

はしがき

本書は、弁護士や企業の法務部門に所属する方など、法務の専門知識を持つ読者を想定して、生成AIに関する法務の実務をテーマに執筆したものです。

本書では、生成AIの法的論点を紹介するだけにとどまらず、実務で直面する課題やその対応のヒントになるよう意識して解説を行っています。

生成AIの登場は、近年で最大の変化です。生成AIは、本書の執筆を進める短い間のうちにも、技術的に著しい進化を遂げるとともに、社会的に大きな影響力を持つに至っており、事業者の活動の様々な場面で活用が進められています。その一方で、生成AIをめぐる法令の適用や解釈への影響、リスクやその他の含意については、十分な理解が進んでいない点もまだ多く存在します。

本書の執筆に当たっては、筆者（齊藤）が代表を務める法律事務所LAB-01の有志により、定期的な所内の研究会を通じて知見を共有し、検討を深めながら進めました。筆者は、総務省・経済産業省「AI事業者ガイドライン（第1.0版）」の策定を始め、この分野の政策的な議論にも参画してきましたが、企業実務の中で得た経験に加え、その知見も本書に反映しています。

本書では、まず、法的な分析に必要な限りで、生成AIに関する基本的な技術や仕組みを平易に解説した上で、著作権を始めとする知的財産権の扱いや、人格権とこれに由来する権利に関連する議論、データや個人情報保護との関係、契約実務における留意点、さらにAIガバナンスの議論動向に至るまで、実務上の論点を広く取り上げています。

本書の内容には、可能な限り、最新の技術やサービスの状況を反映するように努めましたが、その発展や拡大があまりに速いため、必ずしも最新とはいえない内容が含まれているように見える部分もあるかもしれません。ただその場合であっても、法的な分析には影響がないように書き進めています。

本書を通じて、読者が生成AIをめぐる法的な論点を理解し、実務上の判断や検討に当たっての出発点やヒントとなる知識を得る一助となれば幸いです。そして、本書が生成AIの法的な課題をめぐる対話の土台となり、読者自身の検討や議論を促す契機となることを願っています。

令和7年8月

編著者 齊藤友紀

CONTENTS

第1章 生成AIの基本を押さえよう

- 1 生成AIとはどのような技術か 14
生成AIとは／生成AIの開発(学習)／生成AIの利用とプロンプト／生成AIとリスクの管理
- 2 生成AIの動かし方 18
プロンプトとは／生成AIとプロンプトの処理／データの再現とプロンプト／プロンプトと法的な課題
- 3 生成AIが苦手なこと 22
生成AIの技術的性質と限界／RAGと外部の情報ソースの活用／ファインチューニングと専門分野への特化／生成AIの技術的限界への対応
- 4 生成AIを利用するときの2パターン 26
ブラウザUI利用とAPI経由利用／API経由利用時の責任の構造／API経由利用時のリスクと法的な課題／API経由利用に関するその他の注意点
- 5 生成AIに関連する論点にはどのようなものがあるか 30
生成AIと知的財産権等／生成AIとデータの保護／生成AIと契約関係／生成AIとAIガバナンス

第2章 生成AIと著作権の問題を知ろう

- 6 生成された表現は著作権で保護されるか 36
AI生成物と著作権／AI生成物と著作物への該当性／生成AIの利用と創作的寄与／AI生成物を事業上で利用する際の注意点

- 7 著作者の著作権と作風の模倣 40
スタイルの模倣と著作権侵害の成否／生成・利用と著作権侵害の成否／追加的な学習と著作権侵害の成否／その他注意すべき事項
- 8 AI生成物を加工・編集したものは著作権で保護されるか 44
生成AIの部分利用と著作権／生成されたコンテンツに対する人の加工／作成されたコンテンツに対する生成AIの加工／生成されたコンテンツの利用
- 9 他者の著作物を学習させることの法律問題 48
生成AIの学習と著作権の効力／柔軟な権利制限規定／複数の目的が併存する場合の考え方／著作権者の利益を不当に害する場合の考え方／特化型生成AIの開発上の注意点
- 10 国内開発した生成AIを国外で商用化した場合 52
著作権法と準拠法の決定／生成AIの開発に関する法律関係／生成AIの提供・利用に関する法律関係／適法に開発された生成AIの商用化の際の注意点
- 11 生成された表現の利用が著作権侵害となる場合 56
生成AIの利用と著作権侵害の成否／既存の著作物に関する利用者の認識がある場合／既存の著作物に関する利用者の認識がない場合／開発者・提供者の注意すべき点
- 12 著作権侵害があった場合に権利者ができる法的措置 60
学習による著作権の侵害とその責任／学習による著作権の侵害の差止め／学習による著作権の侵害に基づく損害の賠償／権利行使する側の注意点
- 13 生成された情報の利用が不法行為となる場合 64
著作権の保護を受けないAI生成物／一般不法行為と著作権の侵害／著作物として保護を受けない場合の不法行為の成否／AI生成物の複製と不法行為の成否

