

第9回 AI時代における民事司法を考える研究会

日時：令和8年4月24日（金）18:30～21:10

場所：公益社団法人商事法務研究会会議室（オンライン併用）

議事概要

- 3月31日に開催された第2回分科会における議論の概要について報告がされた。

（AIモデルの選択について）

- AIモデルの選択については、AIが急速に進歩しており、AIモデルのバージョンアップに伴う出力精度の揺らぎに対応するためのコストについても検討すべきではないか。
- AIモデルのバージョンアップについては、大手企業がクラウド上で提供するAIモデルを利用するのか（既存モデル）、AIモデルをダウンロードし、裁判所内部等実行環境を制御できるローカル環境に配置して利用するのか（ローカルモデル）でそのリスク等が異なる。既存モデルについては、サービスが停止した場合には、利用ができなくなる可能性がある。他方で、ローカルモデルはそのリスクはなく、一定期間安定した利用ができる。
- 既存モデルについては、複数のサービスを組み合わせて利用することがあり、バージョンアップに伴い、他のサービスとコンフリクトすることが問題となり得る。他方で、ローカルモデルを採用した場合には、メンテナンス費用が過大となる。
- AIモデルの選択（調達）後、AIを運用していく過程で問題が顕在化し得るが、そもそも調達段階で全ての問題を審査するには限界があるため、AI調達後の定期的なチェックや第三者による審査等の制度設計が必要である。

（情報セキュリティ・AIセキュリティについて）

- 完全な閉域網で運用することが現実的ではない以上は、通信回線等についてセキュリティ上の手当てをするということを前提としつつ、AIセキュリティという観点から特別の問題が生じるかどうかを整理・検討すべきであり、その整理・検討の結果が今回の取りまとめに向けた検討の記載であると理解している。
- 情報セキュリティ・AIセキュリティについての研究会資料9の記載については、概ね異論はない。
- 裁判所におけるAI利活用についても、ソブリンAIの考え方が前面に出てくる可能性があるので、今後の議論の推移を把握したほうがよい。
- 営業機密等が問題となる事案について生成AIを利用しないということに

については、そもそも民事裁判の記録管理システムのセキュリティの問題として検討すべきものであり、A I 特有の問題ではなく、別の取扱いをする必要はないように考えられる。

- 学習をしない設定でA Iを利用する限りは、A I自体に秘匿すべき情報等が入り込むわけではない。RAG等として秘匿すべき情報等を利用する場合には、当該情報がデータとして送信されることになるが、これはデータ送信についてのセキュリティの問題であってA I自体の問題ではないように考えられる。
- 特定の場合に生成A Iの利活用を除外する運用にすると、当事者がそれぞれに特別な事情があるなどとして、A Iの利用を除外するよう求めることになってしまうのではないか。

（生成A Iシステムの監査とA Iガバナンスについて）

- 生成A Iに係るシステム監査の手法として、システムが動作すべき又は動作すべきではない検査項目を定める監査項目の作成、システムの脆弱性を検証するペネトレーションテスト、ログ管理等が考えられる。
- 監査の対象については、システムが正常に作動しているかを検証する監査を指すのか、システムを使用する人に対する監査なのか、対象が不明確である。裁判官の職権行使の独立との関係が問題となるのは、人に対する監査ではないか。
- A Iシステムの場合、適正なアウトプットが出力されたかを確認することは、出力内容だけでなく、利用者がどのような出力を期待してプロンプトを入力したかを一体として把握する必要があるということに他ならないという点が特殊な点ではないか。
- 個別の事件について監査を実施するのではなく、定期的に一定の類型・使用方法について監査することは考えられるのではないか。「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」という表記では、裁判官がどのように使用したのかというプロセスの適正性の話のように読めるので、表現ぶりは検討してもらったほうがよい。
- 人に関する監査については、裁判官の行為規範と関係するのではないか。
- A Iシステムに入力を行った場合には、適切な出力がされているかというパフォーマンス管理の問題とセキュリティの問題に分かれる。システム監査においては、組織内における心理的安全性が確保されていることが重要であり、裁判所においても同様ではないかと考えられる。A Iシステムの監査においても、裁判官の職権行使の独立を担保しつつ、またこれが担保されていると感じられるような形式で行うことが重要である。
- A Iを利用したかどうか、その使い方が適切であったのかどうかは外部から判明し難い以上、個別の事件におけるA I利活用の適否について、上訴制度

の中での解決を期待することは困難ではないか。

- A I 利用が広がってくると、控訴審の審理の中で、第一審の争点整理手続における A I 利用の適否の評価が問題になるということはあるのではないかな。
- A I の出力の活用場面によって、上訴制度で解決すべき問題と裁判官の行為規範の遵守の問題に分けて考える必要があるのではないかな。
- A I 利活用において最終的に人間がチェックするということは大前提であるが、裁判官という専門的かつ信頼のおける立場の人であれば適正に判断してくれていると考えるというのでもよいように思う。
- 裁判官が A I を適正に利用できる人であることを制度的に担保しておくことが必要である。
- プロンプトは、裁判官の中では共有してその精度を高めていくことが求められるのではないかな。
- プロンプトは匿名化するなどしたものを研修等の場面で使っていくということでもよいのではないかな。
- プロンプトの共有については、従来から組織で共有されていたノウハウの伝承の延長にあるもので、ノウハウの蓄積・共有として位置づけられるのではないかな。
- 裁判官同士のノウハウの共有のために活用することは必要であるが、プロンプトを解析して裁判官の仕事ぶりを把握することで裁判官の職権行使の独立に影響を与えないようにすることも必要ではないかな。

