弁護士法人　三宅法律事務所

Miyake　& Partners

Miyake newsletter

生成 AI サービスを使用する際の留意点・規定例

はじめに

平素より大変お世話になっております。

さて、今回は「生成AIサービスを使用する際の留意点・規定例」をご案内させていただきます。

令和５年７月５日

弁護士法人三宅法律事務所

＊本ニュースレターに関するご質問・ご相談がありましたら、下記にご連絡ください。
弁護士法人　三宅法律事務所
弁護士　渡邉雅之,　弁護士　越田晃基,　弁護士　岩田憲二郎（執筆者）
TEL 03-5288-1021　FAX 03-5288-1025
Email: m-watanabe@miyake.gr.jp
k-koshida@miyake.gr.jp
k-iwata@miyake.gr.jp

生成 AI サービスを使用する際の留意点・規定例

弁護士法人三宅法律事務所

ChatGPT をはじめとする生成 AI サービス（質問・作業指示（プロンプト入力）等に応えて生成する AI を利用したサービス）を利用する場合には、その利便性だけでなく、個人情報や著作物の取扱い等のリスクについて留意する必要があります。

本稿においては、事業会社において、ChaTGPT をはじめとする生成 AI サービスを利用する場合の留意点や規定例について解説いたします。[1]

第１．個人情報の取扱いに関するリスクと事業会社における取扱い

１．個人情報保護法のルール

個人情報の保護に関する法律（以下「個人情報保護法」または「法」といいます。）では、事業者（個人情報取扱事業者）は、個人情報を**特定された利用目的の範囲内で利用**しなければなりません（法 18 条１項）。

また、事業者が**個人データを第三者に提供**する場合には、**本人の同意を取得**するのが原則です（法 27 条１項）。この点、**個人データの取扱いの委託**に該当する場合には、第三者への提供とはみなされず、**本人の同意は不要**となります（法 27 条５項１号）。

さらに、事業者が EEA 加盟国・英国以外の外国にある第三者に個人データを提供する場合には、①提供する外国名や外国の個人情報保護法制に関する情報等を提供した上で、外国にある第三者に提供する旨について本人の同意を得るか、または、②個人情報保護法上の事業者と同等の基準適合体制を整備した上で、定期的に当該外国の個人情報保護法制に関する情報その他のリスク情報等を提供した上で本人の同意を得るなどしなければなりません（同法 28 条１項・２項）。

２．ChatGPT における個人情報の取扱い

OpenAI の提供する ChatGPT の生成 AI のサービスは、単に機械的に委託元から依頼された入力や記録作業をするだけではなく、顧客から入力されたプロンプトに基づき、外部からの情報を収集して文章・画像等を AI に基づき生成するものであり、「個人データの取扱いの委託」（法 27 条５項１号）として、本人の同意を得ないで個人データを提供できる場合として整理することには疑義があります。

また、OpenAI の API データ利用ポリシー（API data usage policies）[2]によれば、2023 年３月１日以降、API を経由して顧客から送信されたデータについては原則としてモデルのトレーニングや改善に利用しない（ただし、顧客が OpenAI とデータを共有することについて明示による同意をした場合を除く）とされています。

これに対して、API を経由しないで ChatGPT を利用する場合には、ChatGPT や DALL-E などの API 以外の消費者向けサービスについては、サービスを改善するために、プロンプト、応答、アップロードされた画像、生成された画像などのコンテンツを使用する場合があると

---

[1] 生成 AI サービスの利用に関するルールについては、一般社団法人日本ディープラーニング協会（JDLA）が 2023 年５月１日に公表した「生成 AI 利用ガイドライン」（https://www.jdla.org/document/#ai-guideline）が参考になる。

[2] https://openai.com/policies/api-data-usage-policies

されています。また、顧客は OpenAI の提供するフォームに記入することにより、いつでも当社のサービスを改善するためにコンテンツが使用されることをオプトアウトするように要求できるとされています（ただし、オプトアウトは 2023 年３月１日以降のみ利用可能）。[3]

