

特別記事

敵か、味方か… 「生成AI」による 働き方改革に備えよ



ChatGPTに代表される生成AIによって、事務や法務などの一部が将来自動化されると予測されています。実務担当者の働き方にどのような変化がもたらされるのかを概観したうえで、実務に実装する際の留意点を検証します。

森・濱田松本法律事務所

田中 浩之 パートナー弁護士・ニューヨーク州弁護士

上田 雅大 カウンセル弁護士・ニューヨーク州弁護士

松井 佑樹 アソシエイト弁護士

生成AIは企業の実務にどの程度役立つか

生成AIを利用する際の法的論点

生成AIの実務利用における留意点



生成AIは 企業の実務に どの程度 役立つか

生成AIの 仕組みと特徴

「生成AI」とは、様々な成果物を生成することができるAIの総称です。入力されたデータに対する分析・判断（画像や文章の識別・抽出、パターン検証など）といった従来のAIの利用方法にとどまらず、AI自身が新しいコンテンツを生成できるという点に特徴があります。

生成AIについては、2022年夏にはすでに、文章のプロンプト（指示）を入力すれば、それに

応じた画像を生成する「画像生成AI」のブームが起こっていました。さらに2022年11月に、米オープンAI社が開発・公開した対話型の生成AI「Chat（チャット）GPT」が、全世界で爆発的な普及をしたことで一気に注目が集まりました。

生成AIの種類は、テキストの入力情報からテキスト、画像、動画、音楽、プログラミングコード、3Dモデル等の成果物を生成するものや、逆に音声や動画等の入力情報からテキスト（要約）を生成するものなど、すでに多種多様なものが存在しています（次頁「図表1」）。

その技術の進歩に応じて、今後もありエーシオンが増えていくことが予想されます。1つのAIで、複数のモジュール（入力情報）を処理することができるようになる生成AIも増えています。

生成AIは、「ディープラーニング（深層学習）」という機械学習の手法を用いて訓練された、ニューラルネットワーク（何十億ものニューロンが相互接続された人間の脳の仕組みにたとえて呼ばれるネットワーク）の1つである「基盤モデル」に支えられています。

す。基盤モデルは、一般に、大量のデータを取り込み、そのデータからパターンと相関関係を事前に学習することができます。

対話型生成AIであるチャットGPTに用いられている、大規模言語モデルであるLLM（Large Language Models）も基盤モデルの1つですが、これもインターネット等から収集した大量かつ多様なテキストデータを学習し、文章の次に来る確率の高い単語を予測できるように学習させています。

つまり、チャットGPTのような大規模言語モデルを組み込んだ対話型生成AIは、ユーザーが入力したプロンプトに応じて、自然と思われる言葉を数珠つなぎのようにつなげていくことにより、プロンプトに対する応答が成り立つようになっていきます。

人間のように一定の感情や主義・思想をもって会話をしているわけでも、あらかじめ用意された大量の問いと答えのデータベースから答えを引き出しているというわけでもありません。

ただし、常に確率が最も高い言葉を並べるだけでは、出力結果の創造性・柔軟性が下がるため、あって確率はそこまで高くなっても

適切な言葉を続けている場合もあると思われます。

実際に、チャットGPTやグーグル社の生成AIであるBardに、まったく同じプロンプトを複数回入力したとしても、一言一句同じ出力結果が出力されるわけではなく、毎回、異なる応答が出力されます。

生成AIの 弱点

対話型生成AIが、このような仕組みで文章を生成している以上、時折、入力したプロンプトに対して一見正しいように見えて誤っている応答をすること（「ハルシネーション（幻覚）」といいます）は、よく理解しておかなければなりません。

また、大量のデータを取り込み、そのデータからパターンと相関関係を事前に学習するという仕組みから、学習時点以降の最新情報を踏まえた応答をすることができないといった限界もあります。

たとえば、チャットGPTのベイスとなつているGPTは、2021年9月時点までの情報しか学習していないことにも気を付ける

図表1 主な生成AI(2023年7月20日現在)

