

取りまとめに向けた検討（２・情報セキュリティ等関係）

A I モデルの選択等（裁判所業務関係）

【短期的展望に関する論点・第２の２(3)ア、オ関係】

１ 裁判所が独自の A I モデルを開発することについて

裁判所が独自の A I モデルの開発に着手することは、後記 2 のとおり、想定ユースケースにおいては、汎用の A I モデルの性能で対応できると考えられる上、事前学習から独自で行うことのみならず、独自の追加学習をさせることも含め、裁判所において要件定義等を行う必要があり、これらに要する費用や人材の確保等の観点から踏まえると、少なくとも現時点においては現実的ではないということで、良いか。

２ A I モデルの選択に当たって考慮すべき事情について

まず、A I モデルを選択するに当たっては、裁判所における利用目的や用途に照らして、当該 A I モデルが必要な性能を満たしていることが大前提となる。ところ、想定ユースケースとして挙げられている争点整理の補助といったものであれば、大手外国企業が開発した A I モデルは必要な性能を満たしていると考えられる。これに加え、国内企業が開発した A I モデルはこれらよりもやや性能が劣る部分があると考えられるものの、プロンプトの設定が出力の精度に大きな影響を与える面がある上、性能は日々進化しており、将来の裁判所における導入時点においては十分な性能を有していることも考えられる。

次に、司法権が国家主権の一部であることや裁判官が外部から不当な影響を受けずに法と良心に従って職権を行使するという裁判官の職権行使の独立との関係を考慮する必要があると考えられ、これらの点は、究極的には司法権の行使に対する国民の信頼の確保に帰着するから、裁判所における A I の利活用についても国民の信頼が得られるか否かが重要であると考えられる。

また、近時のソブリン A I の考え方（一般的には、A I の開発・学習・運用に必要なデータ、計算資源・インフラ、モデル、人材などを可及的に自国内で調達・管理し、国外への依存を抑制しようとする政策・方針のことをいう。）も考慮する必要があるのではないか、といった意見もあった。これらの観点からは、裁判所において利用する A I モデルが「外国製」であるか「国産」であるかが問題となりうるが、そもそも「外国製」といっても、外国企業が開発したことを意味するのか、機械学習が外国で行われたことを意味するのかなど、様々な観点があり、結局のところ、利用目的や用途との関係で当該 A I モデルを利用することが司法権の行使に対する国民の信頼を揺るがせるものではないといえるかが重要であると考えられる。

この点、争点整理の補助のような想定ユースケースでは、最終的に裁判官が出力

結果を確認することが前提とされていることから、このような場面での利用を念頭に置いて、裁判所が「外国製」A Iモデルを採用することは「外国製」A Iモデルについて指摘されることがあるバイアスの存在といった観点を考慮しても、直ちに我が国の司法権の行使に外国企業が不当な影響を及ぼすおそれがあるとは考えにくいようにも思われる。

さらに、A Iモデルを選択するに当たっては、ベンダーロックイン（特定のベンダーの技術やサービスに依存し、他社への切り替えが困難になる状態をいう。）や開発企業の撤退等によるサービス提供停止といったリスクを考慮する必要があると考えられる。

以上のような観点や政府が検討を進めている国内A Iモデルの利活用の状況を踏まえつつ、裁判所において想定ユースケースにおいて利用するA Iモデルを適切に導入することが期待されるということで、良いか。また、裁判所におけるA Iモデルの選択について、国民の信頼を確保するという観点から、透明性確保のための仕組みやガバナンスを検討する必要があるということで、良いか。

情報セキュリティ・A Iセキュリティ（裁判所業務関係）

【短期的展望に関する論点・第2の2(2)、(3)イ、ウ、エ、(5)ア関係】

1 情報セキュリティ・A Iセキュリティ全般について

裁判所業務において利用されるA Iシステムにおいて求められる情報セキュリティ・A Iセキュリティは、行政事務において求められる情報セキュリティ・A Iセキュリティと大きく異なるところはないと考えられるから、これまでと同様に政府機関等のサイバーセキュリティ対策のための統一基準群に準じた情報セキュリティ対策を講じることが重要であるということで、良いか。

なお、営業機密等が問題となる事案や、被害者の秘匿等が問題となる事案等、一定の場合には生成A Iの利活用を除外すべきではないかという意見もあったところ、どのように考えるか。

2 A Iモデルの配置場所等について

A Iモデルの配置場所として、オンプレミス（システムの稼働やインフラの構築に必要となるサーバ、ネットワーク機器及びソフトウェア等を自社で保有し運用するシステムの利用形態をいう。）は、調達・構築・維持管理のコストや導入期間の長期化等の課題があることを踏まえると、裁判所が管理する日本国内サーバのクラウド上に配置する手法が情報セキュリティの水準や国民の信頼を確保するといった観点からみても総合的に最も妥当ではないかとの意見があったところである。