これらの点からも、OpenAI の提供する ChatGPT の生成 AI のサービスを「個人データの取扱いの委託」（法 27 条５項１号）として、本人の同意を得ないで個人データを提供できる場合として整理するのは困難です。

OpenAI は米国カルフォルニア州サンフランシスコの事業者であり、日本の事業者がこれを利用する場合には、外国にある第三者に個人データを提供する場合（法 28 条）に該当する可能性が高いです。

OpenAI が個人情報保護法上の事業者と同等の基準適合体制を整備しているかは明らかではありませんので、提供する外国名や外国の個人情報保護法制に関する情報等を提供した上で、外国にある第三者に提供する旨について本人の同意を得る必要があります（法 28 条１項）。

個人情報保護委員会は、令和５年（2023 年）６月２日に公表した「生成 AI サービスの利用に関する注意喚起等」においては、生成 AI サービスの利用に際しての個人情報取扱事業者の個人情報の取扱いの留意点として、以下の事項が記載されています。

① 個人情報取扱事業者が生成 AI サービスに個人情報を含むプロンプトを入力する場合には、特定された当該個人情報の利用目的を達成するために必要な範囲内であることを十分に確認すること。
② 個人情報取扱事業者が、あらかじめ本人の同意を得ることなく生成 AI サービスに個人データを含むプロンプトを入力し、当該個人データが当該プロンプトに対する応答結果の出力以外の目的で取り扱われる場合、当該個人情報取扱事業者は個人情報保護法の規定に違反することとなる可能性がある。そのため、このようなプロンプトの入力を行う場合には、当該生成 AI サービスを提供する事業者が、当該個人データを機械学習に利用しないこと等を十分に確認すること。

３．事業会社における ChatGPT の利用の留意点・規定例

事業会社は、個人情報保護法上の自ら業務で取得した個人情報をデータベースに入力して利用するので、個人情報保護法上の事業者（個人情報取扱事業者）に該当します。

事業会社の役職員が ChatGPT のプロンプトに個人データを含むデータを入力する場合には、自らのプライバシーポリシー等で特定している利用目的の範囲内であるか確認するとともに、外国にある第三者に提供する旨の本人の同意を得なければならないと考えられますが、これは現実的ではありません。

したがって、事業会社の役職員が ChatGPT のプロンプトにデータを入力する場合は、個人情報（氏名、生年月日など特定の個人が識別される情報（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）を入力しないようルール化しておく必要があります。

[3] 「消費者サービスのデータ利用に関する FAQ（Data usage for consumer services FAQ）」（https://help.openai.com/en/articles/7039943-data-usage-for-consumer-services-faq）

この点、上記２のとおり、API を経由して ChatGPT を利用する場合には、OpenAI において個人データの利用がないこととされていますが、この場合でも「個人データの取扱いの委託」に該当することについては疑義があるため、個人情報の入力をすることは控えるべきです。

上記のとおり、ChatGPT のプロンプトに個人情報の入力をすること自体を禁止すべきであるので、特定された個人情報の利用目的の範囲内であるか否かの範囲であるかの判断は不要です。

個人情報については、その氏名や生年月日、E メールアドレスなど特定の生存する個人を識別できる情報を削除したとしても、他の情報と容易に照合することができ、それにより特定の個人を識別することができる場合には個人情報に該当します（個人情報保護法 2 条 1 項 1 号括弧書き）。

また、個人情報保護法の解釈上、提供先である事業者において特定の個人が識別できない場合であっても、提供元において特定の個人が識別できる場合には個人情報・個人データに該当し、個人データの第三者提供に該当すると解されています（いわゆる「提供元基準」）。

したがって、厳格に解する場合には、ChatGPT のプロンプトに入力するデータは、他の情報と照合して容易に特定の生存する個人が識別できる情報を排除したデータを入力する必要があります。

