生成 AI の利用ガイドライン【簡易解説付】

第１.1 版（2023 年 10 月公開）

【2023 年５月１日】制定

【2023 年 10 月 6 日】改訂

＜前文＞

本ガイドラインは、民間企業や各種組織が生成 AI を利用する場合に組織内のガイドラインとして最低限定めておいた方がよいと思われる事項を参考として示したものです。

利用する生成 AI の内容や組織の性質、業務内容等によって、各組織が、本ガイドラインを参考にしていただき、各組織内で定めている既存のデータポリシー等と整合性を取るなど、加筆修正を行って使うためのひな型として提供するものです。本ガイドライン中の【】内は適宜改変してください。

独自のガイドラインを作成する際には、別途公開されている「生成 AI 利用ガイドライン作成のための手引き」を参考にしてください。

1　本ガイドラインの目的

本ガイドラインは、みなさんが【（例）会社】の業務で【（例）ChatGPT】などの生成 AI を利用する際に注意すべき事項を解説したものです。

生成 AI は、業務効率の改善や新しいアイデア出しなどに役立つ反面、入力するデータの内容や生成物の利用方法によっては法令に違反したり、他者の権利を侵害したりする可能性があります。本ガイドラインをよく読んでいただき、生成 AI を上手に利用してください。

2　本ガイドラインが対象とする生成 AI

本ガイドラインが対象とする生成 AI は【OpenAI 社が提供する ChatGPT】です。それ以外の生成 AI の利用を希望する場合には【セキュリティ部門】にお問い合わせください。

【解説】

生成 AI は当該 AI サービスの構造や処理内容によって法的リスクが異なります。そのため、業務のために生成 AI の利用を許可する場合には、ホワイトリスト方式（利用してよいサービスを特定した上で列挙する方式）で指定することをお勧めします。

また、組織内の問い合わせ先は体制構築の経営/業務方針、リスクマネジメント管理体制によってセキュリティ部門の他、法務部門や経営層等、さらには複数部門の連携が必要になることもあります。既存のデータポリシー等の整備状況も踏まえて各組織にてご検討ください。

3　生成 AI の利用が禁止される用途

当【社】では以下の用途・業務での生成 AI の利用を禁止します。

【（1）　・・・】

【（2）　・・・】

【解説】

生成 AI を利用する機関によっては、特定の用途での利用を禁止したい場合もあると思われます。その場合は、生成 AI の利用そのものを禁止する場合と、生成 AI「のみ」を用いて出力された生成物を禁止対象とするのか、明示するとよいでしょう。

たとえば、東京大学が 2023 年 4 月 3 日に公表した「生成系 AI(ChatGPT, BingAI, Bard, Midjourney, Stable Diffusion 等)について」においては「本学では学位やレポートについては

、学生本人が作成することを前提としておりますので、生成系 AI のみを用いてこれらを作成することはできません。」とされています。

　そのような場合は、ガイドラインにおいて一定の用途での利用を禁止することが考えられます。

4　本ガイドラインの構成

生成 AI は、いずれのサービスも基本的に「ユーザが何らかのデータを入力して何らかの処理（保管、解析、生成、学習、再提供等）が行われ、その結果（生成物）を得る」という構造です。

そのため、本ガイドラインは以下の 2 つのパートから構成されています。

▼　データ入力に際して注意すべき事項

▼　生成物を利用するに際して注意すべき事項

5　データ入力に際して注意すべき事項

生成 AI に入力（送信）するデータは多種多様なものが含まれますが、知的財産権の処理の必要性や法規制の遵守という観点からは、以下の類型のデータを入力する場合、特に注意が必要です。

（1）　第三者が著作権を有しているデータ（他人が作成した文章等）

　単に生成 AI に他人の著作物を入力するだけの行為は原則として著作権侵害に該当しません。

もっとも、当該入力対象となった他人の著作物と同一・類似する AI 生成物を生成する目的がある場合には、入力行為自体が著作権侵害になる可能性があります。

また、生成されたデータが入力したデータや既存のデータ（著作物）と同一・類似している場合は、当該生成物の利用が当該著作物の著作権侵害になる可能性もありますので注意してください。具体的には「6（2）生成物を利用する行為が誰かの既存の権利を侵害する可能性がある」の部分を参照してください。

