

AI 利活用に伴う契約時の留意事項の検討 第 1 回検討会 議事要旨

令和 6 年 10 月 30 日 11:00~13:00

オンライン開催

- 本チェックリスト策定の背景・目的を踏まえ、対象とすべきユースケースは適切か？

【委員意見の概要】

- 取引の当事者がどの程度力を持ち交渉しているのか等、ルールセッティングをする側について前提の共通認識を持つべき。
- 利用規約は個別変更が困難なため、チェック後にとり得る行動は少ない。条項を踏まえた利用時の留意ポイント等、利用の際の視点も必要ではないか。
- チェックリストの目的に関して、現時点での一般的な AI サービスの利用規約の状況を想定し、実用性を考慮することは当然。加えて、長い目で見たときに、企業ユーザが安心して営業秘密や個人データの処理を委ねることができる程度の、高い安全水準を実現するサービス水準を示し、それらの基準を積極的に満たそうと意欲して開発する動機を生じさせるという効果の実現も視野に入れるべき。
- 日本国内のみのプレーヤーが受益する AI サービスを開発する場合、オンプレミス型や特化型になる可能性が高いが、想定ユースケースにより議論が変わるため、前提の議論が必要である。
- 個人情報保護法上、AI サービスの利用者が安全性を確認できない限り、個人データを、第三者が管理支配するクラウド型の AI サービスに処理させることはできない。法が求める安全措置を満たすために、日本政府として考える、利用者が確認すべき安全性の基準を提示することで、たとえば現在は安全基準を満たしていないサービスであっても、市場に受け入れられるためにそれらの基準を積極的に満たそうと意欲して開発する動機になり、AI の活用が可能な場面が増え有益ではと考える。
- 個人情報や営業秘密に関して、法律的な観点から、提供先（AI ベンダ）が国内事業者か国外事業者かで議論が異なるのは、個人情報の第三者提供に関する部分のみ。それを除くと、法律的観点から国内外で中立的になるため、AI ベンダが国外事業者であることの論点があるとする、利用者の心情による部分や、当該国の法制度との差異が大きい。法律に明記されていない要素をいかにチェックリストに反映させるかは悩ましいが、挑戦してみる価値はある。
- 厳しいチェックリストを作成すると、アプリケーションの開発提供者(規模が小さい企業が多い)は、大元の基盤モデル提供者と生成 AI サービスユーザの板挟みになってしまうのではと考える。

- 想定使用場面を踏まえて、アウトプットイメージは適切か？

【委員意見の概要】

- チェックリストをすべて満たさない場合の判断のために、若しくは重要なポイントを示すために、チェックリスト内の項目に重みづけをするか。何らかの形で重み付けをするのであれば、重要なポイントを満たすサービスを選ぶように誘導できると考える。

- CLOUD Act を含むようなガバメントアクセスの論点では、重みづけ・強調をすることが重要である。ベンダ側の対応を調査し、反映可能なところは反映するのはどうか。
- 利用企業側では、気に入った AI サービスが既にあり、導入がほぼ決まっている場面が多いと思うので、契約是非を決定するためのものではなく、契約後の利活用場面を見据え、営業秘密や個人データを扱わせて良いか否かといった使い方を判断できるチェックリストにしたほうが、実用的ではないか。たとえば、通常、企業ユーザが入力したデータは、他ユーザと確実に分離がなされ、第三者や AI サービス事業者のための学習利用が決して行なわれないことは当然として、個人データを扱わせる場合は、サイバー攻撃を受けても漏えいしない強固な仕組みの実装と担保が必要だ。そのような事柄が担保されているかを規約を読んで判断できるチェックリストにすべきではないか。
- 利用者が適切に意思決定できるよう、アウトプットは単なる項目の羅列ではなく、チェックする意味や、満たさない場合に留意すべき点などを補足説明することが重要。
- 既存の規約は秘密保持条項を入れずに一般的な使用禁止の条項が入っている場合が多い。AI・データ契約ガイドラインの際の議論内容と表面的に異なると受けられかねない点もあるため、整合性を考えると、1～2 ページのアウトプットは難しいのではないか。
- 仮に条項をチェックしてそれが基準を満たせていないときの対応策が何かしら示すことができれば、ユーザにとって実務上有益なものになると思う。基準を満たしていないときのユーザの行動を示すにあたり、考慮すべき法令および情勢の背景を書く必要がある。
- ベストプラクティスを追求するのか、必ずしも今やられているわけではないが将来的に満たすべきものを書くべきか判断が必要。

○ 全体の検討アプローチについて、違和感はないか？

【委員意見等の概要】

- 今回の検討対象をどこまでにするかを明確化すべき。契約書（利用規約）を読むだけでは確認が難しい要素についても、AI ベンダの選択という観点からはユーザが事前に検討すべき項目はあるが、数が多いため、すべてを網羅することは難しい。今回のチェックリストの利用目的を考慮し、利用規約に表れない項目のうちどこまでのものを含むか、検討する必要がある。セキュリティ要件は含むということであるが、それ以外にも、サーバーの所在地や、学習用データセット、著作権侵害の担保等も、本来であればサービスを選定する際には確認すべき事項である。また、実際に使用されている利用規約について検討対象とするかについて議論必要。
 - 契約履行されないリスクの担保等セキュリティ要件は、主な問題意識の「適切な対価が得られるか・想定外の不利益を被らないか」の 2 点に焦点を当て、関連するところを中心に検討したい。（事務局）
 - あくまで利用者が提供又はプロンプト入力するデータに関連するものに限定するということでした。
- コスト次第だが、実際の利用規約を分析する作業ができるとよい。類似研究が少ないため、実際の利用規約を分析し、どのような条項が多いかや傾向を把握することが有益である。

○ 論点・議論の全体像は適切か？

【委員意見の概要】

- 契約に関して、契約チェックリストで対応すべきものと独禁法を視野に入れるべきものがあるのではと思う。
- 個人情報保護法に関する部分はチェックリストのかなり重要な部分を占めるのではと思う。

以上