種類	名称	運営会社	URL
対話型AI	ChatGPT	Open AI	https://openai.com/blog/chatgpt
	ChatSonic	Writesonic	https://writesonic.com/chat
	Bard	Google	https://bard.google.com/
画像生成AI	DALL-E 2	Open AI	https://openai.com/product/dall-e-2
	Midjourney	Midjourney	https://www.midjourney.com/
	Stable Diffusion	Stability AI	https://ja.stability.ai/stable-diffusion
コード生成AI	Amazon CodeWhisperer	Amazon	https://aws.amazon.com/jp/codewhisperer/
翻訳AI	Mirai Translator	みらい翻訳	https://miraitranslate.com/service/miraitranslator/
記事作成AI	Catchy	デジタルレシピ	https://lp.ai-copywriter.jp/

必要があります。
なお、この限界については、チャットGPT Plusユーザー向けにGPT-4で、ウェブサイトを上の最新情報を取り込んで出力を行なうWebブラウジング機能が提供されています(本稿執筆時点で一時停止中)。この機能を有効にすることや、プラグインの利用により最新の様々なデータを取

企業の実務における生成AIの利用法

り込むことにより、弱点を補うことができます。

こうした生成AIの仕組みや特徴、限界および後述する様々な留意点に気を付ければ、生成AIは、多様な成果物の生成を短時間で

人間が長時間をかけて行なってきた作業の負担を、大幅に軽減できる便利なツールとして、様々な業務の効率化・コスト削減に大きな力を発揮してくれるでしょう。生成AIの実務における利用にも関心が高まっています。

業務が効率化された結果、まだ生成AIに任せるには難しい、付加価値があり複雑度の高いタスクに人間が時間を割くことができるという意味では、新たな「働き方改革」であるとも表現できます。

一般的には、対話型生成AIだけでなく、場面に応じた適当な文章の生成、情報収集、文章の要約・ブラッシュアップ、言語翻訳などの作業に役立てられるといわれています。実際に業務に利用している企業も増えています。

そのほか、生成AIを使うことにより、顧客対応、マーケティング、営業、研究開発といったあらゆる業務を効率化する余地があるといえます。

それぞれの業務におけるユースケースについて、例を挙げて具体的に検討してみましょう。

① 顧客対応

対話型生成AIを利用して、顧客からの問い合わせメールに対する適切な返信メールを作成すること等が可能と考えられます。

さらに進んで、対話型生成AIを利用したチャットボットを構築し、顧客対応を自動化することも考えられるでしょう。

ただし、対話型生成AIを精度の高いチャットボットとして利用するためには、自社独自の資料を回答の前提として取り込む「プロンプト・エンジニアリング(プロンプト・デザイン)」の手法を用いることや、自社独自の資料による特定の学習用データセットによる「ファインチューニング(基盤モデルの微調整)」を行なうといった高度な工夫が必要になると考えられます。

まずはできるところから少しずつ

つ、利用の範囲を考えていくべきだと思われます。

② マーケティング

商品の名前・見出し・キャッチコピーや広告(画像)を、対話型生成AIや画像生成AIを用いて生成・検討したり、特定の顧客層のデータについての分析・予測をさせることも考えられます。

様々なデータを学習している対話型生成AIを「壁打ち」の相手に使い、思考整理や新規事業のアイディア創出のために用いることもできそうです。

その際には後述する法的リスクも鑑みて、社外秘にあたるようなデータをプロンプト化しないような仕組みも必要になるでしょう。

③ 営業

テキストを、スライドや図表に変換・作成する生成AIを利用すれば、プレゼン資料作成などの業務効率化を図ることができます。

正確性を慎重に確認する必要がありますが、資料の翻訳・多言語化に生成AIを利用すれば、翻訳に必要な費用・時間を大幅に削減できます。

校正に手がかかっても、一から

翻訳することに比べれば、手間は半減するのではないでしょうか。

④ 研究開発

アプリ開発に関していえば、生成AIを用いてプログラミングコードの作成やレビューを行なうことが考えられます。

作成したコードを走らせ、問題のある点を発見、修正させることも可能です。販売するソフトに使用しないまでも、社内で使用する簡単なアプリなどは、自社開発が可能でしょう。

また生成AIに、自社独自のチューニングを行なうことで、創業などの研究開発の加速・効率化を図ることもできるでしょう。

生成AI利用時に 有益な手法

ここまで例として挙げたどのケースにおいても、自社の企業価値やポリシーを反映するためには、前述したプロンプト・エンジニアリング（プロンプト・デザイン）の手法やファインチューニング（基盤モデルの微調整）を行なう等の工夫が重要になってきます。しかし、ファインチューニング

