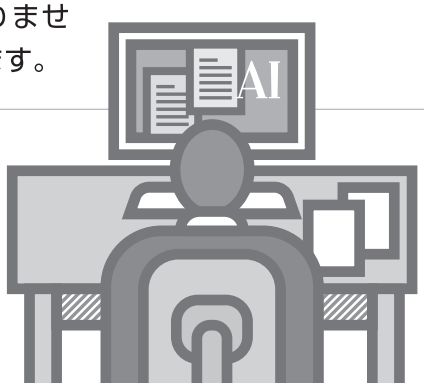
社内文書・議事録作成に
生成AIを利用する際の
社内ルールを整備しよう

社内文書や議事録作成を行なう目的で文章生成AIを利用する場合、秘密情報や著作権などの観点から留意すべきリスクも少なくありません。それらの法的留意点と社内ルール整備のポイントを解説します。



STORIA法律事務所
弁護士
坂　田　晃　祐

本稿では、OpenAI社が提供する「ChatGPT」や、Google社が提供する「Bard」のような、大量のテキストデータで学習を行ない、一定の入力指示（プロンプト）に対して生成物を返すAIモデル（大規模言語モデル、Large Language Model、LLM）を提供するサービスのことを、「文章生成AIサービス」として定義します。

文章生成ＡＩサービスを、様々な形で業務に活用しようとする人が増えています。

たとえば、議事録やＷｅｂページの内容を自動で要約できたり、社内文書の雛形が自動で作成できたりすれば、業務時間が削減でき、より多くのタスクがこなせるようになります。

しかし、文章生成ＡＩサービスを利用するにあたっては、情報を入力する際および生成物を利用する際に生じる法的リスクを理解し、適切なリスク管理を行なう必要があります。

社内にある「情報」を整理しよう

リスク管理の前提として、まずは文章生成ＡＩサービスに入力し得る「情報」の類型を整理することが大切です。一般に、文章生成ＡＩサービスに入力する際のリスク分析に必要な視点は、３つの情報類型に分類されます（**図表１**）。

⑴　秘密情報

社外に開示することが予定されておらず、秘密として保持すべき情報です。秘密情報には、次の２つがあります。

①　自社の秘密情報

②　取引相手とＮＤＡ（秘密保持契約）を締結して開示された情報

①については、社外に開示することで、不正競争防止法における「営業秘密」としての保護を受けられなくなるなどの不利益が生じます。②については、社外に開示するとＮＤＡ違反の責任を負う可能性があります。

⑵　個人情報

個人情報保護法における「個人情報」とは、次の３つの情報のいずれかに該当するものです。

①　当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの

②　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

③　個人識別符号が含まれるもの

特に②が重要であり、当該情報単体では特定の個人を識別できなくても、社内に存在する他の情報と容易に照合すること、特定個人を識別することが可能であれば「個人情報」となります。

また、個人情報のうち、体系的なデータベースを構成し、容易に検索可能なものを「個人データ」

といいます（個人情報保護法16条3項）。個人データに対しては、単なる個人情報よりもさらに厳しい規制が課されています。

(3) 秘密情報・個人情報以外の情報

公開されている情報等、社外に開示されても問題のない情報が該当します。ただし、後述する著作権の観点については留意する必要があります。

図表1　社内にある情報の3つの類型

秘密情報	①自社の秘密として保護すべき情報（社外秘の情報） ②取引相手方から秘密保持義務を負う形で開示された情報 例：NDA（秘密保持契約）の対象になっている情報
個人情報	①当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの ②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 ③個人識別符号が含まれるもの
秘密情報・個人情報以外の情報	上記以外の情報

社内にある情報を入力する際に生じるリスク

秘密情報および個人情報については、文章生成ＡＩサービスに入力する際に、以下のような様々なリスクが生じます（**図表2**）。

(1) 秘密情報

自社の秘密情報（前項(1)①）を文章生成ＡＩサービスに入力する行為は、何らかの法令に違反する行為ではないものの、当該文章生成ＡＩサービスの学習に用いられる可能性があることに留意する必要があります。

図表2　秘密情報および個人情報の入力により生じるリスク

秘密情報の入力により生じるリスク	① NDA 違反に該当するリスク ② 秘密情報の外部漏えいにつながるリスク
個人情報の入力により生じるリスク	① 利用目的の範囲外利用になるリスク ② 個人データの第三者提供に該当するリスク

文章生成ＡＩサービスのベースとなっている大規模言語モデル（ＬＬＭ）は、学習に利用したデータから成果物を生成するので、自社の秘密情報が学習に用いられると、文章生成ＡＩサービスの利用者に向けて自社の秘密情報が漏えいしてしまう可能性があります。

