2024 年 7 月 11 日

AI に関する日本の法規制

創・佐藤法律事務所
弁護士　齊藤　創
同　佐藤　有紀
同　齊藤　千穂
同　安　昌秀
同　水島　優

近時、AI（人工知能）は飛躍的な革新を遂げ、新しいコンテンツを生成する生成 AI 技術が広まるなど、各種産業においては自動化と最適化が図られ、また人々の日常生活にも少なからぬ変化が生じてきました。他方で、AI の倫理的な問題やプライバシーへの懸念、労働市場における悪影響など、社会的な課題も指摘されています。EU では、EU 域内で一律に適用される人工知能（AI）の包括的な規制枠組み規則（AI 法）が成立するなど、統一的な規制整備が進みつつあります。

本稿では、AI に関する日本の法規制について概説します。

1. AI をめぐる現在の規制の紹介（法令・ガイドライン）

(1) AI に関する規制についての近時の議論

日本において、現時点では AI を包括的に規制する法令は存在せず、拘束力のないガイドラインが定められているのみです。

2019 年 3 月に「人間中心の AI 社会原則」（注 1）が策定され、また AI に関する一般的なガイドラインとして、総務省主導で「国際的な議論のための AI 開発ガイドライン案」（2017 年 7 月 28 日）（注 2）及び「AI 利活用ガイドライン」（2019 年 8 月 9 日）（注 3）が、経済産業省主導で「AI 原則実践のためのガバナンス・ガイドライン Ver. 1.1」（2022 年 1 月 28 日）（注 4）が公表されています。さらに、2023 年 5 月の G7 広島サミット、G7 各国閣僚級会合による「広島 AI プロセス包括的政策枠組み」取りまとめを経て、これらの 3 つのガイドラインを統合・見直し、その後に発展した AI 技術の特徴及び国内外における AI の社会実装に係る議論を反映して、2024 年 4 月 19 日に、新たに「AI 事業者ガイドライン（第 1.0 版）」（注 5）（以下「新ガイドライン」といいます。）が総務省及び経済産業省より公表されました。

(2) 新ガイドラインの概要

新ガイドラインが対象としているのは、政府、自治体等の公的機関を含む、様々な事業活動において AI の開発・提供・利用を担う全ての者、すなわち、AI 開発者、AI 提供者及び AI 利用者です。これに対し、事業活動以外で AI を利用する者又は AI を直

接事業で利用せず、AI システム・サービスの便益を享受し若しくは損失を被る者（以下、あわせて「業務外利用者」といいます。）は対象とされていません（注 6）。また、データ提供者も新ガイドラインの対象者とはされていません。データ収集は色々な方法が考えられる中で、新ガイドラインでは、データの提供を受ける者・データを入手する者にあたる AI の開発・提供・利用を担う者がデータを取り扱う際の責任負う形で記載がなされています。

新ガイドラインは、AI により目指す社会として尊重すべき基本理念として、(i)人間の尊厳が尊重される社会（Dignity）、(ii)多様な背景を持つ人々が多様な幸せを追求できる社会（Diversity and Inclusion）及び(iii)持続可能な社会（Sustainability）の 3 つの価値を掲げ、かかる基本理念を実現するため、各主体が連携してバリューチェーン全体で取り組むべき共通の指針として、人間中心、安全性、公平性、プライバシー保護、セキュリティ確保、透明性、アカウンタビリティ、教育・リテラシー、公正競争確保及びイノベーションの 10 個に整理しています。これに加えて、AI 開発者、AI 提供者及び AI 利用者の各々にとっての重要な事項を挙げています。主なものは以下のとおりです。

AI 開発者にとっての重要な事項としては、データ前処理・学習時における適切なデータの学習及びデータに含まれるバイアスへの配慮、AI 開発時における人間の生命・身体・財産、精神及び環境に配慮した開発、適正利用に資する開発、AI モデルのアルゴリズム等に含まれるバイアスへの配慮、セキュリティ対策のための仕組みの導入並びに検証可能性の確保、AI 開発後における最新動向への留意、関連するステークホルダーへの情報提供、AI 提供者への「共通の指針」の対応状況の説明及び開発関連情報の文書化が挙げられています。