生成AIと特許・商標・人格権の問題を知らう

- 14 生成された情報をヒントとした発明と特許 70
 発明と生成AI／生成AIの発明者適格／生成AIを利用した個人の発明者該当性／創作的な寄与の証明方法
- 15 生成AIへの入出力を繰り返したアイデアと特許 74
 生成AIによる発明の支援／特許発明と新規性／生成AIと発明の新規性／新規性の喪失リスクとその対応
- 16 生成されたロゴの商標登録 78
 ロゴと生成AI／商標権が保護するもの／商標調査の重要性／他人の著作権と抵触する可能性に注意
- 17 生成されたロゴを自社サービスに使用する際の注意点 82
 ロゴデザインのツールでの作成／商標権による保護の範囲／不正競争防止法の商品等表示規制／AI生成物の商標としての使用時の注意点
- 18 特定の人の声を生成するサービスと人格権 86
 声の生成と著作隣接権の限界／声の財産的価値とパブリシティ権／生成された音声の使用とパブリシティ権／声の権利に関するその他の議論
- 19 生成したアバターが無断利用されている場合 90
 アバターの価値の保護／知的財産権等によるアバターの保護／人格権等によるアバターの保護の可能性／人格権等によるアバターの保護に関する注意点
- 20 生成AIに入出力されたデータは誰のものか 94
 生成AIとデータの関係／データに対する法的な保護／データ・オーナーシップの議論／契約によるデータの管理

生成AIサービスの契約関係を知らう

- 21 生成されたコンテンツの利用規約の定め方 100
 生成AIサービスの提供と利用規約／生成AIモデルの契約関係／生成AIモデルを利用したサービスの契約関係／生成コンテンツに関する利用規約の作成のポイント
- 22 利用者が著作権侵害した場合のサービス提供者の責任 104
 生成AIの利用と提供の責任／提供者の責任と「規範的行為主体論」／提供者の責任と対処方法／技術的な措置と契約上の措置
- 23 サービス提供者の意図に反し個人情報が入力された場合 108
 サービス提供者と個人情報保護法／個人情報の「取得」の意義／プロンプトの入力と個人情報の取得／サービス提供者のとるべき対応
- 24 利用者が規約に違反してデータを収集した場合 112
 機械的なデータの収集と課題／機械的なデータ収集の禁止と契約上の効果／機械的なデータの収集と著作権法30条の4／機械的なデータの収集に関する留意点
- 25 サービス提供者が利用者の入力データを
 利用する際の注意点 116
 入力データとその取扱い上の課題／入力データの使用に関する定め／入力データの制限等に関する定め
- 26 生成されたソースコードの法的な取扱い 120
 プロダクト開発と生成AIの利用／生成されたソースコードと「著作物」の該当性／生成されたソースコードの「営業秘密」の該当性／生成されたソースコードの利用と契約上の制約

データの取扱いに関する 法律問題を知ろう

- 27 生成AIモデルを公開する際の利用条件** 126
生成AIモデルの公開とライセンス／生成AIモデルの利用許諾の範囲／生成AIモデルの利用許諾の条件／生成AIモデルの利用条件の定め方
- 28 生成AIを利用して自社プロダクトを開発する際の注意点** 130
生成AIとプロダクト開発／秘密情報とリスクの評価／生成AIと入出力データの取扱い／生成AIのリスクへの対応
- 29 秘密保持義務を負う情報を取り扱う場合** 134
生成AIと秘密保持義務／クラウドサービスと秘密保持義務／生成AIとクラウドサービスの関係性／秘密保持義務の履行上の注意点
- 30 不正競争防止法に違反しないために** 138
生成AIと契約上の秘密保持義務／不正競争防止法上の営業秘密／生成AIの利用と入力データの秘密管理性／生成AIの利用と善管注意義務
- 31 利用者が入力した情報は個人データに当たるか** 142
プロンプトと個人情報保護法／プロンプトと個人情報等の該当性／生成コンテンツと個人情報等の該当性／個人情報の非個人情報化の可否
- 32 利用者から収集した個人情報に基づくサービスの注意点** 146
生成AIのサービスの類型／個人情報の利用目的に関する規制／個人情報の第三者への提供に関する規制／個人情報保護法の規制の実務への影響
- 33 国外で提供されるサービスと個人情報** 150
生成AIモデルの開発と利用／外国にある第三者への提供に関する規制／基準に適合する体制を整備している者の例外／外国における個人データの取扱いに関する規制

