

生成A I の法律問題

Legal issues regarding generative AI

(神奈川県弁護士会 IT 法研究会)

飯田直久、佐藤隆志 (総合監修、はじめに)

内山浩人 (第1章 生成A I と著作権)

川添利賢 (第2章 生成A I と個人情報保護法)

遠藤政尚 (第3章 A I と不正競争防止法)

はじめに

生成AI (Generative AI : ジェネレーティブ AI) とは、一言で言うと新たなコンテンツを創造できるAI (人工知能) である。2022年11月に対話型生成AIが公開されて以後、各検索サイトを中心として爆発的に普及した。決められた行為の自動化が目的だった従来のAIと異なり、生成AIは、与えられた課題や情報により、データのパターンや関係を学習・解析し、新しいコンテンツを生成する。そのため、容易に人が作成したものと同等、あるいはそれ以上の質を有するコンテンツを自動で生成できることから、既存のビジネスや業務のあり方を変えていく存在として注目を集めている。他方で、生成されたコンテンツの権利帰属や既存の著作物との問題、個人情報や機密情報のコントロール、生成されたコンテンツの犯罪利用といった新たな問題が生じ、これに対する法規制が不可欠となってきた。

本論稿では、生成AIの登場によって、新たに生じるであろう幾つかの法的課題について、現段階で可能な限りの紹介・分析を試みた。本論稿が、生成AIを巡る今後の法的問題に対処するにあたって、読者の一助となれば幸いである。

第1章 生成A I と著作権¹

第1 著作権総論

1 目的

著作権法は、著作物の公正な利用に留意しつつ、著作者等の権利の保護を図ることで文化の発展に寄与することを目的としており(法1条)、そのため、著作権法では、各種規定で権利者等の権利・利益の保護と著作物等の円滑な利用とのバランスをとっている。

2 対象物 (著作物)

著作権法では、思想・感情の創作的表現を「著作物」として保護の対象とされており、アイデアそのものや単なるデータ自体は保護対象とされていない(法2条1項1号)。

3 著作者、著作権者

著作物を創作するものを著作者といい(法2条1項2号)、著作者が著作物を創作した時点で著作権を取得し、とくに手続なく著作権者となる(法17条1項、2項)。

4 権利 (支分権)

著作権者の権利は、大きく分けて著作者人格権と(狭義の)著作権に分けられる。

このうち、狭義の著作権の具体的な内容は、著作物の利用形態ごとに支分権として定められている。

たとえば、執筆した文章を印刷・製本する際は複製権、これを書店で販売するには譲渡権、購入者が購入図書を私的にコピー・スキャンす

る行為は複製権（私的使用のための複製）、スクリーンしたものをネットにアップロードする行為は公衆送信権、といった具合である。

5 権利侵害（同一性・類似性+依拠性）

著作権が著作権（支分権）の対象とする行為をしようとする場合、原則として著作権者の許諾が必要であり（法 63 条 1 項）、それが無ければ原則として著作権侵害となる。

著作物が著作権侵害をしているかどうかが争点となる場合、一般には類似性（既存の著作物と同一、又は類似していること）、依拠性（既存の著作物に依拠して制作されたこと）の両方を満たすことが著作権侵害の要件とされている。

このうち、類似性については、単に両者が似ているというだけでは足りず、両者の創作的表現が共通していることまでが必要である。したがって、例えば「アイデア」や「単なる事実」が類似していても「表現」が類似しているとは言えず、また、ありふれた表現が類似していても「創作性」が類似しているとは言えないことになる。

また、依拠性については、既存の著作物に接してそれを自己の作品の中に用いたことが必要であり、偶然に一致したに過ぎないような場合は依拠性がないとなる。

6 著作権侵害に対する民事請求、刑事罰

仮に著作権侵害が認められた場合には、侵害行為の停止・予防措置の請求が認められる。

また、侵害により損害を被った場合は損害賠償請求が認められる。

また、故意の著作権侵害行為は刑事罰の対象にもなっている。

7 例外（私的複製、引用、学校等）

著作権者の許諾がない場合であっても、私的利用のための複製（法 30 条）、引用（法 32 条）、教育機関における複製（法 35 条）等、著作物の利用が認められている場合がある。

第 2 生成 AI による著作権侵害

1 総論

一般的に、生成 AI の開発から利用までの流れをみると、学習データを収集・加工して学習用データセットを用意し、これを学習プログラムに入力してパラメータ等の調整をもって学習済みモデルを作成する①開発・学習段階と、この学習済みモデルがセットされた推論用プログラムに対して指示、入力することにより AI 生成物を出力する②生成・利用段階がある（第 2 章の図表を参照）。

生成 AI と著作権について考えるにあたり、生成 AI の開発・学習段階と生成・利用段階では著作物の利用行為が異なっていることから、これを分けて考える必要がある。