AI 提供者にとっての重要な事項としては、AI システム実装時における人間の生命・身体・財産、精神及び環境に配慮したリスク対策、適正利用に資する提供、AI システム・サービスの構成及びデータに含まれるバイアスへの配慮、プライバシー保護のための仕組み及び対策の導入、セキュリティ対策のための仕組みの導入並びにシステムアーキテクチャ等の文書化、AI システム・サービス提供後における適正利用に資する提供、プライバシー侵害への対策、脆弱性への対応、関連するステークホルダーへの情報提供、AI 利用者への「共通の指針」の対応状況の説明及びサービス規約等の文書化が挙げられています。

AI 利用者にとっての重要な事項としては、AI システム・サービス利用時における安全を考慮した適正利用、入力データ又はプロンプトに含まれるバイアスへの配慮、個人情報の不適切入力及びプライバシー侵害への対策、セキュリティ対策の実施、関連するステークホルダーへの情報提供、関連するステークホルダーへの説明並びに提供された文書の活用及び規約の遵守が挙げられています。

各主体が連携しバリューチェーン全体で共通の指針を実践して、AI を安全安心に活用するためには、AI ガバナンスの構築が重要とされていますが、サイバー空間とフィジカル空間を高度に融合させたシステムを基盤とする社会は、複雑で変化が速く、リスクの統制が困難であることから、AI ガバナンスは、事前にルールや手続が固定したものではなく、(i)環境・リスク分析、(ii)ゴール設定、(iii)システムデザイン、(iv)運用、(v)評価といったサイクルをマルチステークホルダーで継続的かつ高速に回転させていく「アジャイル・ガバナンス」の実践が重要とされています。また、(i)環境・リスク分析では便益/リスクの理解、AI の社会的な受容の理解及び自社の AI 習熟度の理解、(ii)ゴール設定では AI ガバナンス・ゴールの設定、(iii)システムデザイン（AI マネジメントシステムの構築）ではゴール及び乖離の評価並びに乖離対応の必須化、AI マネジメントシステムの人材リテラシー向上、各主体間・部門間の協力による AI マネジメント強化並びに予防・早期対応による AI 利用者及び業務外利用者のインシデント関連の負担軽減、(iv)運用では AI マネジメントシステム運用状況の説明可能な状態の確保、個々の AI システム運用状況の説明可能な状態の確保及び AI ガバナンスの実践状況の積極的な開示検討、(v)評価では AI マネジメントシステムの機能の検証及びステークホルダーの意見の検討を、それぞれ各主体が AI ガバナンスの構築において留意する観点としての行動目標としてあげています。

新ガイドラインの別添（付属資料）では、様々な実践のポイント及び具体的な実践例が挙げられています。AI ガバナンスを構築する際には、これらの実践のポイントや実践例を参照して、各主体が置かれている個別具体的な状況や、各主体が開発・提供・利用する AI システム・サービスの目的、方法、評価の対象等も考慮して、どのような AI ガバナンスを構築するか決めていくことになるであろうと推測されます。また、複数の企業による AI ガバナンスの構築に関する実際の取組事例も紹介されており、今後 AI ガバナンスを構築しようとする際に参考になると思われます。

新ガイドラインでは、高度な AI システムに関係する事業者は、広島 AI プロセスを経て策定された「全ての AI 関係者向けの広島プロセス国際指針」（注 7）及び「高度な AI システムを開発する組織向けの広島プロセス国際指針」（注 8）を遵守すべきとし、高度な AI システムを開発する AI 開発者についてはこれらに加えて「高度な AI システムを開発する組織向けの広島プロセス国際行動規範」（注 9）についても遵守すべきとしています。

(3) その他のガイドライン

上記の一般的なガイドラインのほか、個別の分野に特化したガイドラインもいくつか公表されています。例えば、教育現場での生成 AI の活用に関して、文部科学省が「初等中等教育段階における生成 AI の利用に関する暫定的なガイドライン」（2023 年 7 月 4 日）（注 10）を、佐賀県教育委員会が「生成 AI 利用ガイドライン