- 34 生成AIと「クラウド例外」** 154
個人データとクラウドサービス／クラウドサービスと「クラウド例外」／生成AIと「クラウド例外」の適用可能性

より良い活用のためのルールや 管理方法を知ろう

- 35 参考になる公的なガイドライン** 160
公的なガイドラインの策定状況／人間中心のAI社会原則／事業者に通ずる指針の検討／AI事業者ガイドラインの利用方法
- 36 社内ルールを策定する際に検討すべきこと** 164
生成AIの業務利用と社内ルール／入力データの扱いに関する方針／生成コンテンツの利用に関する方針／社内ルール策定時のその他の留意点
- 37 生成AIを利用している事実は利用者に開示すべきか** 168
生成AIの利用と透明性／透明性の確保に向けた方法の決定／透明性の確保に向けた具体的な方法の例／透明性の確保に向けたその他の留意点
- 38 サービス提供により問題が起きたときの備え** 172
生成AIの事故とサービス提供者の説明責任／生成AIの事故の原因とサービス提供者の責任／サービス提供者の責任と情報の記録化／サービス提供者のレピュテーションリスクとその対応
- 39 学習に用いるデータの品質の管理** 176
生成AIとデータの品質管理の必要性／学習用データの品質の基準／学習用データの品質管理プロセス／学習用データに関するその他の留意点
- 40 生成AIの利用や提供による典型的なリスク** 180
生成AIのリスクを理解する重要性／生成AIの普及前から議論されてきたリスク／生成AIの普及に伴って顕在化してきたリスク／生成AIのリスクに関するその他の留意点

41	サービス提供者が考えるべき偽情報の問題 184
	生成AIとディープフェイク／ディープフェイクと利用者の責任／ディープフェイクとサービス提供者の責任／ディープフェイクとガバナンス
42	生成された結果の利用により 利用者に生じた損害の責任 188
	生成AIとハルシネーション／ハルシネーションに伴う法的責任／サービス提供者の責任と「債務の本旨」／サービス提供者の責任に関するその他の注意点
43	法律相談への自動回答サービスと弁護士法 192
	AIとリーガルテック／リーガルテックと弁護士法／法律相談チャットボットと弁護士法／弁護士法の適用リスクへの対応策
44	法的拘束力がないガイドラインとはどういう意味か 196
	ガイドラインと「非拘束的なソフトロー」／ソフトローとAI事業者ガイドライン／AI事業者ガイドラインと既成の法律の関係性／AI分野のソフトローの実際の意義と展望
45	生成AIの法規制はどうなっていくのか200
	AIと法規制の概要／欧州の法規制／米国の法規制／日本の法規制

凡 例

法令名等の内容は、2025年8月現在施行のものによります。

本文中、資料、判例を略記した箇所があります。次の略記表を参照してください。

■法令等

〈略記〉	〈正式〉
個人情報保護法	個人情報の保護に関する法律
個人情報保護法施行令	個人情報の保護に関する法律施行令
個人情報保護規則	個人情報の保護に関する法律施行規則
考え方	文化庁「AIと著作権に関する考え方について」
個人情報保護法 GL	個人情報の保護に関する法律についてのガイドライン
個人情報保護法 Q&A	「個人情報の保護に関する法律についてのガイドライン」に関する Q&A
ガイドライン	総務省・経済産業省「AI事業者ガイドライン（第1.1版）」
不競法	不正競争防止法

■資料

〈略記〉	〈正式〉
民集	最高裁判所民事判例集
判タ	判例タイムズ

〈判例の表記〉

判例は、以下のように略記して示しています。

（略記） 最判平成24年2月2日民集66巻2号89頁

（正式） 最高裁判所判決平成24年2月2日最高裁判所民事判例集66巻2号89頁

生成AIへの入出力を 繰り返したアイデアと特許

Q

生成AIへの入出力を繰り返したアイデアについて特許を受けることができますか。

A

生成AIに発明のアイデアをプロンプトとして入力し、あるいは出力させることで、特許を受けるための要件である新規性を満たさなくなるおそれがありますので、一定の注意を払うことが必要です。

1 生成AIによる発明の支援

発明を創作する過程は、一般に、着想と具体化の過程に分けることができます。そのそれぞれの過程で生成AIを利用することができ、たとえば、技術的な課題やその解決のニーズを探索するために生成AIと議論したり、新しい技術のアイデアの有効性や問題点について生成AIにレビューをさせたりすることが考えられます。