事業会社の社内規程・社内ルールの規定例としては以下のような規定が考えられます。

（規定例）
ChatGPT などの生成 AI サービスを利用する場合には、質問・作業指示（プロンプト入力）をする場合には、違法な個人データの第三者提供に該当する可能性がありますので、個人情報を入力しないでください。氏名、生年月日などの特定の個人が識別できる個人情報を削除しても、他の情報と照合して容易に特定の個人を識別できる場合には個人情報に該当しますので、そのような情報の入力もしないでください。

第２．著作物の取扱いに関するリスクと事業者における取扱い

１．著作権法上のルール

平成 30 年の著作権法改正（平成 31 年（2019 年）１月１日施行）により設けられた著作権法 30 条の４においては、「著作物は、**次に掲げる場合その他の当該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、その必要と認められる限度において、いずれの方法によるかを問わず、**利用することができる。**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は、この限りでない。**」とされ、同条２号に「**情報解析（略）の用に供する場合**」（AI が学習するためのデータの収集・利用等の行為）が掲げられています。

政府の知的財産戦略本部が令和５年（2023 年）６月に公表した「知的財産推進計画 2023」によれば、OpenAI の ChatGPT や画像生成サービスである Dall-E などの生成 AI と著作権に関して、①AI をめぐる最近の動向として、「生成 AI」の技術が急激に発展し、画像生成、文章作成等の分野で急速に普及し、②これにより、生成 AI がオリジナルに類似した著作物を生成するなどの懸念や、著作権侵害が大量に発生し、個々の権利者にとって紛争解決が困難となる等のおそれも指摘され、③ AI 技術の発展とクリエイターの権利保護等の双方の観点に留意しながら、必要な方策を検討することとされています。

これに関して、AI による文章や画像等の生成物の「生成段階」では、(i)「学習済みモデル」の利用者に「創作意図及び創作的寄与」がある場合には、出力された生成物は著作物に

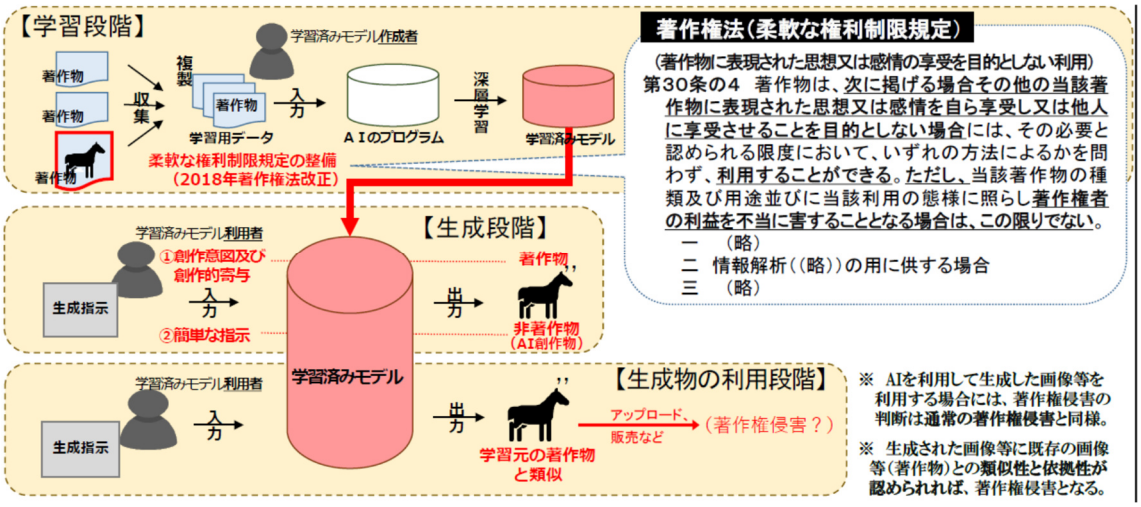
該当するが、(ii)簡単な指示である場合には、出力された非著作物（AI 創作物）であるとされています。

ChatGPT のような文章生成 AI サービスのユーザーが何らかの指示をして、何らかのリサーチ結果、アイデアや回答を得た場合、出力テキストにはユーザーの「創作意図及び創作的寄与」は通常はありませんので、文章生成 AI サービスによる出力テキストには著作権は発生しないと考えられます[4]。