【vol.1】」（2023 年 7 月 14 日）（注 11）を公表しており、ヘルスケア領域生成に特化した AI 活用のガイドラインとして、日本デジタルヘルス・アライアンスが「ヘルスケア事業者のための生成 AI 活用ガイド」（2024 年 1 月 18 日）（注 12）を、一般社団法人日本プライマリ・ケア連合学会が「プライマリ・ケアにおける AI 利用ガイドライン」（2023 年 12 月 1 日）（注 13）を公表しています。

2．AI を用いた事業に関する法規制

(1)　AI を開発、提供又は利用する事業者において問題になる法規制

(i)著作権

AI と著作権の関係については、今後、裁判例を含む具体的な事例の蓄積、AI に関連する技術の発展、諸外国における検討状況等を踏まえて検討されることになりますが、現時点においても、①学習・開発段階における著作権侵害、②生成・利用段階における著作権侵害、③生成物の著作物性に関する議論が活発化しています。

まず、①主として AI 学習を実施する者が、既存の著作物に係る著作権を侵害することにならないかが問題になります。著作物を利用しようとする場合、原則として著作権者の許諾を得る必要があるところ、2018 年に情報解析のための著作物の利用に関して「柔軟な（著作権者の）権利制限規定」（注 14）が創設され、「著作物に表現された思想又は感情を自ら享受し又は他人に享受させることを目的としない場合には」著作権者による許諾を要せず著作物を利用できることとされました。この「非享受目的」は、いわゆる「過学習」（overfitting）を意図的に行う場合のように、非享受目的と享受目的が併存する等、複数の目的の内にひとつでも「享受」の目的が含まれていれば否定され、その AI 学習を実施した者は、著作権侵害として、損害賠償請求、差止請求（例、学習済みモデルの廃棄請求等）を受ける可能性があります。

②生成・利用段階における著作権侵害としては、主として、AI サービスの提供者や利用者による、AI 生成物の生成及びインターネットを介した送信等の利用行為が、既存の著作物の著作権侵害とならないかが問題となります。AI 生成物による著作権侵害は、従来の著作権侵害の有無の判断基準と同様、既存の著作物との「類似性」及び「依拠性」がある場合に認められます。「類似性」の有無は人間が AI を使わずに創作したものと同様に考えることができます。他方「依拠性」は、(i)Image to Image のように、AI の利用者が既存の著作物を認識していたと認められる場合、及び(ii)既存の著作物を認識していなかったが、AI 学習用データに既存の著作物が含まれる場合で、かつ、当該生成 AI の開発・学習段階で当該著作物を学習していた場合に、認められる可能性が高くなります。生成・利用段階で著作権侵害が認められる場合、AI の利用者だけでなく、生成 AI に関するサービス提供者が著作権侵害について責任を負う可能性が高いものと思われます。

③生成物の著作物性とは、AI 生成物が著作権法による保護を受けるかどうかという議論であり、従来の「著作物」の解釈と同様、生成 AI に対する指示が表現に至らないアイデアにとどまるような場合には、創作性が認められず著作物性は認められません。個々の AI 生成物について、①指示・入力（プロンプト等）の分量・内容、②生成の試行回数、③複数の生成物からの選択、④生成後の加筆・修正等の種々の要素に鑑み、個別具体的な事例に応じて総合的に判断されることになります。

