【不正競争防止法、
個人情報保護法、著作権法】

生成AIの業務利用(Part Ⅱ)
～生成AIの利用に関する社内ルールの策定～

大江橋法律事務所 パートナー 弁護士 ／
カリフォルニア州弁護士
廣瀬 崇史
▶ PROFILE
takashi.hirose@ohebashi.com

第1 はじめに

PartIで述べられているように、文章生成AI（以下、単に「生成AI」といいます。）には、法規制や生成AIの性質から生じる法的留意点があることから、生成AIの利用に起因する法的リスクの発生を抑制するために、業務において生成AIの利用を許す場合には、社内ガイドラインや内部規則（以下、単に「社内ルール」といいます。）を策定して運用することが望ましいと考えられます。

社内ルールの適用範囲については、生成AIの試験的な導入をし、特定の部署や人員にのみ生成AIの使用を許可するような場合には、当該特定の部署や人員への限定的な適用となりますが、一般的な傾向としては、全社的に適用することを想定するものが策定されていることが多いと思われます。また、PartIで述べられているように、法的留意点について、未解決の論点が複数存在していることから、社内ルールの内容としては、比較的保守的な内容を定めてスタートすることがしばしば見受けられます。

なお、生成AIのサービス自体や生成AIに関する法務も発展途上であることから、社内ルールを一旦定めた後も、社内の実際の利用状況、具体的な業務ニーズ、利用対象の生成AIの性質、費用、機能改善、新サービスの登場、裁判例や法改正の状況、実務運用の状況等を考慮する必要があります。そのため、社内ルールの運用開始後も、社内外における情報収集や社内のモニタリングを実施してゆき、利用対象の生成AIの範囲、用途、社内ルール等についての継続的な見直しも重要となります。

とはいえ、まずは、早期に社内ルールを策定することが重要であることから、本記事は、社内ルールの策定の初期段階に役立つと思われる策定手法や社内ルールの項目例について簡潔に紹介することで、実務の参考となるような情報を提供することを目的としております。

第2 社内ルール策定のプロセス及び方法等

1 公表されているガイドライン等の情報収集

社内ルールの策定方法については、対象企業の性質、社内環境、ニーズ、情報収集の状況等に応じていろいろな方法がありえ、一義的な正解はないと思われますが、例えば、まず、一般に公開されているガイドライン等を収集し、その内容を把握し、一定程度参考としながら、社内ルールを作成することが考えられます。

例えば、政府は「ChatGPT等の生成AIの業務利用に関する申合せ（第2版）注)1」を2023年9月15日に公表しています注)2。これは、関係省庁が連携して生成AIに関する実態の把握に努め適切な措置を講じていく必要性から、同年5月8日に政府が関係省庁宛に周知した、省庁の生成AIの業務利用において要機密情報

注)1
https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/c64badc7-6f43-406a-b6ed-63f91e0bc7cf/e2fe5e16/20230915_meeting_executive_outline_03.pdf
注)2 なお、総務省は、2019年に、「AI利活用ガイドライン」を開示しており、記載項目が参考となるところがあります。
https://www.soumu.go.jp/iicp/research/results/ai-network.html

を原則として扱わないことや、承認を得ない職員等による生成AIの利用を防止すること等を内容とする申合せの改訂版です。申合せという性質上、社内ルールとしてはそのままでは使えませんが、要機密情報の取扱いや、利用者の承認を必要とする取扱い等の考え方が参考になります。

また、複数の地方自治体が、生成AIの利用に関するガイドラインを策定し、公開をしています。例えば、2023年6月には、神戸市が「神戸市生成AIの利用ガイドライン注)3」を、同年8月には、東京都デジタルサービス局が、東京都職員向けに、「文章生成AI利活用ガイドライン注)4」を、同月に神奈川県も「神奈川県生成AIの利用ガイドライン注)5」の第1版を策定し公開をしています。これらのガイドラインにおいては、ガイドラインの目的、生成AIの特徴、リスク、生成AIへのプロンプト入力時の注意事項、プロンプト入力後の生成物を利用する上での留意事項、その他の留意事項や活用事例等についての具体的な記載が見受けられ、一定程度参考となります注)6。

