牛島総合法律事務所
IT/個人情報/知的財産ニューズレター

ChatGPT をはじめとする生成 AI を利用する際の法的論点

2023 年 5 月 16 日

弁護士　影島広泰

＜目次＞

ChatGPT をはじめとする生成 AI（ジェネレーティブ AI）を企業が利用する際にどのような法的論点を検討すべきであろうか。本ニューズレターでは、典型的に検討すべき論点をピックアップする。

なお、各論の詳細については、特集記事「ChatGPT の利用について法務が検討すべき 3 つのポイント」を参照されたい。また、個人情報保護法に関するより具体的な例を踏まえた分析は、特集記事「ChatGPT と仮名加工情報・個人情報」を参照されたい。本ニューズレターは、これらの記事から法的論点を抽出した“ダイジェスト”である。

1. 生成 AI（ジェネレーティブ AI）とは

生成 AI（Generative AI）とは、厳密な定義があるわけではないが、「プロンプトに応答してテキスト、画像、またはその他のメディアを生成できる人工知能（AI）システムの一種」（Wikipedia）などとされている。従来の AI システムがパターンを認識して予測するように設計されているのに対し、生成 AI はテキスト、画像、音声などの新しいコンテンツを作成する点に特色がある。

IT 大手の投資額（例えば、Microsoft の OpenAI 社に対する投資額は 100 億ドル（約 1.3 兆円）にのぼる。）をみれば、今後、生成 AI を含む AI の分野では技術及びビジネスが急速に発展していく可能性が高いため、次々と新しいサービスが生まれるものと予想されるが、2023 年 5 月 16 日時点で一般的に利用できるサービスとして、例えば以下がある。

- OpenAI 社：ChatGPT（チャット）、各種モデルの API 利用
- Microsoft 社：Azure OpenAI Service（OpenAI のモデルを利用できるサービス）
- Google 社：Bard（チャット）
- Stability AI 社：Stable Diffusion（画像生成）

これらの生成 AI の特徴は、「プロンプト（Prompt）」と呼ばれる入力によって、様々なタスクを行わせることができる点にある。プロンプトは、モデルが生成するレスポンスのコンテキストや方向性を決定する。たとえば、「ローマの歴史を簡潔に説明してください」というプロンプトをモデルに与えると、モデルはローマの歴史についての要約を生成する。モデルは直接的な指示（「ローマの歴史を説明する」）だけでなく、より抽象的な指示（「私

がローマの歴史についてのエッセイを書いていると想像してください」）にも反応する。プロンプトの設計は、モデルの出力を最適化するために重要なスキルとなる（プロンプト・エンジニアリングと呼ばれる。）。

2. プロンプトに、回答を得る対象として入力する場面

(1) 個人情報保護法

プロンプトに個人情報を入力し、個人情報としての出力を得ることは、個人情報の利用に当たる。

したがって、利用目的の特定（個人情報保護法 17 条 1 項）及び通知等（21 条 1 項）が必要となる。

また、AI ベンダへの第三者提供（27 条）又は外国にある第三者への提供（28 条）も大きな問題となり得る。この点は、個人データの「提供」に当たるか否か、すなわち AI ベンダが個人データを「取り扱う」といえるかによって結論が変わってくるため、生成 AI の利用規約やアプリの設定等を確認し、検討することになる。

(2) 契約上の秘密保持義務

契約上の秘密保持義務の対象となっている情報を入力する場合、秘密保持義務違反とならないかが問題となる。とりわけ、自社がオーナーシップを持っている情報ではなく、他者から預かっている情報（例えば、IT ベンダのサービスを利用している顧客企業がサービス上に保存しているデータ）を入力する際には、法的にもビジネス的にも慎重な判断が必要となると考えられる。生成 AI の利用規約等を確認し、秘密保持義務に違反しないかを検討する必要がある。目的外利用禁止の条項についても同様である。

(3) 著作権法

著作物をプロンプトに入力する場合、プロンプトの内容、すなわち生成 AI への指示の内容によっては、著作権を侵害する可能性がある。例えば、小説を要約するように指示したり、プログラムのソースコードを改変するように指示するようなケースである。