また、ファインチューニングによる独自モデルの作成や、いわゆるプロンプトエンジニアリングのために他者著作物を利用することについても原則として著作権侵害に該当しないと考えられます。

【解説】

単に生成 AI に他人の著作物を入力するだけの行為は、原則として著作権法 30 条の 4 の「情報解析」「非享受利用」に該当すると思われますので、著作権侵害のリスクはかなり低いと思われます。もっとも、当該入力対象となった他人の著作物と同一・類似する AI 生成物を生成する目的がある場合には、「享受目的」が併存しているとして、著作権法 30 条の 4 が適用されず入力行為自体が著作権侵害になる可能性があります。

また、ユーザがファインチューニングによる独自モデル作成に際して他者著作物を利用する行為についても同様の理由で著作権侵害のリスクは低いでしょう。

さらに、いわゆるプロンプトエンジニアリングのために、ユーザが自社サーバ内や生成 AI サービス事業者のサーバ内に他人の著作物を蓄積する行為を行うことも考えられます。

プロンプトエンジニアリングとは、具体的には、生成 AI においてより精度の高い出力を生成させるために、ユーザの入力（プロンプト）を補完したり加工したりする行為をいいます。したがって、プロンプトエンジニアリングのための著作物蓄積行為は、生成 AI における出力生成の前提としての解析（「情報解析」）に「必要と認められる限度 」の行為として、著作権法 30 条の 4 により適法ではないかと考えられます。

ただし「必要と認められる限度 」でしか利用は認められませんので、たとえば「プロンプトエンジニアリングのためにサーバ内に他人の著作物を蓄積」しつつ、同時に「当該著作物をデータベース化して人間が参照したり読んだりすることができる」のであれば「必要と認められる限度」を超えていますので、30 条の 4 は適用されず著作権侵害に該当すると思われます。

（2）　登録商標・意匠（ロゴやデザイン）

商標や意匠として登録されているロゴ・デザイン等を生成 AI に入力することは商標権侵害や意匠権侵害に該当しません。

もっとも、この点は著作物と同様、あくまで「入力行為」に関するものである点に注意が必要です。故意に、あるいは偶然生成された、他者の登録商標・意匠と同一・類似の商標・意匠を商用利用する行為は商標権侵害や意匠権侵害に該当します。

すなわち、生成 AI にロゴやデザインを入力する際には登録商標・意匠の調査の必要性は乏しいですが、生成物を利用する場合には調査が必要です。

（3）　著名人の顔写真や氏名

著名人の顔写真や氏名を生成 AI に入力する行為は、当該著名人が有しているパブリシティ権の侵害には該当しません。

ただし、生成 AI を利用して生成物された著名人の氏名、肖像等については、それらの氏名や肖像等を商用利用する行為はパブリシティ権侵害に該当しますので注意してください。

（4）　個人情報

【ChatGPT】においては入力したデータが【OpenAI 社】のモデルの学習に利用されることになっていますので、【ChatGPT】に個人情報（顧客氏名・住所等）を入力する場合、当該個人情報により特定される本人の同意を取得する必要があります。そのような同意取得は現実的ではありませんので、個人情報を入力しないでください。

【ただし、利用する生成 AI によっては、特定の条件を満たせば個人情報の入力が適法になる可能性もあります。詳細は【セキュリティ部門】にお問い合わせください。】

【解説】

個人情報（個人データ）を生成 AI に入力する行為が適法か否かは、当該生成 AI 内でのデータの取扱いや、当該生成 AI サービス提供者が外国にある事業者なのかによっても結論が分かれ、非常に複雑です。たとえば、WEB 版の ChatGPT においてはデータ管理機能の追加により、対話履歴をオフに設定することで、学習に使われないようユーザが管理できるようになっていますが、OpenAI 社は外国の第三者であるため、個人情報保護法上、あらかじめ本人の同意を得ることなく個人データの入力はできない可能性があります。