（最高裁検証結果について）

- 最高裁検証結果でリスク・課題等として指摘された、抜け漏れについてはプロンプトの構成が不適切な可能性があり、出力の再現性についてもランダム性を無くす設定にする、R A G 等を活用するなどして回避することが可能であるなど、総じて技術的検証が不十分である可能性があるのではないかな。
- 最高裁検証結果では、A I の有用性について、やや中立的な記載であるようにも思われるが、実際の参加者からは、リスク等の指摘はされつつも、前向きな回答が得られているとのことであるので、更なる検証に期待したい。
- 今回は、初歩的な検証にとどまっているということであるが、今後の検証については、客観的かつ再現可能な評価が可能な統計的な分析も必要となってくるのではないかな。
- 今後の検証の在り方については、更に検討する必要があると思われる一方で、争点整理の場面において利活用をするに当たっても、個別の事件に応じたプロンプトの修正等が必要となることもあり、統計的分析、定量的評価が困難なところもあるのではないかな。
- 「最終判断と責任は裁判官が負う」という記載につき、「責任」としては、

象徴的なもの、法的なものの様々想定できることから、どのような位置づけで考えるのか実質的な検討が必要ではないか。

（想定ユースケースの抽出について）

- 最高裁検証結果で示されたような場面を中心に検討を進めるということについては、異論はない。ただし、訴状審査、証拠調べ、更には民事執行手続等の民事裁判全体をユースケースとして広く抽出し、議論の対象とすることも考えられるのではないか。

（想定ユースケースにおけるA I利活用伴うリスク・課題について）

- 最高裁検証結果を踏まえた検討が必要であることについて異論はない。
- 検証結果の要旨（参考資料2）においては、生成A Iに関わるリスクと、人（裁判官）に関わるリスクが指摘されており、取りまとめに向けても、問題となるリスクに着目した議論の整理が必要となるのではないか。また、「リスク」、「課題」という言葉の使い分けについても再考する必要があるのではないか。
- 一般的なリスクとして記載のある、説明責任の担保の部分につき、アルゴリズムは全て公開されているので、「公開されていないアルゴリズム」という点は誤った表現である。
- 本人訴訟を念頭に置いた場合には、法的素養がないために本人自らが利用したA Iの出力結果の正確性等の判断ができずに本人が不利益を受けることのほか、裁判所から出力結果等について確認を求められた場合にも、本来主張したかったことが抜けていること等に気付くことができないといったリスクもあるのではないか。
- 上記の本人訴訟におけるリスクは、当事者本人との認識共有の在り方の問題としてA Iを利活用するかどうかにかかわらず現在も生じ得る問題であり、A Iの利活用によって問題が顕在化しやすくなるというような位置付けではないかと考えられる。
- 想定ユースケースごとにリスクや対応策等も異なってくる可能性があるのではないか。

（考えられる対応策等について）

- 最高裁検証結果では、ヒューマン・イン・ザ・ループが不可欠であるとされているが、利活用の場面によっては、ヒューマン・オン・ザ・ループなど、人の関与の在り方が異なってくるところもあるのではないか。
- 用語については改めて検討が必要かもしれないが、想定ユースケースはいずれも、ヒューマン・イン・ザ・ループが必要な場面ではないか。
- 主として人間による対応策が記載されているが、大規模言語モデル（LLM）

それ自体による対応策についても記載すべきではないか。

(透明性確保について)