AI による文章や画像等の生成物の「利用段階」においては、自らの著作物と認められない AI 創作物（AI を利用して生成した画像等）を利用する場合には、著作権侵害の判断は通常の著作権侵害と同様に判断され、学習元の著作物と類似性・依拠性が認められるものを外部に配信・アップロード・販売する場合には著作権侵害となり得るとされています。

もっとも、既存の著作物を生成 AI に入力すること自体が「著作権者の利益を不当に該当することになる場合」は営利目的ではない自己利用であっても著作権侵害に該当することになり得ます。

「知的財産推進計画 2023」では、①AI 生成物が著作物と認められるための利用者の創作的寄与の考え方、②学習用データとして用いられた元の著作物と類似する AI 生成物が利用される場合の著作権侵害に関する考え方、③AI（学習済みモデル）を作成するために著作物を利用する際の、著作権法第 30 条の４ただし書に定める「著作権者の利益を不当に害することとなる場合」についての考え方について、今後の検討課題とされています。



【出所】「知的財産推進計画 2023（概要）」知的財産戦略本部

２．事業会社における取扱い・規定例

OpenAI の ChatGPT や画像生成サービスである Dall-E などの AI 生成サービスに文章や画像を入力した場合に、AI 生成物が入力した個人の著作物と認められるか否かは「創作的意図及び創作的寄与」が必要であることを事業会社内に周知する必要があります。

次に、自らの著作物と認められない AI 創作物（AI を利用して生成した画像等）を利用する場合には、学習元の著作物と類似性・依拠性が認められるものを外部に配信・アップロード・販売など他人に享受させることを目的とする場合には著作権侵害に該当します。

[4] 「生成 AI の利用ガイドライン【簡易解説付】」（一般社団法人日本ディープラーニング協会（JDLA））参照。

そこで、著作権侵害の「類似性・依拠性」を判断するのは困難な場合もあるので、生成 AI サービスのプロンプトに既存著作物、作家名、作品の名称などを入力しないようルール化することが考えられます。

また、AI 生成サービスの生成物を利用（外部に配信・アップロード・販売など他人に享受させることを目的とする場合）には、その AI 生成物が既存の著作物に類似しないか調査を求めることが考えらえます。

なお、著作物の自己利用であっても、著作権法 30 条の４ただし書に定める「著作権者の利益を不当に害することとなる場合」として認められない場合が今後政府から示される可能性があります。したがって、自己利用であるからといって安易に他人の著作物である文章や画像などを生成 AI サービスのプロンプトに入力しないように求めることが考えられます。

事業会社の社内規程・社内ルールの規定例としては以下のような規定が考えられます。

（規定例）

AI 生成サービスに文章や画像を入力した場合に、AI 生成物が入力した個人の著作物と認められるためには「創作的意図及び創作的寄与」が必要であることに留意してください。

自らの著作物と認められない AI 創作物（AI を利用して生成した画像等）を利用する場合には、学習元の著作物と類似性・依拠性が認められるものを外部に配信・アップロード・販売など他人に享受させることを目的とする場合には著作権侵害に該当します。著作権侵害の「類似性・依拠性」を判断するのは困難な場合もあるので、生成 AI サービスのプロンプトに既存著作物、作家名、作品の名称などを入力しないようにしてください。

AI 生成サービスの生成物を利用（外部に配信・アップロード・販売など他人に享受させることを目的とする場合）には、その AI 生成物が既存の著作物に類似しないか調査してください。

AI 生成サービスの生成物を自己利用のみに利用する限りは著作権侵害には基本的に該当しませんが、AI 生成サービスの利用自体が著作権者の利益を不当に害する場合には著作権侵害に該当する場合もあり得ますので留意してください。