(ii)個人情報保護法

AI の開発や利用にあたっては、個人情報がしばしば利用されることから、「個人情報保護法」に違反しないよう十分注意する必要があります。具体的には、まず、①生成 AI を提供する事業者（ChatGPT を提供する OpenAI など）が、生成 AI を開発するために個人情報を取り込もうとする時には、正しく利用目的を示して個人情報を入手したか、実際の利用方法が利用目的から外れていないか、人種や信条といったセンシティブな情報を取得する際のルールに違反していないか、などの問題が起こりやすいと言えます。この問題については、2023 年 6 月に OpenAI に対して、利用目的を日本語で通知することや、センシティブな情報の取得についての注意喚起が行われました（注 15）。また、②生成 AI を利用する側でも個人情報についての注意が必要です。例えば従業員の個人情報を管理している企業が、業務効率化のために生成 AI を利用する時に、個人情報を入力することが考えられます。この場合、正しく利用目的を示して個人情報を入手したか、実際の利用方法が利用目的から外れていないか、注意が必要です。また、入力された個人情報が生成 AI 側で学習に使われてしまう場合、入力した側でも、第三者に個人情報を提供したことになる（外国の生成ＡＩを利用した場合には、さらに外国へ個人情報を移転したことになってしまう）可能性があり、個人情報保護法に違反することになります。このように、利用する側でも個人情報保護について十分な注意が必要であり、2023 年 6 月には個人情報保護委員会から「生成 AI サービスの利用に関する注意喚起等」（注 16）が公表されています。

こうした、生成 AI 開発・利用における個人情報保護法上の留意点については、新ガイドラインにおいても詳細に言及されており、個人情報保護の観点が強く意識されていると言えます。

(iii)プライバシー

プライバシー権との関係では、ＡＩだからこそ特に注意が必要となる問題が２つ存在します。一つ目は、本人は、一つ一つはそれほどセンシティブとは言えない情報だけを出したのに、AI がそれらの情報を統合して処理した結果、センシティブな情報が明らかになってしまう、という問題です。二つ目は、ＡＩによる処理の結果、本来の自分と

はかけ離れた人物像が形作られ、利用されてしまう（しかも、ＡＩの処理が非常に複雑であるため、その正誤を検証することができない）、という問題です。
こうした問題に対し、EU ではＡＩによる処理の中止を求める権利や、ＡＩの判断のみに基づいて重要な決定をされない権利を認める法規制が法律によって認められています（注 17）が、日本では実現していません。もっとも、上述のとおり、政府が公表する新ガイドラインでは、AI による処理を行う場合に、個人の尊厳を尊重すること、人間の判断を介在させること、国際的な個人データ保護の原則や基準を参照したプライバシー保護などが求められており、AI 特有のプライバシー侵害の問題が意識されつつあり、今後の議論の進展が待たれます。

(iv)営業秘密

近時、業務の円滑化等の目的から、生成 AI に自社の情報を入力し利用する事業者が増えています。しかしながら、従業員が自社の機密情報を生成 AI に入力することを許してしまうと、不正競争防止法の「営業秘密」や「限定提供データ」として、同法による保護を受けることができなくなる可能性があります。即ち、「営業秘密」として不正競争防止法によって保護されるためには、①秘密管理性（秘密として管理されていること）、②有用性（事業活動に有用な技術上又は営業上の情報であること）、③非公知性（公然と知られていないこと）が必要ですが、従業員が何のルールもなく生成 AI に機密情報を入力できるとすると、①秘密として管理されているとは言えず、当該機密情報は「営業秘密」として認められなくなると思われます（ただし、ＡＩサービス提供事業者との間で、営業秘密を特定した秘密保持契約（NDA）を締結するなど、自社の秘密管理意思を明らかにしているような場合は秘密管理性が失われないとも考えられます（注 18）。また、同法上の「限定提供データ」は、①限定提供性（業として特定の者に提供されること）、②相当蓄積性（電磁的方法により相当量蓄積されていること）、③電磁的管理性（電磁的方法により管理されていること）が要件とされるところ、③電磁的管理性が失われると考えられます。事業者においては、自社の機密情報を生成 AI に入力しない等ルール作りをすることが望まれます。

(v)競争法

公正な競争の実現が、ＡＩの利用によって妨げられる場合、独占禁止法違反となる可能性があります。この問題について、2021 年 3 月に、公正取引委員会が主催する研究会が取りまとめた報告書（「アルゴリズム/AI と競争政策」）（注 19）が公表されています。この報告書では、価格設定・価格調査アルゴリズムにより価格競争が活発になる場合がある一方で、その利用の態様によっては競合する企業間でＡＩを利用した協調的な価格調整が行われたり、競合する利用者と消費者の取引の妨害（略奪的な価