さらに、民間の団体として、日本ディープラーニング協会が、2023年5月に、生成AIの活用を考える組織が社内ルールの導入ができるように、社内ルールのシンプルなひな形として「生成AIの利用ガイドライン第1版」を公開しており、同年10月には、これに改訂を加えた「生成AIの利用ガイドライン第1.1版」を公開しています。当該雛形にも、ガイドラインの目的、対象とする生成AIの説明、利用禁止用途、データ入力（プロンプト入力）の時の留意点、生成物の利用時における留意点等についての項目が記載されています。

これらのガイドライン等の項目、内容等を一定程度参考としつつ、自社で利用が想定されている特定の生成AIの特徴、利用目的、社内の状況やニーズ、他の情報管理に関する社内規程類等に照らして、自社にあった内容を模索してゆくことが考えられます。

なお、政府は、2023年9月に、事業者向けのAIガイドラインの骨子案注)7を開示しており、当該ガイドラインの正式な内容が策定・公開される予定であることから、その内容についても留意が必要ですが、本記事の執筆時点では公開されていないことから、本記事には、その内容は反映されていないことにご留意ください。

2 社内の状況やニーズ、利用対象の生成AIの特徴に合わせた社内ルール策定のための情報取集

社内ルールの策定においては、一般的な参考情報を考慮しつつ、利用する生成AIの特徴や自社の業務状況等に親和性のある内容とすることが重要です。自社にあった生成AIの利用決定やそれに関する社内ルールの内容を模索するため、次のような流れが、一例として考えられます注)8。

まず、存在している生成AIの種類・サービス内容・機能、セキュリティレベル、利用者による入力データの学習への利用の有無、データ保存の状況、使用開始までの期間（開発期間の有無・開発費用の負担）、運用コスト、契約条項や利用規約の内容といった当該サービスの特徴やリスクに関する情報収集を広く行うことが重要です。

また、それと同時並行的に、社内における生成AI利用ニーズ等に関する調査を行うことが考えられます。PartIでも述べられているように、部署や業務内容注)9によって、生成AIの利用場面・

注)3　https://www.city.kobe.lg.jp/documents/63928/seiseiaiguideline.pdf
注)4　https://www.digitalservice.metro.tokyo.lg.jp/ict/pdf/ai_guideline.pdf
注)5　https://www.pref.kanagawa.jp/documents/102838/guideline-ai-kanagawa2.pdf
注)6　但し、私企業とは団体の性質・業務内容が異なることや、利用しているサービスの前提が異なり得ることを理解した上で、参考とすることが必要です。
注)7　https://www8.cao.go.jp/cstp/ai/ai_senryaku/5kai/gaidorain.pdf
注)8　企業の業態、性質、企業の情報把握の状況や業務環境等に応じて、一義的な正解はなく、バリエーションがあります。
注)9　会社の業態によっても異なります。

方法・用途は異なり得ることから、生成AIを業務利用することが想定される部署、当該部署において想定される利用方法の例、当該利用方法にまつわるリスクを把握するための情報収集を行うことは重要です。その際、ニーズの状況を広く把握する観点から、本社の特定の部署に限定することなく、可能であれば、広く情報収集を行うことも望ましいと考えられます。また、社内の状況やニーズ等を具体的に把握するために質問内容・表現や情報収集の方法にも留意することが重要と考えられます注)10。

このように収集された社内のニーズ等に関する情報や、存在している生成AIサービスの特徴・リスク・費用等を総合的に考慮しながら、どのような種類の生成AIサービスの使用を許可するのか、個別の契約を認めるか自社でベンダーと一括契約をしたサービスの利用に限定するか、当該使用許可の内容や対象を部署や人ごとに検討するか一律の取扱いとするのか、具体的に許可される利用場面・方法・用途をどう確定するか（例、生成AIの利用を許す業務の種類、プロンプト入力制限の有無・内容、生成物の利用を社内利用に留めるか否か）等を検討します。