は成功すれば大きな効果を得られますが、一般に多額のコストがかかる場合がほとんどです。

またチューニングを進め過ぎると、元のモデルのよさが失われ、精度が下がることもあるので、資金的に余裕のない中小企業には、あまりお勧めできません。

プロンプト・エンジニアリングについては、ファインチューニングに比べると比較的手軽に行なうことができるといえます。

プロンプト・エンジニアリングとは、生成AIが期待に沿った成果物を出力するように、プロンプトを設計、改良、最適化することです。自社独自のデータを、回答の前提としてプロンプトに取り込んで、回答の精度を上げることも1つの方法です。

一方、データの取込みをせずに、入力するプロンプトに工夫を加える方法も考えられます。

たとえば、対話型生成AIについていえば、漠然としたプロンプトでは期待どおりの成果物が出力されない場合でも、できるだけ具体的かつ詳細に定義するようなプロンプトを入力することにより、より適切な出力結果を得ることができます。

画像生成AIについても、期待に沿った画像の成果物を得るためには、プロンプトの内容が非常に重要になってきます。そのようなプロンプト作成のノウハウや、プロンプトの情報自体を有償で提供している事例も見られます。

今後、企業の実務に生成AIを導入していくのであれば、このようなプロンプト・エンジニアリングのスキルがますます重要になってくるでしょう。早い段階から、各従業員に対しプロンプト・エンジニアリングについて基礎的な研修を行ない、エキスパートを育成していくことが有益です。

中小企業において、生成AIの利用を積極的に進めていくためには、各部署・従業員において個別的・属人的に取り組むのではなく、組織として慎重かつ協調的に対応していくことが求められるでしょう。

具体的には、マーケティング、営業、エンジニアリング、法務などの各部門に横断的なチームを立ち上げ、一丸となって対応することが考えられます。

全社的な体制を整えることにより、自社において生成AIを導入するうえで最も付加価値の高いユ

ースケースが見えると思われるます。社内での有益なプロンプトの作成法の情報が集積され、同時により適切かつ具体的な社内の利用ルールの作成・見直し等にも有益でしょう。

生成AIを 利用する際の 法的論点



チャットGPT等の生成AIを利用するにあたって、注意が必要な法律上の問題は、

- データの入力段階の論点
 - 成果物の出力段階の論点
- の2つに大きく分けられます。

また、ビジネスに利用しようと考える場合、生成AIの利用規約や、分野によっては業法等との関

係にも留意する必要があります。

データの入力段階の論点

生成AIに個人情報を入力することについて、自社が公表等している個人情報の利用目的と適合しているのか、個人データを第三者に提供するにあたっての個人情報保護法上の規制に適合しているのか等が論点になります。

データ入力の前提となる、インターネットからの大量の情報の収集段階において、犯罪歴や病歴等の要配慮個人情報が含まれてしまう、という問題への対応も留意すべき点となります。

また、自己の営業秘密（機密情報）や、第三者と秘密とすることを約束して管理している営業秘密（機密情報）等を生成AIに入力することにより、自己の営業秘密としての保護が失われてしまったり、第三者との機密保持義務違反の責任を問われないようにするための法的対応が必要になります。

このほか、他人が著作権を持つ著作物を、生成AIに情報として入力することについては、著作権法との関係が論点になります。

自社で独自に工夫したプロンプト自体を、著作権その他の知的財産権で保護することができるといふ点も論点になります。

成果物の出力段階の論点

個人情報保護法やプライバシー権との関係では、生成AIが出力した個人に関する情報について、生成AIの利用者と生成AIの提供者事業者は、それぞれについてどのような責任を負うべきかが問題となります。

著作権法との関係では、生成AIにより生成されたコンテンツが、他人の著作物に類似していた場合、著作権侵害になるかどうかの判断基準も論点となります。

生成AIによる成果物に著作権がそもそも発生するかどうか、発生するとして誰に発生するのかも論点になるでしょう。

また、画像生成AIの場合には、生成される肖像について、肖像権や、生成AIにより芸能人等の有名人そっくりの肖像等が生成された場合に、知的財産権の1つであるパブリシティ権の侵害になるかが論点になります。