また、仮に学習に利用されない場合でも、営業秘密としての保護が失われる危険性もあります。

もっとも、自社の秘密情報については、すべて入力を禁止するとかえって作業効率が損なわれる可能性もあるため、自社の秘密情報の要保護性（漏えいした場合のリスク）に応じて、入力してよい情報とそうでない情報を分けることも考えられます。

入力してよい自社の秘密情報を分類する方法としては、入力禁止情報の類型を列挙する「ブラックリスト方式」や、入力可能な情報の類型を列挙する「ホワイトリスト方式」等があります。

また、利用する文章生成ＡＩサービスの規約次第では、文章生成ＡＩサービスに秘密情報を入力する行為は、当該文章生成ＡＩサービスを運営している企業に対して秘密情報を開示していることになります。

そのため、取引相手とＮＤＡを締結して開示された秘密情報（前項(1)②）については、文章生成ＡＩサービスに入力すると、当該ＮＤＡ違反に該当する可能性があります。こうした情報については、自社の秘密情報のようなリスクに応じた取扱いが難しいため、一律に入力を禁止する対応が望ましいでしょう。

なお、前項(1)②における「秘密情報」の意味は、取引相手とのＮＤＡにおいて定義されるため、どの情報が秘密保持義務の対象となるかは契約によって異なります。たとえば、ＮＤＡにおいて秘密情報の定義が「開示されたすべての情報」とされている場合には、「Confidential」「社外秘」等の表示の有無を問わず、相手方から開示された情報がすべて秘密情報となるため、注意が必要です。

(2) 個人情報

個人情報取扱事業者は、本人の同意がない限り、あらかじめ通知

公表した利用目的の範囲でしか個人情報を利用することができません（個人情報保護法18条1項）。

文章生成ＡＩに個人情報を入力する目的は様々ですが、プライバシーポリシー等で通知公表した利用目的の範囲内に、個人情報を入力するにあたっての最終的な利用目的が含まれている必要があります。利用目的の範囲内である限り、文章生成ＡＩに個人情報を入力することは許されますが、漏えい等のリスクがある点については自社の秘密情報の場合と同様です。

また、個人情報が「個人データ」に該当する場合、当該個人データを第三者に提供するにあたっては、原則として本人の同意を要します（個人情報保護法27条）。

議事録に記載されている個人名などは、特定の個人を検索可能な形で体系的に構成されているとはいえず、個人データには該当しないケースが多いと思われます。しかし、たとえば議事録内の発言者単位で検索できるようなシステムを構築している場合には、議事録自体も個人データに該当する可能性があるため、注意が必要です。

個人データの提供先の当該第三者が外国に所在する場合には、より厳しい規制が課されます（個人情報保護法28条）。文章生成ＡＩサービスの運営元には海外事業者も存在するため、国内事業者が運営する文章生成ＡＩサービスを利用する場合よりも、厳しい規制を遵守しなければならないケースもあります。

また、個人データの種類によっては、そもそも本人の同意を取得することは現実的ではない場合があります。

個人情報保護委員会が発出した「生成ＡＩサービスの利用に関する注意喚起等（令和5年6月2日）」によると、入力した個人データが単に応答結果の出力にのみ利用される場合には、文章生成ＡＩサービスに個人データを入力したとしても、「個人情報保護法の規定に違反することとならない可能性」があります。

しかし、文章生成ＡＩサービスは、入力情報を学習・不正検知のために利用しているのが通常であり、この場合は「単に応答結果の出力にのみ利用される」といえず、「個人情報保護法の規定に違反することとなる可能性」が排除できないといえます。

このため、個人データを文章生成ＡＩサービスに入力できるのは、本人の同意を取得する等の法令上の規制をクリアした場合に限られます。

ただし、同意取得が現実的ではないケースも多いでしょう。そのような場合は、個人データを文章生成ＡＩサービスに入力することはできません。

(3) 他者の著作物

たとえば、文章生成ＡＩサービスに他者の著作物を入力すること自体は、原則として著作権侵害に該当しませんが、他者の著作物と同一・類似の生成物を得る目的での入力は、著作権侵害に該当する可能性があります。

生成物を利用する際に生じるリスク

文章生成ＡＩサービスにより得られた出力その他の生成物（以下「生成物」といいます）を利用するにあたっても、様々なリスクを考慮する必要があります。

(1) 他者の著作権を侵害していないか

生成物が、入力した情報または入力情報以外の既存の著作物と同一・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があります。