また、当該検討結果及び収集した前述の情報を考慮し、社内ルールの案・骨子を作成してゆき、一定程度まとまった時点で、その内容について各部署から意見等を収集し、社内ルールをより具体的な内容に調整し、確定注)11してゆくといった手順も考えられます。なお、前述のとおり、社内ルールについて、社内に一般的に適用されるものを策定しつつ、個別の部署の生成AIとの関わり合い方、例えば、機密情報を扱うことが多い部署、生成AIによるコンテンツ利用の頻度が高い部署、対外的な活動に用いる可能性がある部署等について、特別に適用されるルールを策定することも考えられます。

加えて、社内ルールの確定後は、生成AIの利用に関する組織のスタンスや生成AIの特徴、リスクに関する情報とともに、社内ルールの周知、内容についての啓蒙注)12活動を行うことも重要です。

なお、前述のとおり生成AIの利用には法的留意点（未解決のものを含む）が複数存在し、生成AI自体や生成AIに関する法務も発展途上であることから、社内ルールを一旦定めた後も、社内の実際の利用状況、具体的な業務ニーズ、利用対象の生成AIの性質、費用、機能改善、新サービスの登場、裁判例や法改正の状況、実務運用の状況等を考慮し、利用対象の生成AIの範囲、用途、社内ルール等についての継続的な見直しを行うことも重要と考えられます。

第3　社内ルールの一般的な項目

1 はじめに

以下では、現状の法的議論を前提として、社内ルールを策定する際に参考となる社内ルールの項目の代表的な例を紹介していきます注)13。なお、本記事は、簡潔な情報提供を目的としており、かつ、前述のとおり生成AIの利用には法的留意点（未解決のものを含む）が複数存在し、生成AIに関する法務も発展途上であることから、完全・網羅的なリストとならないことについて、ご留意ください。

注)10　Yes　Noで答えるような簡単なアンケートの配布回収に留めず、実態把握のため、部署ごとの聞き取り等を行うことも考えられます。また、上記で情報収集した生成AI自体の情報（特徴、リスク等）を踏まえ、質問表現を工夫することも考えられます。サービスの前提が異なり得ることを理解した上で、参考とすることが必要です。

注)11　なお、社内の権限規程といった社内規程の内容に応じて、適切な会議体、役職者による意思決定を経ることも必要となり得ます。

注)12　説明会等で具体的に説明をする、社内システムを通じて、ウェビナーを視聴してもらうことも考えられます。

注)13　なお、紹介する社内ルールの内容は、比較的保守的な策定例として見受けられるものを参考としたものです。会社の属する業界、生成AIを利用する部署や業務の性質、具体的ニーズ等に応じ、アレンジを検討することも重要と考えられます。

2 目的等

生成AIに関する社内ルールにおいては、会社の方針、社内ルールの背景や個別項目の理解を促進する観点から、社内ルールの目的等に関する項目が設けられることが比較的多く見受けられます。その際、生成AIの利用についての会社のスタンス（積極的か、抑制的か等）、生成AIの利用方針、社内ルールの概要等が記載されることがしばしば見受けられます。

なお、企業においては、秘密情報や個人情報等に関する情報利用・管理に関する社内規程が存在していることが多いところ、生成AIに関する社内ルールにおいてはプロンプトへ入力する情報への制約が記載されることもあり、社内ルールと既存の社内規程との関係性について触れられることもあります。

また、前述のとおり、社内ルールは継続的な見直しをすることが重要であることから、社内ルールの策定後も継続的な改訂があり得ることについて注意喚起するものも見受けられます。

3 使用を許可する生成AIサービス、対象者、用途等

社内ルールにおいては、適用対象が明確になるように、利用が許可される具体的な生成AIを特定する情報や、社内ルールの適用対象者（許可対象となる部署、従業員等の範囲注）14）についての記載がみられます注）15。その際、実際に使用を許可する特定の生成AIサービスの特徴、リスクの概要についても触れられることもあります。すなわち、生成AIに関する社内ルールにおいては、必須ではありませんが、各個別のルール・条項について理解がしやすくなるように、その前提となる生成AIの一般的な特徴、仕組み、（正確性に関するリスク、情報漏洩リスク、権利侵害リスク等の）法的リスクの概要についての記載がみられることがあります。さらに、当該法的リスクの記載を踏まえて、生成AIの利用場面・方法・用途に関する制約の概要についても記載されることがあります。