そのため本ガイドラインでは一律個人情報の入力を禁止することにしています。

一方で、OpenAI の API や、Azure OpenAI サービスを利用する場合には個人情報保護法上の規制をクリアできる場合もあります。そのため【ただし、利用する生成 AI によっては、特定の条件を満たせば個人情報の入力が適法になる可能性もあります。詳細は【セキュリティ部門】にお問い合わせください。】と記載しています。実際には約款等の調査が必要になるため、法務部門との連携が必要になってくると思われます。

なお、2023 年 6 月 2 日に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」が公表されています。同注意喚起別添１においては「（１） 個人情報取扱事業者における注意点」として以下の記載がなされています。

「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。」

当該注意喚起をどのように読むのか（入力された個人データが応答結果の出力生成の目的のみで取り扱われる場合は個人データの「提供」に該当しないのではないか等）は様々な意見があるところですが、少なくとも、あらかじめ本人の同意を得ることなく入力された個人データが、生成 AI サービス提供者において機械学習に利用される場合は、当該入力行為が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点に留意する必要があります。

（5）　他社から秘密保持義務を課されて開示された秘密情報

外部事業者が提供する生成 AI に、他社との間で秘密保持契約（NDA）などを締結して取得した秘密情報を入力する行為は、生成 AI 提供者という「第三者」に秘密情報を「開示」することになるため、NDA に反する可能性があります。

そのため、そのような秘密情報は入力しないでください。

【解説】

①生成 AI 提供者が入力データに監視目的での限定されたアクセスしかしない、あるいは一切アクセス・保存しない場合において、②組織が秘密情報の利用目的として定められている目的のために生成 AI に秘密情報を入力（プロンプトエンジニアリングのために利用することも含む）して分析・生成する行為については、NDA に違反しないでしょう。一方、大規模言語モデル（LLM）の多くは入力データが学習に利用されますので、NDA 違反を構成する可能性が高いと思われます。

また、NDA の解釈によっては第三者の管理下に置くこと、たとえば、GCP や AWS といったクラウドサービス上にデータを置くこと自体が違反とされるケースも見受けられます。そのため、本ガイドラインでは一律入力を禁止しています。

（6）　自組織の機密情報

自【社】内の機密情報（ノウハウ等）を生成 AI に入力する行為は何らかの法令に違反するということはありませんが、生成 AI の処理内容や規約の内容によっては当該機密情報が法律上保護されなくなったり特許出願ができなくなったりしてしまうリスクがありますので、入力しないでください。

6　生成物を利用するに際して注意すべき事項

（1）生成物の内容に虚偽が含まれている可能性がある

大規模言語モデル（LLM）の原理は、「ある単語の次に用いられる可能性が確率的に最も高い単語」を出力することで、もっともらしい文章を作成していくものです。書かれている内容には虚偽が含まれている可能性があります。

生成 AI のこのような限界を知り、その生成物の内容を盲信せず、必ず根拠や裏付けを自ら確認するようにしてください。

（2）生成物を利用する行為が誰かの既存の権利を侵害する可能性がある

① 著作権侵害

生成 AI を利用して出力された生成物が、既存の著作物と同一・類似している場合は、当該生成物を利用（複製や配信等）する行為が著作権侵害に該当する可能性があります。

そのため、以下の留意事項を遵守してください。

・ 特定の作者や作家の作品のみを学習させた特化型 AI は利用しないでください。

・ プロンプトに既存著作物、作家名、作品の名称を入力しないようにしてください。

・ 特に生成物を「利用」（配信・公開等）する場合には、生成物が既存著作物に類似しないかの調査や生成物の利用が権利制限規定（著作権法 30 条 1 項や同 30 条の 3 等）に該当するかの検討を行うようにしてください。

② 商標権・意匠権侵害

画像生成 AI を利用して生成した画像や、文章生成 AI 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ので、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してください。

③ 虚偽の個人情報・名誉毀損等

【ChatGPT】などは、個人に関する虚偽の情報を生成する可能性があることが知られています。虚偽の個人情報を生成して利用・提供する行為は、個人情報保護法違反（法 19 条、20 条違反）や、名誉毀損・信用毀損に該当する可能性がありますので、そのような行為は行わないでください。