- 手続保障の観点のみならず、心証形成における裁判官の独立の維持、ひいては司法の民主的統制等の観点からも、一定の透明性確保が求められるという点については、賛成する。ただし、どのような情報をいかなる態様で、どの時点で開示すべきか等は、研究会資料8・3(2)に記載のとおり、具体的な利用場面等に応じて異なってくるところがあり、過剰な情報開示が紛争の長期化を招くおそれがあることも指摘されたとおりである。手続保障の観点からは、一般的には透明性確保が望ましいが、具体的な在り方については様々な意見がある。
- 主張整理表等のたたき台を作成する目的は、争点及び重要な証拠について、当事者と認識共有を図ることを促進することにあり、裁判官が最終的に確認した成果物等については、何らかの形で共有して透明性を確保していくことが合理的ではないか。主張整理表を共有するような運用はこれまでもなされてきたところではあるが、A Iの利活用によってこれが容易になってくるのではないか。
- 当事者に成果物等を共有すると、当事者においてもA Iを利用し、自らが提出したものが正しいなどと主張することも考えられ、裁判遅延の原因とはならないか。
- A Iを利活用するかどうかにかかわらず、争点整理に当たって主張整理案等を示すか否かも含めてある程度決まった手続で行った方が良いか、よりざっくりばらんな形で行った方が良いかについては、従前から様々な意見があった。透明性の確保という観点から主張整理表等を作成して共有することが重要であるということを強調しすぎると、当事者の警戒心を招き、硬直的な運用となってしまうおそれがあるのではないか。A Iの利活用によって、これまで時間等を要していた主張整理表等の作成が容易になるということはそのとおりかもしれないが、当事者において、主張整理表等の共有のニーズがどの程度あったのかには疑問がないではない。また、この点を措くとしても、A Iを利活用したことまで示す必要があるかどうかは別の問題であるように考えられる。
- 主張整理表等を作成した場合に、必ずしも常に当事者と共有しなければならないものではないが、最終的な成果物等については、共有する方が望ましいように考えられる。他方で、A Iを利活用したこと自体を明らかにする必要は必ずしもないようにも思われる。いずれにせよ、当事者への公表時期、公表対象などは、実務のプラクティスとして積み重ねる必要がある。
- 大量の書面等の要約については、そもそも直前に大量の書面を提出するような訴訟活動が良いのかという問題があるが、そのような事態が生じてA Iを

使って概要を把握したのであれば、基本的には、把握した概要を当事者にも伝えて認識共有を図っていくことが望ましいように思われる。もっとも、そのような事案では、当事者との信頼関係を構築することができていないことも少なくなく、どのような運用が望ましいかについては悩ましいところもある。

- A Iによる不正確な出力等がされていないかどうかは、最も利害関係がある当事者が確認することが望ましい一方で、出力を開示することによってかえって紛争が長期化する場合がある指摘もそのとおりであると考えられ、悩ましい。

(裁判官が生成A Iを利活用する手順・方法等について)

- A Iの出力結果を確認もせずに、そのまま判決に記載するようなことは許されないであろう。ガイドラインという言葉が適切かどうかは分からないが、国民の信頼の確保という観点からすると、そのような最低限の共通認識を何らかの形で言語化していくことが望ましいのではないか。
- A Iの使い方の巧拙等については、プラクティスの形成に委ねつつも、現時点で考えられるような最低限のコアなルールについては言語化しておくということは一つの考え方であるように思われる。もっとも、ルールの形式や、何を最低限と考えるのかについては、なお検討が必要ではないか。
- 最低限のルールを設けることとした場合には、敗訴した当事者は当該ルール違反を控訴理由として主張し、これを受けた高等裁判所がA Iの使い方についても判断しなければならないようなおそれもあるのではないか。
- 不意打ち防止の観点からすると、何らかのルール化をすることが望ましいが、ルールで拘束するということは、裁判官の職権行使の独立や自由心証主義を害することにならないかという懸念もある。ルール化によって、A Iの使い方が控訴理由となり得るとしても、これが認められるためには、ルール違反の痕跡が必要となるだろう。ルールの定め方としても、禁止規範ではなく、あるべき行為規範を定めることによって、国民の信頼を確保するということも考えられるのではないか。
- A Iの使い方の巧拙等が、訴訟法上の問題になるかということそうではないように考えられる。A Iの出力結果を裁判官が確認した上で活用するというようなことは行為規範としてあるべきであるが、それは、従来からあるような裁判官倫理の問題であるようにも考えられ、このような観点からは、新しい技術への対応としてリテラシーを高めていくことが求められる。A I適正化指針等において、責任ある適正利用が求められており、裁判官にも適正利用が求められることは当然であるが、何を「適正利用」というかについては、プラクティスの積み重ねによらざるを得ない部分も考えられる。したがって、現時点では「適正利用」を言語化することは難しい部分もあり、言語化する

としても、本研究会における取りまとめや、研修における資料等にとどまり、ルール化まですることには困難を伴うようにも考えられる。そうだとすると、適正利用原則違反をもって、訴訟法上の問題とはならないというような整理もあり得るのではないか。このような整理が国民からの信頼を得られるかについては問題となるが、ルール化をし、これが法的な効果を持つことによって、裁判手続が遅延したり、裁判官の萎縮に繋がるようなことは避けなければならない。

- A I の使い方が訴訟法上大きな問題となり得るとすれば、裁判官による裁判ではなく、A I による裁判であると評価されるような場合ではないか。
- 透明性の確保の在り方やルール化については難しい問題があるが、A I の使用ごとに個別的な説明、了解を得るのではなく、審理の序盤において当事者双方と訴訟の進行方針について協議するに当たって、A I の利活用の在り方についても協議をするということも考えられるのではないか。
- 当事者と協議をしてA I の利活用を進めるような運用も考えられる一方で、当事者がA I の使用を拒否した場合の対応等をめぐって紛争が生じ、A I を活用すべき場面で活用ができないというようなことも考えられるのではないか。争点整理等の場面でA I を利活用していくといった範囲については、個々の事件というよりも、組織である裁判所として公表していくという形が良いのではないか。