このほか、生成AIが不正確な情報を出力した場合に、その責任が生成AIの利用者と生成AIの提供者事業者のどちらに生じるのかなどということも論点になるでしょう。

営業秘密（機密情報）の管理との関係で、プロンプトとして入力した営業秘密（機密情報）が、他人の入力したプロンプトに対する出力結果として出力されてしまう可能性、および発生してしまった場合の実務上の対応も考える必要があります。

まだ実際に法的に問題となったケースが少ないため、今後の指針等の制定が待たれるところです。

営業秘密（機密情報）に関しては、後述します。

利用規約や業法等との関係など

生成AIの利用にあたっては、生成AIの提供者事業者が定めた利用規約などを遵守する必要があります。

たとえば、チャットGPTの場合、一般的なルールとして、「利用規約（Terms of use）」が存在しているほか、「利用ポリシー

（Usage policies）」で用途の制限が定められています。

「共有と公開のポリシー（Sharing & publication policy）」では、利用時における表示の規制（AI成果物であることを示すことや、人間とAIの合作である場合に、100% AIや人間が作成したものと誤解を与えるような表示をせず、その役割を説明すること）等が要求されています。

さらに、「ブランド指針（Brand guidelines）」も定められているため、これらに違反が生じないように留意が必要です。

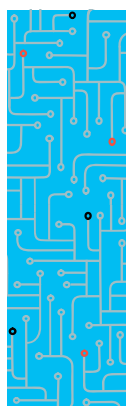
そのほか、一般的には成果物の商用利用が禁止されているケースや、成果物について他人への権利行使が制限されているケースも多いため、生成AIによる成果物の販売等を考えている企業は、特に留意が必要です。

また、免許・資格等が必要な特定の業種の業務を自動化するような生成AIを開発し、また有償で提供する場合には、業法との抵触等も問題となります。

さらに、免許・資格等が必要な事業者が、生成AIによるサービスを提供する場合にも、業法で禁止されるような行為を行わない

ように注意が必要です。
たとえば、金融商品取引法では、顧客に対し、不確実な事項について確実であると誤解させるおそれのあることを告げて、金融商品取引契約の締結の勧誘をする行為が禁止されています。生成AIによるチャットボットが、このような発言をしないように設計しておくことが必要となります。

生成AIの実務利用における留意点



生成AI利用のための社内ルールを策定する

生成AIの社内での利用を検討

している場合には、社内ルール（ガイドライン）を定めることが有益です。

策定にあたっては、たとえば日本ディープラーニング協会が、生成AIの利用ガイドラインのひな形を無料で公開しています。

社内ルールについては、完璧を求めるあまりになかなか決められないという問題が生じることがありますが、利用する生成AIサービスの態様や規約の変化、実務の進展等を踏まえて適宜改訂すればよいため、まずは、抽象的な最低限のものでも導入することが大切です。

具体的なルールを定めるのなら、社内ですべて利用する具体的な生成AIと、その利用場面を特定する必要があります。複数の生成AIサービスを利用する場合には、サービスごとの具体的なルールを定めることも一案です。

社内ルールの策定にあたっては、まずは生成AIの利用目的を明確に定めることが重要です。業務との関係で、生成AIをどのような場面・用途で使うかを明確化することで、方向性が定まり、生成AIの利用を禁止すべき行為と許容される行為を、合理的に特定

することができず。

なお、利用を禁止すべき行為と許容される行為を検討する際には、禁止と許可の2区分に固執する必要はなく、個別承認事項を設けることも考えられます。

また、全社で統一されたルールを作成しなければいけないということはありません。利用する目的に応じて、たとえば、研究開発部門用の特別ルールを設けるなど、部署ごとに異なるルール・特則を設けることも1つの選択肢です。

社内ルールにおける営業秘密（機密情報）保持

社内ルールの策定にあたっても、前述したデータの入力段階の論点と、成果物の出力段階の論点を考慮する必要があります。

企業での利用を想定した場合、重要な点として、営業秘密（機密情報）の入力におけるルールの策定が挙げられます。

利用する生成AIの利用規約において、入力された情報の機密保持が規定されていない場合はもちろんですが、忘れてはならないのが、生成AIに入力した情報については、生成AIサービス提供事