このような意見も踏まえつつ、裁判所においてその在り方を検討すべきであるということで、良いか。

3 A Iセキュリティ・A Iモデルの公表について

裁判所におけるA I利活用でのA Iセキュリティについては、特にプロンプトインジェクション攻撃、プロンプト窃盗攻撃等のおそれについて留意する必要があるところ、一般的に求められる対策を講じることが重要であり、裁判所独自で対策を講じる必要はないという意見があったところである。このような意見も踏まえつつ、裁判所においてその在り方を検討すべきであるということで、良いか。

また、A Iモデルの公表は、一般には透明性と予測可能性が高まることや今後のA Iモデルの調達における公平性の確保にもつながるメリットがある一方、攻撃者における脆弱性の発見等のおそれ等のデメリットがある旨が指摘されたが、現在広く利用されている汎用の生成A Iに対する攻撃のリスクについては、近時はそのような事例は見当たらず、大きな問題とはならないのではないかと意見があった。

そこで、裁判所における生成A Iの利活用に当たっては、一定の透明性の確保が求められる一方、A Iモデルの公表による弊害が少ないことに照らすと、A Iモデルを公表することが望ましいようにも考えられるが、どうか。

4 生成A Iシステムの調達について

裁判所が利活用するために生成A Iシステムの調達を検討する際には、現在改定作業中の政府ガイドライン（行政の進化と革新のための生成A Iの調達・利活用に係るガイドライン）に準拠した検討が必要であり、かつ、それで足りるということで、良いか。

5 生成A Iシステムの監査について

生成A Iシステムに対する監査としては、一般的なA Iの監査基準は整備されつつあるとの指摘があったものの、個々の事件におけるプロンプトの使用方法について監査することは、当該裁判官の判断過程の評価を伴う可能性があり、裁判官の職権行使の独立との関係で問題が生じることから、裁判所においてはA Iの学習・推論・生成におけるすべての過程の適正性に係る監査証跡を保存してそれに監査（特にリスト型）を実施することで客観的に示すことは困難であるという意見があった。他方で、裁判所において一般的な監査基準によって監査を実施することは相当ではないとしても、裁判官の判断の適正性を担保するという観点からは、裁判所に特化したA Iの情報セキュリティマネジメントを構築し、第三者による定期的な評価を行うことで説明責任を果たすべきではないかと意見もあった。

これらの意見も踏まえ、裁判所においては一般的なA Iの監査基準によって監査を実施することは相当ではないものの、裁判官の判断の適正性を担保するという観点からA Iガバナンスの検討を更に進める必要があると考えられるが、どうか。

6 裁判所において使用するプロンプトについて

【短期的展望に関する論点・第2の3(1)にも関連】

裁判所において使用するプロンプトについては、当該プロンプトを使用した出力

が適正なものであることを担保する手法として、これを公開したり、監査の対象とすることも考えられるところではある。もっとも、個々の事件におけるプロンプトの使用方法を裁判所の外部に公開することにより、担当裁判官の判断過程や方向性が使用するプロンプトから推察される可能性が高まり、裁判官の職権行使への影響が問題となり得ることから、非公開とすることで良いのではないかと、また、前記5のとおり、個々の事件におけるプロンプトの使用方法について監査することは、当該裁判官の判断過程の評価を伴うことになり、裁判官の職権行使の独立との関係で問題が生じうるとの意見があった。

他方で、裁判官が使用しているプロンプトを裁判所内部では相互に共有することによって、A I の出力の精度を上げていくことに活用できるのではないかという意見もあった。さらに、具体的な場面におけるニーズに即したより精度の高い出力を得るには適切なプロンプトチューニング等が必要であるとの指摘もある。

以上のような観点を踏まえつつ、裁判所において使用するプロンプトについて、A I の利活用をより効果的なものとするための方策や裁判所内外での透明性を確保する方策についてどのように考えるか。

7 A I ガバナンスについて

【短期的展望に関する論点・第2の2(5)エにも関連】

「取りまとめに向けた検討(1)」において、想定ユースケースにおけるA I 利活用に伴うリスク・課題への対応策等に関連して、A I ガバナンスも取り上げられたところであるが、第2回分科会においては、裁判所が利用するA I モデルの選択や生成A I システムに対する監査の観点からもA I ガバナンスについて議論が及び、裁判所が利用するA I モデルの選択やA I セキュリティの状況、更には裁判所におけるA I の利活用の状況に対する裁判所による定期的な検証評価の必要性が指摘されたところである。

具体的には、個別の事件におけるA I 利活用の適否は、当該担当裁判官の心証形成の問題として上訴等の訴訟法上の不服申立手続において解決するものとしつつ、裁判所による上記検証評価を実施することで、裁判所のA I 利活用に対する国民の信頼を確保してはどうかとの意見があったが、このような検証評価においては、裁判官の職権行使に対する影響を考慮する必要性も指摘されたところである。

以上を踏まえ、裁判所による定期的な検証評価の実施について、どのように考えるか。仮にこのような検証評価を実施することとした場合、その在り方について、第三者が関与することや検証評価の結果を一定の範囲で公表すること等を含め、どのように考えるか。