こうした過程では、利用者が自らのアイデアをプロンプトとして生成AIに入力したり、アイデアに当たる情報を生成AIに出力させたりします。また、特許出願に必要な書類の作成に生成AIを利用しようとする場合は、特許を受けようとする発明が記載された特許請求の範囲（クレーム）を含む、**発明の技術内容の入出力**を行うこととなります。

利用者と生成AIとのこうした相互作用は、共同発明者や発明の補助者とのコミュニケーションに例えても違和感が少ないように見えます。ただ、外部の事業者が管理する生成AIとの間でそうしたやり取りを行うに当たっては、複数の人間の手で発明を創作する場合と同様、発明を適切に扱うための措置が必要なのではないかという疑問が生じます。

2 特許発明と新規性

特許を受けることができる発明の条件の一つとして、**その発明が今までにない新しいものであること（新規性）**が必要です。特許法は、特許出願前に「日本国内又は外国」で、①「公然知られた発明」、②「公然実施をされた発明」、③「頒布された刊行物に記載された発明又は電気通信回線を通じて公衆に利用可能となった発明」のいずれにも該当しない発明について特許を受けることができると規定しており（特許法29条1項）、こうした発明には新規性があると評価されます。

この中で、公然知られた発明の「公然」とは、その発明が秘密状態を脱したことをいいます。これは、発明者や出願人のために秘密を守るべき関係のない**不特定の人に対して公になること**をいいます。不特定の人が多いか少ないかは関係なく、たとえば、秘密を保持する義務を負わずに発明を知った者がわずか数名の場合でも、公然知られた発明となります。逆に、発明を知った者が多数いる場合でも、その全員が秘密を保持する義務を負う場合には、公然知られた発明といいません。

競合企業が先に同じ発明を公開した場合はもちろん、出願前に発明者自身が発明を公開した場合や、秘密にしていた発明が発明者の意に反して不特定の第三者に知られてしまった場合でも、新規性の喪失により特許を受けることができなくなります（ただし、新規性喪失の例外規定（特許法30条）が適用される場合を除きます）。たとえば、公然知られることとなった原因が日本国外で起こった場合でも、結果に影響はありません。

3 生成AIと発明の新規性

生成AIのサービスの大半は、（少なくとも現状では）クラウドベースで提供されており、利用者が生成AIにプロンプトを入力すると、そのプロンプトはインターネットを経由して外部のサーバに送信され、そこでの処理の結果が出力されます。つまり、生成AIに入力されたプロンプトは、生成AIの提供者が管理するサーバで取り扱われ、その上で何

生成AIモデルを 公開する際の利用条件

Q

生成AIのモデルを公開したいのですが、利用条件を定める際のポイントを教えてください。

A

モデルの使用場面や、望ましい使用方法、想定される利用者などを整理し、改変や再配布、商用利用の可否や条件を考えていきましょう。また、提供者の責任、著作権の表示義務、競合モデルへの使用制限なども検討することが望ましいと考えられます。

1 生成AIモデルの公開とライセンス

ソフトウェアを開発する個人や企業が、自らが開発した製品を無償で公開することがあります。時間や費用をかけて開発したソフトウェアをあえて公開する意図や目的は様々ですが、こうした場合の公開の方法としては、GitHubやHugging Faceのような**開発者向けのプラットフォーム**を利用するやり方が一般的です。

他のソフトウェアの場合と同様に、生成AIのモデルを公開すると、様々な目的をもった利用者のアクセスが可能になります。場合によっては、公開時に想定していなかった形でモデルを使用されたり、商用利用を望んでいなかったのに、カスタマイズされたモデルが他所で販売されたりするかもしれません。また、(そうした人は多くないでしょうが) モデルの利用者から、動作保証を求められたり、意図しない挙動によって損害を被ったと主張されたりするかもしれません。

そこで、生成AIのモデルを公開する際には、こういった場面でのどのように使ってほしいのか、という利用のルールを定めるために、また、

公開したモデルの利用者からのクレームから法的に自分の身を守るために、モデルの利用をどの範囲で、またどのような条件の下で許諾するかを定めることが望ましいと考えられます。

このような許諾を行う行為そのものや、許諾の範囲や条件などを定めた内容を一般に「**ライセンス**」と呼びます。では、その内容を定める際のポイントとして、こういったことを考慮すべきでしょうか。

