は自主評価でよいという事になっている。ただその自主評価の基準が欧州委員会か

ら示されることになっているが、今後標準化団体と協議をして基準が制定されることになる。現時点では企業側でできることを考えていく。

以上の 7 項目のほか、AI ビジネスによっては次の 2 項目を検討する必要もある。

- アメリカ大統領令固有の AI リスク

アメリカと関係のあるサービスや安全保障を考えないといけない AI は大統領令を意識する必要がある。

- AI に関する輸出入・投資・M&A のリスク

国内専業の企業でない場合は輸出入・投資・M&A の場合のリスクとして、権威主義的国家との貿易管理上のリスクやデューデリジェンスの困難性に対する対処などを考える必要がある。

2.5.2. AI 内部統制体制づくり

既存のガバナンス体制を利用し、無理なくすすめるのがよい。それぞれの事業本部の方に AI リスク担当を兼務してもらい、その担当の方に責任を負わせるのではなく情報を上げてもらうようにお願いし、情報がガバナンス組織まで上がってくるような仕組みを作る。

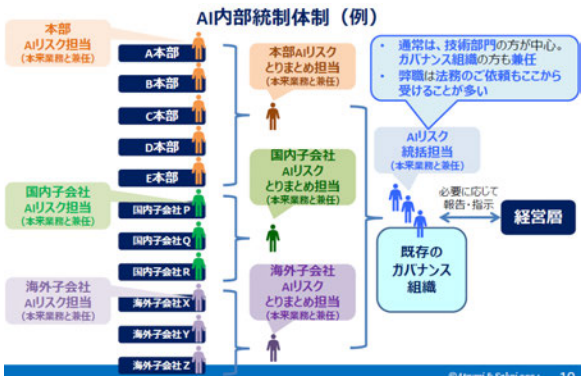

Fig. 3 AI 内部統制体制

ガバナンス組織には AI リスク統括担当を置くが、技術のわかる技術部門の方を中心に、ガバナンスをやっている方や法務の方にも入っていただく。ただし、いずれも本来業務と兼任とし、負担を分担しあうやり方がよい。専門組織を作るとうまくいかない。社内で軋轢を生んで大変なことになってしまうケースが多い。

2.6. まとめ

最後に、申し上げたい事を 3 つにまとめた。

- 日本独自の AI の勝ち筋を見出し、資源を集中

もともと日本が得意としてきた AI 分野・技術を活用しそれを生成 AI の応用開発と組み合わせて価値の創造を目指す。地方創生につなげて日本全域でソリューション創出する構造とする

- AI ガバナンスで西側諸国と歩調を合わせ AI 法規制の導入と現行法の改正を進める

今のままでは羅針盤がないため AI 不祥事が頻発し AI 攻撃を受けやすく輸出・投資・M&A にも支障がある。国民・国家・企業を守るためには 4 つのリスク対策をやらなくてはならない。そのためにも法規制があった方が都合がよい。

- 企業は自主的な AI リスク対策を急げ

国が歩調を合わせるまでの期間は、これまで日本で議論されてきたソフトローでは企業は守れない。日本企業は自らリスク対策を講じる必要がある。アメリカ・EU の内部統制を参考に体制を構築し、EU・アメリカ・中国の AI 法規制に詳しく日本の現行法の障害についても詳しい法律家と協議する事がよい。

最後に、早合点しては危険だという事を申し添える。アメリカ・EU は 2019 年から多くの専門家を動員し長い時間をかけて現在に至っている。日本で AI 法の議論をする方も、AI ビジネスの法務知識が必要な方も少しの情報だけでわかっていると考えるのは危険だ。AI リスク対策は国内外の法律の動き、不祥事事例、その他さまざまな動きをわかっていないとできない。企業が個別に情報収集しようとすると膨大なエネルギーとコストと人員がかかってしまう。私は長年取り組んできた経験や知見を企業の皆様のお役に立てている。是非相談いただきたい。

3．おわりに

全 2 回に分けて講演していただいた。欧州・アメリカ・中国の AI 法規制動向およびそれらに立ち遅れている日本の現状、その国際情勢を踏まえた上で AI に携わる企業が生き残るための 4 つのリスク対応策についてお話を聞くことができた。多面的で幅広い情報収

集とそれらの情報を読み解く洞察力で大局的な関係性や細部の具体的事項の紹介および提案などで大変わかりやすく且つ幅広い観点で解説していただいた。AI 関連のビジネスを推進していくことの大変さを突き付けられた感じだが、取り巻く環境や取り組む方向性などを垣間見ることができたのは貴重な一歩となった。今後、企業が AI リスク対策を検討する際には、専門の弁護士に相談することも選択肢の一つとなる。

AI 法規制に関しては、2023 年後半から急進展を迎えている。ビジネス機器業界も無関係ではいられない状況の中で、世界の動きと日本の対策について今後も注目していく必要があると考えている。

講演会には会員各社の方が多数参加され、講演終了後の質疑応答、講演会前後のディスカッションでも多くの質問や意見があり、講演内容への関心の高さが伺えた。

最後に、三部様にはお忙しい中、時間を割いていただき、分かりやすい講演を行っていただいた。この場を借りて御礼申し上げる。

2023 年度「ビジネス機器関連技術調査報告書」“Ⅰ－２－２”部

発行　2024 年 6 月
一般社団法人 ビジネス機械･情報システム産業協会（JBMIA）
技術委員会 技術調査専門委員会
〒108-0073　東京都港区三田三丁目 4 番 10 号 リーラヒジリザカ 7 階
電話　03-6809-5010（代表） / FAX　03-3451-1770