社外に生成物が開示されない場合であっても、これらに該当する場合は著作権侵害に該当する可能性があるため、注意が必要です。

たとえば、社内利用する目的でＷｅｂページの内容を翻訳・要約することを目的として、文章生成ＡＩサービスに当該Ｗｅｂページの内容を入力する行為は、当該Ｗｅｂページ制作者が持つ著作権の1つである翻訳権あるいは翻案権（著作権法27条）を侵害する可能性がある行為ですので、行なわないことが望ましいでしょう。

(2) 虚偽の情報が含まれていないか

大規模言語モデルは、ある単語に対して次に続く確率が高い単語を予測して文章を生成しているため、最終的な生成物の内容が誤っている場合もあります。

そのため、必ず回答の根拠を確認して、人間が適宜加筆修正等を行なったうえで利用する必要があります。

生成物に虚偽が含まれていることに気づかずに利用し、かつ、生成物が個人情報に該当する場合には、当該生成物の取得または利用が個人情報保護法違反（個人情報保護法19条、20条）に該当する可

能性があります。

(3) 文章生成AIサービスの規約上、商用利用ができるか

文章生成AIサービスの規約によっては、商用利用が認められていないケースがあります。同一事業者が提供する文章生成AIサービスであっても、利用するプランにより商用利用できるか否かが異なるケースもあるため、利用条件・規約についてはよく確認する必要があります。

図表3　社内ルール整備のポイント

利用の監督体制の整備	・利用できる文章生成 AI サービスの制限 ・各社員の利用のモニタリング ・利用にあたり一定の認証を設ける
入力してはいけない情報の整理	・秘密情報は原則入力不可とすべき ・個人情報にも慎重な検討が必要
生成物をチェックする際の注意点	・入力した情報および他者の著作物に類似していないか ・虚偽の情報が含まれていないか ・生成物の内容を確認することなく加筆修正を行なわずに利用していないか

社内ルール整備のポイント

文章生成AIサービスの利用に関する社内ルールを整備するには、以下の観点からチェックすることが有益です（**図表3**）。

(1) 利用を監督できる体制を設ける

まず、社内ルールを整備する前提として、社内における文章生成AIサービスの利用については、各社員に任せるのではなく、全社として監督できる体制を整えておくことが望ましいでしょう。

具体的には、利用できる文章生成AIサービスを指定すること、各社員の入力データ・出力データを確認（モニタリング）できるようにし、不適切な利用を未然に防止・早期発見できるようにすること、利用にあたり一定の認証（社内ネットワークを経由したアクセスでのみ利用可能とする等）を設けること等が挙げられます。

これらの体制は、社内ルールを整備した後において、社内ルールが遵守されているか否かのチェックにも利用することが可能です。

(2) 入力してはいけない情報について規定する

社内ルールでは、社内情報を適切に分類したうえで、文章生成AIサービスに入力してはいけない情報について規定する必要があります。特に、個人データについては、文章生成AIサービスに入力できるケースが限られ、かつ、個人情報と個人データの区別は容易ではない場合もあるため、社内ルールを整備する際には、個人情報の入力を一律に禁止することも考えられます。

(3) 生成物をチェックする際の注意点を規定する

社内ルールでは、生成物の利用によって生じるリスクを回避するために、生成物の内容をチェックする際の注意点について記載する必要があります。

具体的には、入力した情報および他者の著作物に類似していないか、虚偽の情報が含まれていないか、生成物の内容を確認することなく加筆修正を行なわずに利用していないか等をチェックします。

(4) 公表されている雛形を参考にする

一般社団法人日本ディープラーニング協会「生成AIの利用ガイドライン」に社内ルールの雛形が公開されています。

この雛形に、社内の状況に応じて必要な追加や修正を加えて利用するとよいでしょう。

議事録アプリの利用

会議や打合わせの録音録画から内容を文字に起こし、議事録を自動で作成するアプリ（議事録作成アプリ）を利用する場合についても、これまで述べた観点で検討する必要があります。

まず、会社として個々の社員の利用を監督できないアプリを利用することは避けるべきです。使用を申請制にするかどうかはケースバイケースですが、最低限、入力された録音録画および出力された議事録の内容を社内で確認できる機能があるものを選びましょう。

また、会議や打合わせには自社および他社の秘密情報が含まれる可能性があるため、入力した情報がどのように使われるか確認し、特にアプリの学習に利用されるような場合には、アプリの利用は慎重に検討すべきです。

出力された議事録を利用するにあたり、著作権の問題が生じる可能性は低いと思われますが、不正確な要約がされている可能性がある点には注意が必要です。▲

さかた　こうすけ　STORIA法律事務所にてエンターテインメント法務、AI・データ法務、スタートアップ支援の分野に特に注力している。『AIプロファイリングの法律問題 AI時代の個人情報・プライバシー』（商事法務）等著作・寄稿多数。