格設定、意図的なランキング操作（注 20）など）が行われる場合など、ＡＩが関わる問題が丁寧に分析されており、この問題について当局の関心も高いと言えそうです。

(vi)経済安全保障推進法

2022 年 5 月の経済安全保障推進法の成立を受け、AI は「特定重要技術」（当該技術が外部に不当に利用された場合において、国家及び国民の安全を損なう事態を生ずるおそれがあるもの等三類型が存在する。）に指定されました。これによって、AI の研究開発については、国による研究開発促進支援の対象とされました。同時に、海外への技術漏えい対策、営業秘密の保護、研究の健全性や公正性確保などについて十分な配慮が求められることになります（注 21）。

(2) その他規制がある業界

以下では、金融、医療・介護といったいわゆる規制産業と AI の利用について紹介します。

(i)金融（銀行、資産運用、保険）

金融分野では、顧客対応（チャットボットなど）で AI が活用されているほか、銀行、資産運用、保険といった各分野の業務でも AI の利用が進められています。例えば銀行の与信審査、資産運用、保険設計など、金融分野では、昔からデータ分析がビジネスの重要な要素でした。このため、大量のデータを処理する AI と親和性があると言えます。

ただし、ＡＩには、処理過程が人間に確認できず「ブラックボックス」となってしまう、という問題があります。このことが、顧客間で差別的にも見える取扱いが起きたり（AI による信用スコア算定など）、顧客に対する運用方針の説明が困難となったり（AI アドバイザーを用いた顧客資産運用など）といった問題につながるほか、個人情報保護との摩擦を生じる可能性（個人のヘルスケアデータや遺伝子情報などにリンクした保険新商品など）もあります。

もちろん、登録投資運用業者には各種行為規制が課され（注 22）、「金融分野における個人情報保護に関するガイドライン」が定められていますが、金融分野で AI 利用についての統一的な規制はありません。また、個別の法律やガイドラインでも、AI を意識した規制はほとんどみられません。もっとも、2020 年に割賦販売法が改正され、AI によって貸付可能額を算定する場合の規制が作られるなど、重要な変化も見られています。さらに、銀行や生損保などが参加する業界団体（「金融データ活用推進協会」）が、具体的な設定事例に基づいて生成 AI 活用で得られる効果とリスクを整理した「金融生成 AI 実務ハンドブック」を公表し（2024 年 5 月）、また夏頃を目途

に、生成 AI 利用についての自主規制ガイドライン（「金融生成 AI ガイドライン」）の策定が進められています。

(ii)リーガルテック（契約書レビュー）

日本でも、近時、契約書作成・レビュー、文書管理、リサーチ、フォレンジックといった機能において、いわゆるリーガルテック・サービスが登場してきました。これらのサービスのうち、いわゆる契約書 AI レビューサービスについては、弁護士でない者は、報酬を得る目的で、法律事件に関して鑑定をしたり法律事務を取り扱ったりすることを禁止する弁護士法 72 条との関係で問題とならないかが、論点となってきました。これについては、法務省の回答が出され（注 23）「単に言語的な意味内容の類似性を超えて法的効果の類似性を表示するものと評価される場合」は鑑定と評価される可能性が否定できないこと、また弁護士が法律事務所や事業会社においてサービスを利用した結果も踏まえて審査対象となる契約書等を自ら精査し、必要に応じて自ら修正を行う方法でサービスを利用するときであればれば同条項との関係で問題とならないこと等が回答されました。

また、AI を用いた他リーガルテックのサービスの利用に際しては、他社から入手した秘密情報をサービス利用に際して入力することにより、AI サービス提供会社という「第三者」に秘密情報を開示することとなり、自社が秘密保持義務に違反してしまう可能性にも留意が必要です。