なお、比較的規模の大きい会社においては、秘密保持、情報漏洩防止、入力情報の目的外利用の防止を含む情報の適正な管理等の観点から、セキュリティ確保や入力データの学習利用の防止等を求めて、生成AI提供事業者（ベンダー）との間で一括契約した生成AIサービスの利用のみを許可する例が比較的多くみられます。

4 生成AIへプロンプト入力を行う上での留意点

生成AIの利用自体に関する法的留意点については注）16、大きく分けると、プロンプトの入力段階に関連する問題、生成AIの生成物の利用段階に関する問題等があることから、生成AIに関する社内ルールについては、それぞれの段階にわけて留意点が記載されることが、しばしば見受けられます。以下、生成AIへプロンプト入力を行う際の留意点として記載されることが多い事項の例を紹介します注）17。

まず、秘密保持、情報漏洩の防止や情報の適切な管理（特定された利用目的の達成に必要な範囲を超えた個人情報の取扱いの禁止、個人データの第三者提供や「委託」該当性に関する問題等を含みます。PartIの第2参照）等の観点から、秘密扱い等を要する情報について、プロンプトの入力制限をする例が多く

注）14　生成AIの試験的な利用についての社内ルールの場合は、試験的な利用である旨及び試験的利用の対象部署等が記載されることがあります。

注）15　なお、明記された生成AIサービス以外の利用を禁止する旨の記載とする場合、一方で、既存サービスの機能改善が行われることや新サービスが出される可能性も考慮して、利用対象となるサービスの追加を申請できる旨を記載する場合もあります。

注）16　本記事では、学習段階の問題については、触れておりませんのでご留意ください。

注）17　なお、本記事は、生成AIの用途として、一般的な文章作成、要約、情報収集等を想定しており、コード作成等をするような状況は直接念頭においていません。

みられます注)18注)19。例えば、顧客の氏名、住所、メールアドレスといった個人を特定できる又は個人を特定し得る情報注)20、プライバシーに関する情報、人事情報等を入力することを禁止する例がみられます。また、個人情報保護法の規制を意識して個人情報の目的外利用の禁止等を明示している例も見受けられます。さらに、社内にシステム等のユーザーID・パスワード・アクセスキーなどの認証情報の入力を禁止する例もみられます。加えて、自社の営業秘密やその他の秘匿すべき秘密（非公開情報、未公開情報（他部門への開示に制約がある情報、インサイダー情報等を含む））について入力禁止とする例が多くみられます。その際、用いる用語、定義、情報の利用範囲等については、自社における情報利用・管理に関する他の社内規程との調整も必要となることに留意が必要です。

なお、利用する生成AIサービスの特徴（学習への利用がないことや、データ保存の状況等）によっては、自社独自の情報のうち、秘密扱いするものであったとしても、機密のレベルが高くないものについては入力を許す扱いも考えられます。一方、他社からNDAやその他の契約の下で秘密保持義務を課されて開示された秘密情報については、PartIで述べられているように、第三者開示、委託者の負う秘密保持義務、秘密情報の目的外利用該当性といった問題に加え、契約ごとの秘密保持義務内容・制約のバリエーションの存在といった問題があり、生成AIの導入段階では、保守的に考え、まずは一律に入力を禁止する例がしばしばみられます。これらに加えて、契約において、情報・データの利用目的、態様が具体的に限定されている情報についての入力禁止を記載しておくことも考えられます。

次に、PartIでも述べられているように、生成AIの利用については、第三者の著作権に対する侵害の問題があります。誤解を恐れず、簡潔にいうと、（被疑侵害物について）原著作物の創作性の認められる部分との関係で、依拠性と類似性が認められる場合には、権利制限規定の適用といったことがない限り、原則として著作権侵害となります。著作権保護期間内にある著作物の創作性の認められる表現そのものをプロンプトとして入力して利用する場合には、複製をしていることになり、複製権の侵害（そのものを入力しているので依拠性・類似性はある前提です）が問題となり得ます。