3. プロンプトに、few-shot として入力する場面

(1) 個人情報保護法

プロンプトには、質問（タスク）のサンプルを記載することもできる（「few-shot」プロンプトという。）。個人情報を few-shot に入力することも個人情報の利用に当たる可能性が高い。

なお、few-shot として入力した個人情報と質問として入力した個人情報とを照合しないのであれば、few-shot として入力する情報は仮名加工情報としてもよいと考えられる。

(2) 契約上の秘密保持義務

前記 2 と同様、生成 AI の利用規約等を確認し、秘密保持義務に違反しないかを検討する必要がある。

(3) 著作権法

著作物を few-shot としてプロンプトに入力する場合、プロンプトの内容によっては著作権を侵害する可能性がある。例えば、あるアニメのキャラクターのデータを複数入力して、そのキャラクターの別のポーズを作画するように指示した場合、出力した画像がプロンプトとして入力した著作物の著作権を侵害しないかという論点が生ずる。

4. 機械学習の学習用データとして入力する場面

(1) 個人情報保護法

OpenAI 社の API 等では、学習済みのモデルに対して追加学習（fine-tuning）を行うことができる。この場合、出力されるのは再学習された学習済みモデルである。このような学習済みモデルは「個人に関する情報」ではないから個人情報保護法の適用を受けないし個人情報保護員会 Q&A「Q1-8」）、当該モデルを作成することについても制約はない（同「Q2-5」）

(2) 契約上の秘密保持義務

前記 2 と同様、生成 AI の利用規約等を確認し、秘密保持義務に違反しないかを検討する必要がある。

(3) 著作権法

著作物を機械学習の学習用データとして利用することは、「著作物に表現された思想又は感情」を享受する目的としておらず、情報解析の用に供する場合であるため、著作者の許諾は原則として不要と考えられる（著作権法 30 条の 4）。ただし、「当該著作物の種類及び用途並びに当該利用の態様に照らし著作権者の利益を不当に害することとなる場合」には許諾が必要であるため、注意が必要である。例えば、学習用データとして利用するためにクロールすることが明示的に禁止されているウェブサイトのデータをクロールして学習用データとして利用すれば、「著作権者の利益を不当に害する」とされる可能性があるし、別途不法行為が成立する可能性もある。

5. Embedding（ベクトル化・埋め込み）を行う場面

(1) 個人情報保護法

ベクトル化とは、文章を数値化し、似た文書を検索することなどができるようにする処理である。ベクトル化されたデータそのものは「個人に関する情報」ではないから個人情報保護法の適用を受けないが、そのデータと元のデータを紐付けして検索で利用することになれば、個人情報の利用に当たることになる。

(2) 契約上の秘密保持義務

前記 2 と同様、生成 AI の利用規約等を確認し、秘密保持義務に違反しないかを検討する必要がある。

(3) 著作権法

ベクトル化することそのものは「著作物に表現された思想又は感情」を享受する目的としていないと考えられる（著作権法 30 条の 4）。したがって、「著作権者の利益を不当に害する」こととならない利用であれば問題ないと考えられる。

6. 得られた回答を利用する場面

(1) 個人情報保護法

生成 AI が生成した回答は、差別的であったり、内容が不正確だったりする可能性がある。前者は不適正利用（個人情報保護法 19 条）の問題となり、後者は内容の正確性の確保（22 条）の問題となる。

(2) 契約上の秘密保持義務

前記 2 と同様、生成 AI の利用規約等を確認し、秘密保持義務に違反しないかを検討する必要がある。

(3) 著作権法

前記 3 で述べたような few-shot プロンプトで不適切な入力をするような場合を別として、生成 AI が生成した文章や画像等が他者の著作権を侵害するリスクは大きくないと考えられる。

他方で、企業実務としては、生成 AI が生成したものについて権利主張することが難しい点には留意が必要である。例えば、生成 AI が生成したプログラムのソースコードは著作物ではないとされる可能性があるから、ソフトウェア開発委託契約においては権利の帰属等を適切に定める必要性があるように思われる。

以 上