業者により、利用される可能性があることです。

生成AIサービス提供事業者も、営業秘密（機密情報）を管理する企業にとつては第三者です。生成AIサービス提供事業者は、

入力された営業秘密（機密情報）を使い、開示した企業へ成果物を提供する以外にも、他社に向けての成果物へ活用できます。

営業秘密（機密情報）の利用の範囲を開示した企業がコントロールできない以上、法的にみて、営業秘密該当性の喪失の危険性があります。

また、入力した営業秘密（機密情報）が機械学習に使われ、他人が入力したプロンプトに対する成果物として出力されてしまった場合には、実際に他人に営業秘密（機密情報）が使われてしまう可能性もあり、注意が必要です。

自社の営業秘密や機密情報については、生成AIサービス提供者との規約等で機密保持に関する定めがあるのか等をチェックすることが必要です。疑義がある場合には、営業秘密や機密情報を入力しないように、社内ルールを策定する必要があります。

特に、他社から秘密保持義務を

課されて開示された機密情報の入力には、細心の注意が必要です。

一般的に、機密情報のやり取りを行なう際には、会社間で秘密保持契約、いわゆるNDA (Non-Disclosure Agreement) を締結していると思われます。

NDAでは、自社や契約相手の機密情報の利用や、開示の対象が限定され、それ以外の情報の利用・開示は契約違反として損害賠償等の対象となっており、機密情報の漏洩が起きないよう手当がなされています。

第三者との間のNDAにおいて、委託先への開示は、委託先に同等のNDAを課せば可能と設定しているケースもありますが、明記されていない場合のほうが多いと思われます。

この場合には、第三者から開示を受けている機密情報を生成AIに入力することが、第三者とのNDA違反にならないのかの問題が生じ、個別のNDAのチェックが必要になります。

生成AIの普及を見据えて、今後は、NDAにおいて生成AIへの情報の入力許可、不許可を明示的に定め、社内ルールにも明示しておくことで疑義をなくすること

も必要となるでしょう。

このように、営業秘密（機密情報）に関する件など法的な論点を含む複雑なルールを、すべて現場の一従業員が社内ルールを見て判断するのは難しいでしょう。

不明点がある場合には、気軽に相談できるような窓口を案内しておくことも有益です。

これに加えて、問題事例を今後の社内ルールに反映させるために、違反（のおそれ）がある場合に通報・相談できる窓口を設けることも有益です。

また、ルールを作成するのみならず、自社の利用が適切な事例と不適切な事例等のケーススタディを含めて、生成AIの利用を促進しつつ、社内ルールを周知するための研修を行なうことも重要になります。

以上の留意点について、生成AIに関する簡潔な社内ルールの例を、**図表2**にまとめました。限られた紙幅での一例であることはご了承ください。

生成AIの成果物に関する留意点

生成AIを利用する際の留意点

として、生成AIから出力される内容に、

- 事実と異なるもの
- 名誉毀損等になるようなもの
- 不適切な差別発言
- 他者の著作権を侵害するものなどが含まれるケースが挙げられます。

前述したとおり、チャットGPTなどの対話型AIなど、一般的な大規模言語モデルにおいて、生成AIが成果物を生成するプロセスは、入力されたプロンプトに続けるのに適した応答となるように、数珠つなぎのように次に続く言葉として、確率が高いと考えられる応答を出力しているというものに過ぎません。

したがって、生成AIは前述したように、堂々と嘘をつく（真実と異なった応答を行なう）可能性や、名誉毀損的表現、差別的な表現等、不適切な応答を行なう可能性があります。

この点については、生成AIが生成したものを鵜呑みにしてはいけない、ということを教育することが重要です。AIの成果物に対しては、完璧なものとは決して考えずに、常にチェックする必要があるります。

手間と時間を省いてくれる有能な人間の秘書の仕事であっても、提出されたものはチェックするのと同じです。

不適切な応答を避けるためには、プロンプトを制御して、問題発言が引き出されるようなプロンプトの入力自体を制限する仕組みを導入する方法もあります。

あるいは、AIに対して強化学習を行うことにより、出力段階でこうした内容が出力されないようにコントロールすることが考えられます。

しかしこういった方法、特に強化学習のような方法は、一般的な利用企業レベルでは限界があるかと思われれます。

前者・後者のいずれの方法も、結局のところ万全とはいえませんが、生成AIを社内で活用しようとする企業では、信頼されるサービスの提供のためにはまだ人間によるチェックが求められます。