３．商標権・意匠権侵害に関するルール・規定

OpenAI の Dall-E のような画像生成 AI サービスを利用して生成した画像や、ChatGPT のような文章生成 AI サービスを利用して生成したキャッチコピーなどを商品ロゴや広告宣伝などに使う行為は、他者が権利を持っている登録商標権や登録意匠権を侵害する可能性があります[5]。そこで、生成物が既存著作物に類似しないかの調査に加えて、登録商標・登録意匠の調査を行うように事業会社の社内ルールで定めることが考えられます。

第３．ChatGPT の回答の正確性のリスクと事業会社における取扱い

１．ChatGPT の回答の正確性のリスク

ChatGPT は、OpenAI が開発した自然言語処理の AI で、訓練データとして与えられた情報を基に人工知能が自動的に回答を生成します。しかし、訓練データには時折誤った情報が含まれることもあり、それが反映されることがあります。また、情報が古くなっている

[5] 「生成 AI の利用ガイドライン【簡易解説付】」参照。

場合や、訓練データにバイアスが含まれている場合があるため、回答が完全に正確でなく、虚偽が含まれる場合があることが報告されています。

２．事業会社における取扱い・規定例

上記１のとおり、ChatGPT の回答の正確性や信頼性には限界があります。したがって、ChatGPT の回答は一般的な参考情報として使用することが推奨され、重要な判断や意思決定を行う際には、より信頼性の高い専門的な情報源を確認する必要があることを周知する必要があります。

正確でない回答や虚偽の回答を利用（外部への配信や回答）することによって、相手方に損害が生じた場合には不法行為に該当する可能性があります。正確でない特定の個人に関する回答は不適正な個人情報の利用（個人情報保護法 19 条）や不適正な個人情報の取得（同法 20 条）に該当したり、当該個人の名誉棄損に該当する場合もありうることも周知するのがよいでしょう。

事業会社の社内規程・社内ルールの規定例としては以下のような規定が考えられます。

（規定例）

文章生成 AI サービスの回答には、正確性や信頼性に限界があります。したがって、生成 AI サービスの回答は一般的な参考情報として使用することが推奨され、重要な判断や意思決定を行う際には、より信頼性の高い専門的な情報源を確認する必要があります。

正確でない回答や虚偽の回答を利用（外部への配信や回答）することによって、相手方に損害が生じた場合には不法行為に該当する可能性があります。また、正確でない特定の個人に関する回答は不適正な個人情報の利用（個人情報保護法 19 条）や不適正な個人情報の取得（同法 20 条）に該当したり、当該個人の名誉棄損に該当する場合もあり得ます。

このような場合に該当しないように生成 AI サービスの利用については慎重に行ってください。

第４．利用ポリシーによる利用制限と事業会社における取扱い

OpenAI の利用ポリシー（Usage Policy）[6]においては、以下の目的での利用を禁止しています。

- 違法行為
- 児童の性的虐待素材、または児童を搾取または危害を加えるコンテンツ
- 憎悪、嫌がらせ、暴力的なコンテンツの生成
- マルウェアの生成
- 身体的危害のリスクが高い活動
- 経済的損害のリスクが高い活動
- 詐欺的または欺瞞的な活動:
- アダルト コンテンツ、アダルト 業界、出会い系アプリ
- 政治運動またはロビー活動:
- 利用者のプライバシーを侵害する行為
- 許可されていない法律実務に従事すること、または資格のある人が情報を精査せずに

[6] https://openai.com/policies/usage-policies

カスタマイズされた法的アドバイスを提供すること
- 資格のない者が情報を確認せずにカスタマイズされた財務アドバイスを提供すること
- 特定の健康状態を持っている、または持っていないことを誰かに伝えたり、健康状態を治癒または治療する方法について指示を提供したりすること
- リスクの高い政府の意思決定

事業会社の社内規程・社内ルールにおいては、OpenAI の利用ポリシー上禁止されている行為について禁止することが考えられます。

事業会社の社内規程・社内ルールの規定例としては以下のような規定が考えられます。

（規定例）

AI 生成サービスを利用する場合には、当該サービス提供者の利用規約や利用ポリシーで禁止されている事項に利用することはしないでください。