注 1：https://www.cas.go.jp/jp/seisaku/jinkouchinou/pdf/aigensoku.pdf、

注 2：https://www.soumu.go.jp/main_content/000499625.pdf

注 3：https://www.soumu.go.jp/main_content/000809595.pdf

注 4：https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/pdf/20220128_1.pdf

注 5：https://www.meti.go.jp/press/2024/04/20240419004/20240419004-1.pdf 、
https://www.meti.go.jp/press/2024/04/20240419004/20240419004-2.pdf

注 6：ただし、事業活動において AI の開発・提供・利用を担う者から業務外利用者への必要な対応については、新ガイドラインに記載されています。

注 7：https://www.soumu.go.jp/hiroshimaaiprocess/pdf/document03.pdf

注 8：https://www.mofa.go.jp/mofaj/files/100573469.pdf

注 9：https://www.mofa.go.jp/mofaj/files/100573472.pdf

注 10：https://www.mext.go.jp/content/20230718-mtx_syoto02-000031167_011.pdf

注 11：https://www.pref.saga.lg.jp/kyouiku/kiji00397834/3_97834_287223_up_4oo0tku4.pdf

注 12：https://jadha.jp/news/news20240118.html

注 13：https://www.primarycare-japan.com/files/news/news-625-1.pdf

注 14: 著作権法（昭和 45 年法律第 48 号）第 30 条の 4

注 15: https://www.ppc.go.jp/files/pdf/230602_alert_AI_utilize.pdf

注 16: https://www.ppc.go.jp/files/pdf/230602_alert_generative_AI_service.pdf

注 17:GENERAL DATA PROTECTION REGULATION (GDPR)では、プロファイリングの中止を求める権利（21 条「Right to Object」）、プロファイリングのみに基づいて重要な決定を下されない権利（22 条「Automated individual decision-making, including profiling」）が認められています。

注 18:経済産業省「営業秘密管理指針」14 頁参照

https://www.meti.go.jp/policy/economy/chizai/chiteki/guideline/h31ts.pdf

注 19:https://www.jftc.go.jp/houdou/pressrelease/2021/mar/210331_digital.html

注 20　:飲食店ポータルサイトの評価アルゴリズム変更によって飲食店が損害を受けたと主張する訴訟において、独占禁止法違反が認められた裁判例があります（東京地方裁判所 2022 年 6 月 16 日判決、ただし、控訴審においては独占禁止法違反は否定されました（東京高等裁判所 2024 年 1 月 19 日判決））。

注 21　:「特定重要技術の研究開発の促進及びその成果の適切な活用に関する基本指針」

https://www.cao.go.jp/keizai_anzen_hosho/suishinhou/doc/kihonshishin3.pdf

注 22　:例えば、誠実義務（金融商品取引法第 36 条）、契約締結前交付書面の交付（同法 37 の 3）、忠実義務・善管注意義務（同法 42 条）等一般的な規定が挙げられる。

注 23　:2022 年 10 月 14 日グレーゾーン解消制度に係る回答（https://www.meti.go.jp/policy/jigyou_saisei/kyousouryoku_kyouka/shinjigyo-kaitakuseidosuishin/press/221014_yoshiki1.pdf）及び 2023 年 8 月付法務省大臣官房司法法制部からの回答（https://www.moj.go.jp/content/001400675.pdf）。また、無償であれば「報酬を得る目的」がなく同条に違反しないこと、継続的取引の基本となる契約を締結している会社間において特段の紛争なく当該基本契約に基づき従前同様の物品を調達する契約を締結する場合であって、その契約関係を明らかにするために契約書等を作成する場合に当該サービスを提供するときには「法律事件」に該当せず、同条に違反しないと考えられることが説明されています。

留保事項

- 本書の内容は関係当局の確認を経たものではなく、法令上、合理的に考えられる議論を記載したものにすぎません。また、当職らの現状の考えに過ぎず、当職らの考えにも変更がありえます。
- 本書は Blog 用に纏めたものに過ぎません。具体的案件の法律アドバイスが必要な場合には各人の弁護士にご相談下さい。