2 生成AIモデルの利用許諾の範囲

まず、公開するモデルを**営利目的で利用してよいか**を明確にすることが重要です。非営利での利用に限定する場合は、たとえば、非営利での利用を定めるCreative Commons NonCommercial (CC NC) licenseが参考になります。また、Meta社のLlama3.3 Community License Agreementでは、Llama3.3をベースにした製品やサービスが月間7億人のアクティブユーザを超える場合には別途Meta社の許諾を受ける必要があるものの、大多数の利用者による商用利用を事実上認めています。

次に、公開するモデルを利用者が独自に**改変 (カスタマイズ)** したり、改変後の(あるいは派生した)モデルを**再配布**したりしてよいかを明確にします。改変されたモデルを再配布してよいとする場合は、ベースとなった元のモデルの著作権やその入手先の表示を義務付けることも検討します。こうした表示に加えて、Llama3.3ライセンスでは、改変後のモデルの名称には冒頭に「Llama」を含めることとされています。

また、公開するソフトウェアを利用者が再配布してよいとする場合、利用者の側で元のライセンスを変更しないよう求めるのが一般的ですが、生成AIのモデルの場合も同様の措置をとるべきでしょう(なお、参考までに、改変後のソフトウェアの改変部分の再配布や、公開するソフトウェアを含んだサービスの提供を許諾する条件として、元のライセンスを変更しないよう求めるケースや、商用目的での再配布やサービス提供を許諾しないケースもあります)。

公開するソフトウェアの再配布を許諾する場合にも、その著作権やラ

生成AIと「クラウド例外」

Q

クラウドサービスの場合、提供者の個人データの取扱いによって個人情報保護法上の扱いが異なるそうですが、生成AIとの関係を教えてください。

A

クラウドサービスの利用と個人データの第三者への提供に関して、実務で「クラウド例外」と呼ばれている考え方があります。生成AIとの関係でもこの考え方に留意することは重要です。

1 個人データとクラウドサービス

生成AIのサービスの大半は、インターネットを經由して提供・利用されます。このように、インターネットなどのネットワークを經由して提供される情報処理サービスを、**クラウドサービス**と呼びます。利用者は、このサービスを利用する際、自らの端末からデータをサービスの提供者が管理するサーバに送信し、サーバ側で行われた処理の結果を自らの端末に出力して利用します。

問題は、この自らの端末から送信したデータの中に他者から取得した**個人情報が含まれる場合**です。個人情報保護法では、個人情報データベース等を構成する個人情報を特に「個人データ」といいますが（個人情報保護法16条3項）、個人情報データベース等を利用する個人情報取扱事業者がこの個人データを第三者に提供する場合、本人の同意を得ることの要否を検討する必要があります。また、第三者が外国にある場合には、さらに追加の実務対応を検討することも必要となります（同法27条、28条参照）。

そのため、生成AIのサービスの利用者が他者から取得した（個人情

報を含む）データをそのサービス上で処理する際、サービスの利用者から提供者への個人データの提供があったと法的に評価されるかどうかは、サービスの利用者や提供者による個人情報保護法の実務対応に大きな影響が生じます。ここでは、実務で「**クラウド例外**」と呼ばれる考え方を中心に、この問題を検討していきます。

2 クラウドサービスと「クラウド例外」

個人情報保護委員会が公表する指針によれば、個人データの「提供」とは、個人データを自己以外の者が利用できる状態に置くことをいい、物理的に提供されていない場合でも、**ネットワーク等を通じて利用できる状態にあれば**（利用する権限が与えられていれば）、「提供」に当たると説明されています（個人情報保護法GL（通則編）2-17）。

一方で、個人情報保護委員会は、個人データを扱うために他社が提供するクラウドサービスを利用する場合でも、そのサービスを提供する事業者自身がその**個人データを取り扱わないこと**となっている場合には、**その事業者が個人データを提供したことにはならない**という見解を、次のように解説しています（個人情報保護法Q&A7-53）。いわゆる「クラウド例外」とは、この考え方を指すものです。

……クラウドサービスの利用が、本人の同意が必要な第三者提供（法第27条第1項）……に該当するかどうかは、……クラウドサービスを提供する事業者において個人データを取り扱うこととなっているのかが判断の基準となります。

当該クラウドサービス提供事業者が、当該個人データを取り扱わないこととなっている場合には、当該個人情報取扱事業者は個人データを提供したことにはならないため、「本人の同意」を得る必要はありません。

……当該クラウドサービス提供事業者が、当該個人データを取り扱わないこととなっている場合は、契約条項によって当該外部事業者がサーバに保存された個人データを取り扱わない旨が定められており、適切にアクセス制