この点、権利制限規定である、著作権法30条の4では、「情報解析」、又は、「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」（非享受目的）に該当する場合には、「著作権者の利益を不当に害することとなる場合」を除いて、著作物の利用は認められるとされています。上記のような生成AIへの入力行為は「情報解析」に該当するので原則として適法であるという議論がされていますが、本条項は「多数の著作物その他の大量の情報から」要素を抽出することが前提なので、一つの著作物といった少数の著作物をプロンプトに入力することが、「情報解析」に該当しない可能性があり得るとする議論もされています注)21。また、入力した著作物の本質的特徴が生成物に反映されそれを閲読することを狙って入力している

注)18　入力データが学習利用されてしまう生成AIサービスを利用する場合のみならず、学習利用されないサービス設計になっている生成AIサービスを利用する場合であっても、システム設計によっては情報漏洩のリスクが残り得ることから、入力禁止とする例がみられます。また、入力情報が学習に利用されず、かつ、監視等の目的でベンダーが情報取得することを停止している場合であっても、企業によっては、今後の実績や動向を踏まえた評価を必要とし、まずは入力禁止としつつ、今後、調整を検討するケースも見受けられます。

注)19　禁止事項を列挙するブラックリスト方式の場合や、入力を許す事項を列挙するホワイトリスト方式もあります。

注)20　PartIで述べられたように、第三者提供の問題が生じるのは個人データであって、個人情報そのものではないですが、保守的に個人情報の入力を禁止する場合があります。メールアドレス自体は個人情報に該当しない場合もあり得ますが、入力を禁止している場合もみられます。また、業務効率化と漏洩リスクを考慮し、例えば、生成AIを社内会議の議事録の要約等に用いる場合を想定し、利用対象の生成AIの設計や会議内容によっては、自社の従業員の氏名の入力を許すことも考えられます。

注)21　松尾剛行『ChatGPTと法律実務－AIとリーガルテックがひらく弁護士／法務の未来』100頁（弘文堂、2023年）。一方で、学習済みデータ等と合わせれば、多数といえるという考え方もあり得ます（松尾剛行・同101頁（67））。

ことが窺われる場合には、非享受目的に該当しない可能性があり得ます注)22。

さらに、生成AIによる生成物が、既存の著作物と同一又は類似のものとなっている場合は、当該生成物の生成・利用が既存の著作物に関する著作権の侵害になる可能性注)23もあります。

そこで、上記のような事情を考慮して、プロンプト入力段階で、著作権の侵害につながるようなプロンプト入力を禁止する例がしばしばみられます。例えば、当該入力対象となった他人の著作物と同一又は類似する生成物を生成する目的と受け取られるような内容はプロンプトとして入力行為自体を禁止することがあります。これには、プロンプトに既存の著作物、著作物名、著者名の入力を避けるように明記する規定が含まれます。

なお、生成AIの生成物を利用する際に、上記のような著作権侵害のリスクを減らす観点（事後的に侵害リスクの検証ができるようにする観点）、及び、PartIでも述べられているとおり、生成AIによる生成物について著作物性が認められない可能性があるところ、著作物性の判断にプラスとなるように「創作意図」及び「創作的寄与」があることを示す観点等から、プロンプトの入力過程・入力内容の記録化の重要性を、社内ルールに記載することもあります。

これ以外にも、例えば、要配慮個人情報（例えば個人の病状等）の取得については、取得自体に制約があることから、個人情報の不適切な取得、取扱いにつながるようなプロンプト入力を禁止する旨を社内ルールに記載することも考えられます。

なお、既に述べたとおり、社内ルールについては継続的な見直しが想定されていますので、禁止事項の加除修正があり得ることが記載されることもあります。

5 生成AIの生成物を利用する場面での留意点

次に、生成AIの生成物を利用する場面での留意点の項目の代表例について以下紹介します。

まず、文章の生成AIは、大規模言語モデルの原理上、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ものなので、生成物の内容が一見正しいようにみえても、誤った情報が含まれている可能性がありますので、生成物について、信頼のおける根拠、裏付けとなる事実・情報の有無の確認等を求める記載がみられます。