変化するサービス・規制等への対応

チャットGPTのサービス提供開始を皮切りに、生成AIに対する注目は世界規模で日増しに強ま

図表2 生成AI利用の社内ルール例

第1条 社内ルールの適用範囲・生成AI利用の目的・用途等

1 本社内ルールは、別紙所定の当社において利用が許可された生成AI(以下「生成AI」という)の利用に対して適用される。

生成AIの利用にあたっては、当該生成AIの利用規約を遵守する。

また、当社においては、別紙所定のもの以外は利用が禁止されており、許可を求める場合には、第5条所定の相談窓口にご相談する。

2 当社は、生成AIを、別紙所定の目的・用途に限って利用する。

別紙所定の目的・用途以外には利用できない。

【社内で利用を許可する生成AIを特定して、適用範囲を定め、生成AIの利用目的・用途を定める必要があります。社内で利用を許す生成AIは商用利用が許されたものに限りがあります】

第2条 生成AIへの入力情報

生成AIに対しては、以下の情報を入力してはならない。ただし、営業上の重要な必要性から入力することが必要な場合には、第5条所定の相談窓口の事前承諾のもと、これを入力することができる。

- ① 個人情報
- ② 営業秘密・機密情報(当社の社内秘または極秘情報および第三者との関係で当社が秘密保持義務を負う情報を含む)

【生成AIにデータを入力する際に入力してはならない情報を規定する必要があります。】

また、単純に禁止行為を定めるのみならず、ただし書のように例外的な許可のための個別承認条項を入れることも考えられます】

第3条 出力物の著作権

生成AIの出力物については、当社に著作権が発生しない可能性があることについて十分留意する。また、当該出力物が第三者の著作権を侵害する可能性があることから、第三者の著作権を侵害しないことを事前に確認したうえで利用しなければならず、判断に迷う場合には、第5条所定の相談窓口にご相談する。

【本文で述べた生成AIと著作権についての留意事項を踏まえた定めを入れていきます。他の知的財産権についても定めをおくことが本来有益ですが、紙幅の関係上省略します】

第4条 出力物の正確性

生成AIの出力物には、事実と異なる内容の出力物を出力する可能性があり、出力物を利用する際は、出力物の正確性(根拠を含む)を生成AI以外の方法により確認したうえで利用しなければならない。

【生成AIの出力物において、事実と異なる内容が含まれることを前提に、出力物を利用する際のルールを決めておくことが有用です】

第5条 生成AIに関する窓口の設置

1 当社は、生成AIの利用に関し疑問点等が発生した際の相談窓口として、〇〇部に生成AIに関する相談窓口(以下「相談窓口」という)を設置する。

2 従業員は、生成AIの利用に関し疑問点等が発生した場合には、必要に応じて相談窓口を用いる。

3 従業員は、生成AIの利用に関し、本ルールに違反し、または違反のおそれのある行為を認識した際には、速やかに相談窓口にご相談をする。

【生成AIの利用に関して、会社側から相談窓口を設置することも有効です】

たなかひろゆき
うえだまさひろ
まついゆうき
2007年弁護士登録。
2010年弁護士登録。
2022年弁護士登録。

著書『ChatGPTの法律』(共著)など。
著書『アプリ法務ハンドブック』(共著)など。

っています。チャットGPT以外にも、18¹⁾図表1のように、グーグル社が提供を開始した生成AIサービスの Bard など、次々に各分野や領域に特化した生成AIがリリースされています。

それに伴い、生成AIに関する技術やサービスは、常に変化、変更されています。

サービスの更新に伴って、生成AIの利用に関する利用規約等も修正や追加が加えられる可能性があります。生成AIを利用する企業は、生成AIの技術の変化のみならず、サービス内容の変更も踏まえて、必要に応じて随時対応する必要がありますことに留意してください。

さらに、生成AIが普及するにつれ、国内外でAIに関する法律や、政府のガイドライン等による規制が進む可能性があり、これらの動向を踏まえた対応が求められます。

特にEUでは、2023年6月に、欧州議会で修正案が採択されたAI規則案(本稿の執筆時点では未成立)において、リスクに応じた包括的なAI規制を導入し、生成AIモデル事業者にも重い責任を課しており、注目されます。●