【解説】

生成 AI からの生成物が既存の著作物と同一・類似している場合は、当該生成物を利用（複製や配信等）する行為が著作権侵害に該当する可能性があります。

もっとも、どのような場合に著作権侵害に該当するかは明確な基準が存在しない状況です。

そこで、本ガイドラインでは保守的に考え、著作権侵害に繋がる可能性のある行為（「特定の作者や作家の作品のみを学習させた特化型 AI を利用する行為」「プロンプトに既存著作物、作家名、作品の名称を入力する行為」）を禁止し、生成物を配信・公開等する場合には、生成物が既存著作物に類似しないかの調査を行うよう義務づけています。

（3）生成物について著作権が発生しない可能性がある

仮に生成物に著作権が発生していないとすると、当該生成物は基本的に第三者に模倣され放題ということになりますので、自らの創作物として権利の保護を必要とする個人や組織にとっては大きな問題となります。

この論点については、生成 AI を利用しての創作活動に人間の「創作的寄与」があるか否かによって結論が分かれますので、生成物をそのまま利用することは極力避け、できるだけ加筆・修正するようにしてください。

【解説】

① 画像生成 AI の場合

画像生成 AI の場合であれば、自動生成された画像に人間がさらに加筆・修正をした場合などは「創作的寄与」があるとして、それらの行為を行った人間を著作者として著作権が発生することになるでしょう。

一方、①詳細かつ長いプロンプトを入力して画像を生成した場合、②プロンプト自体の長さや構成要素を複数回試行錯誤する場合、③同じプロンプトを何度も入力して複数の画像を生成し、その中から好みの画像をピックアップする場合などに「創作的寄与」があるとして著作権が発生するかについては議論が分かれるところです。

② 文章生成 AI の場合

ChatGPT のような文章生成 AI には様々な用途がありますが、文章生成 AI のユーザ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の創作意図と創作的寄与は通常はありませんので、文章生成 AI による出力テキストには著作権は発生しないということになるでしょう。

文章生成 AI から、よりよい出力を引き出すために、質問（入力）の仕方のヒントやプロンプト文例がたくさん公開されていますが、ユーザが質問をするにあたってそれらの文例を駆使したとしても、出力テキストに対するユーザの創作意図と創作的寄与が認められることはないように思います。

したがって、ユーザが文章生成 AI に指示をして、何らかのリサーチ結果、アイデアや回答を得た場合、それらの出力には著作権が発生しない、ということになりそうです。

（4） 生成物を商用利用できない可能性がある

生成 AI により生成した生成物をビジネスで利用する場合、当該生成物を商用利用できるかが問題となります。

この論点は、利用する生成 AI の利用規約により結論が左右されますが、【ChatGPT の場合、生成物の利用に制限がないことが利用規約に明記されているので、この点は問題になりません。】

【解説】

本ガイドラインでは ChatGPT を主たる例に挙げて言及していますが、たとえば、画像生成 AI である Midjourney の場合、無料会員が生成した画像に関する権利はいったん無料会員に帰属した後、Midjourney に当該権利が移転し、その上で、Midjourney は、当該 AI 生成物を創作した無料会員に対して、CC4.0NC の下、ライセンスをすることになっています。

つまり、無料会員は当該 AI 生成物を商用利用することはできません。

（5）生成 AI のポリシー上の制限に注意する

生成 AI においては、これまで説明してきたリスク（主として法令上の制限）以外にも、サービスのポリシー上独自の制限を設けていることがあります。

【　ChatGPT を利用する場合、以下の点に注意してください。

Usage Policies（https://openai.com/policies/usage-policies）で、「Adult content, adult industries, and dating apps（アダルトコンテンツ、アダルト産業、出会い系アプリ）」「Engaging in the unauthorized practice of law, or offering tailored legal advice without a qualified person reviewing the information（許可なく法律実務を行うこと、または資格のある人が情報をレビューしないままに特定の法的助言を提供すること）」などの具体的禁止項目が定められています。

また、医療、金融、法律業界、ニュース生成、ニュース要約など、消費者向けにコンテンツを作成して提供する場合には、AI が使用されていることとその潜在的な限界を知らせる免責事項をユーザに提供する必要があることも同ポリシーには明記されています。

さらに、関連ポリシー上は、ChatGPT など OpenAI 社のサービスを利用して生成されたコンテンツを公開する際には、AI を利用した生成物であることを明示することなどが定められています。】