また、前述のとおり、生成物について、既存の著作物の創作的表現との間で類似性が認められ、かつ、仮に依拠性注)24も認められる場合には、その利用は著作権侵害となり得ることから、生成物について、既存の著作物と類似していないかの確認を求める記載が社内ルールには多くみられます。例えば、インターネット検索等により、生成物が既存の著作物と同一・類似していないか調査を行うことや、著作権等の侵害の疑いが生じた場合には、法務部等にも確認することを求めることが記載されることがあります。

さらに、生成AIを利用して生成したキャッチコピーや商品名などを商用利用する行為は、第三者の商標権を侵害する可能性がありますのでJ-PlatPat等による登録商標の調査注)25を行う注)26ことを求める記載がよくみられます。また、侵害の疑いがある場合

注)22　松尾剛行・同95頁及び96頁
注)23　PartIにも記載されているように、依拠性については、定説がない状況ですが、プロンプトにおいて、具体的な著作物への言及がある場合には、依拠性を肯定する方向の要素となり得ます。
注)24　前述のとおり、依拠性については、定説がありません。
注)25　なお、本記事の対象とはしていませんが、画像生成AIを利用し、デザインを生成し、当該デザインを商品に利用しようとする場合には、登録意匠の調査等も必要となります。また、不正競争防止法上の、商品形態模倣や商品等表示に関する規制も考慮が必要となります。
注)26　商標権の侵害は、著作権の場合と異なり、依拠性は要件となっていないことから、生成AIの生成物が、偶然既存の商標と同一・類似している場合でも、指定商品又は役務（類似を含む）について、商標的使用をする場合には、差止請求等の対象となります。

には、法務部等にも確認することを求めることが記載されることがあります。

加えて、生成物の表現内容に、第三者の名誉権やその他の人格権の侵害となるよう内容が含まれていないか、差別や偏見につながる表現やその他の社会的に不適切な表現が含まれていないか、個人情報が含まれていないか等について、特に生成物の対外的な利用が想定される場合には、慎重に検討をしておく必要があり、かかる旨を社内ルールに記載しておくことも重要です。

なお、上記の記載とは少し方向性が異なるものの、PartIでも述べられているとおり、生成物には著作権が発生しない可能性があるところ、生成物の著作物性の判断にプラスとなるように、人間の「創作意図」及び「創作的寄与」があることを示す観点から、生成された著作物を一定程度、加筆・修正をして用いることを推奨するような記載をしておくことも考えられます。

そのほかの留意点としては、生成AIのサービス利用規約や、生成AI提供事業者との契約において、生成物の利用について一定の制約が定められている場合を想定した記載をすることが考えられます。例えば、生成AIを用いた生成物についてその旨を記載することが求められている場合や、一定の用途（例、法律違反や社会的に不適切な用途等）での生成AIの利用が禁止されていることがありますので、利用許可の対象となっている生成AIによっては、これらの事項について社内ルールで言及しておくことが考えられます。

6 推奨する利用方法

社内ルールに必須な記載ではありませんが、社内ルールによっては、生成AIの効率的な利用方法について、具体例を記載しておき、社内における業務効率化や、生成AIへの理解の促進を目指すものも見受けられます。

例えば、文書作成の補助（例、要約、言い換え、翻訳）に適している旨や、アイデアだし（壁打ち）に適している旨を記載する例が見受けられますし、また、有効なプロンプトの入力に関して、例えば、質問の前提や内容を具体化すること（例、前提条件、回答の立場、出力の形式の指定等）や、プロンプトを重ねてゆき、回答を改善してゆく方法について記載されることもあります。

なお、当該項目は、利用対象となっている生成AIの特徴に合わせる必要があること、生成AIの機能改善が生じることが想定されること、社内における事例の集積も期待できること等から、当該項目を仮に記載をする場合でも、改訂をしてゆくことが重要です。

以上