2 ①開発・学習段階

この段階では、学習プログラムに入力する学習用データセットを用意するため、学習用データを収集・加工することになる。

従前、この段階で、他人の著作物を学習用データとして用いることが、著作物の複製、譲渡、公衆送信等に該当し、著作権の侵害にあたるのではないか、といった議論があった。

この点、仮に著作権を侵害するとなれば、あらかじめ著作権者の許諾が必要ということになるが、実際、数億点以上となる大量の学習データについて個別に許諾を得ることは不可能、非現実的である。

この点に関しては、技術革新や社会の変化に対応するためには著作物の柔軟な利用が必要であるとして、平成 29 年 4 月に著作権法の改正が行われ、30 条の 4（著作物に表現された思想又は感情の享受を目的としない利用）が新設されている²。

著作物が入力される段階と出力される段階とに分けたうえで、入力段階では通常著作物の表現を享受しない利用であり、著作権者の不利益は生じないと考えられる点を踏まえ、新設された同条項では、原則として著作権者の許諾なく利用できるとした（著作権の権利制限規定）。

もっとも、著作権者の許諾がいらないとされ

るのは「著作物に表現された思想又は感情の享受を目的としない利用」に限るという制限があるが、AI 開発・学習のための情報解析や機械学習のような利用行為は、通常、著作物に表現された思想・感情の享受を目的としない行為となるので、著作権者の許諾なく行うことが可能となっているのが現状である。

これにより、生成 AI の学習段階での著作物の利用は広く認められるようになったといつてよいが、同条項は、そのただし書きで、その利用が著作権者の利益を不当に害することとなる場合は著作権者の許諾が必要であるとしている。具体例としては、すでに大量の情報を容易に情報解析に活用できる形で整理したデータベースの著作物が販売されている場合に、当該データベースを情報解析目的で複製等する行為などが考えられる³。

3 ②生成・利用段階（複製・翻案等、公衆送信・譲渡等）

生成 AI を利用して生成した生成物について、それが著作権侵害となるかどうかは、人が生成 AI を利用せずに生成した場合と同様の判断がされることになる。

つまり、創作的表現の部分が共通しているのか、他人の著作物に依拠しているのか、といった点から著作権侵害の有無が判断されることになる。

このうち、依拠性については、生成 AI を利用した場合にどのようなケースで依拠性が認められるかについては難しい判断が迫られる場合も考えられる。

例えば、生成 AI 利用者が既存の著作物を認識しており、生成 AI を利用してこれに類似するようなものを生成させた場合は依拠性を認めてもよいのではないかと、生成 AI 利用者が ImageToImage、すなわち既存著作物を直接学習させた場合には依拠性を認めてもよいのではないかと、といったような考え方がある

また、特定のクリエイターの著作物を集中的に学習させた場合の有無で依拠性に違いはあ

るか、といったことや、逆に、既存著作物と類似していれば依拠性を推認してもよいのではないかと、といった考え方もある。

実際のところはケース・バイ・ケースで検討することになると思われるが、偶然の一致・類似を排除するため、生成 AI 利用者のある程度の意図的な行為は必要になるのではないかとと思われる。

第3 AI生成物の著作権

1 AI生成物は著作物にあたるか

この点に関しては、従前より、そもそも AI が自律的に生成したものは、「思想又は感情を創作的に表現した」ものとは言えないとして、著作物には該当しないという考え方が示されてきた^{4 5 6 7}。

これに対し、人が思想又は感情を創作的に表現するための道具として AI を利用した場合は、生成物は著作物といえとされている。

つまり、その生成物に著作権が認められるか否かは、生成 AI が自律的に生成したのか、人が「道具」として生成 AI を利用して生成したのか、が判断基準ということになる。

この「道具」として生成 AI を利用したといえるためには、利用した人に創作意図があるか、人が創作的寄与をしたかによって判断されることになる。

ただ、この区別は観念的には理解できるとしても、実際、「AI が自律的に生成したか」「AI を道具として利用したか」といった基準は曖昧であり、実際は、その中間的な生成物、曖昧な生成物が多数を占めるであろう。この点は、今後の事例の集積が待たれる。

2 著作権者は誰か

前段の結果、AI 生成物が著作物と認められるのであれば、その生成を行った AI 利用者自身が生成物の著作者ということになる。

第2章 生成AIと個人情報保護法

第1 個人情報保護法制

I 個人情報保護法の目的

個人情報保護法第1条は、「この法律は、デジタル社会の進展に伴い個人情報の利用が著しく拡大していることに鑑み、・・・個人情報の有用性に配慮しつつ、個人の権利利益を保護することを目的とする。」と定めている。

デジタル社会の形成は、我が国の国際競争力の強化及び国民の利便性の向上に資するとともに、急速な少子高齢化の進展への対応その他の我が国が直面する課題を解決する上で極めて重要であるが(デジタル社会形成基本法1条)、その反面、デジタル社会においては、個人情報は、フィッシング詐欺によるパスワード盗用や、SNSによるフェイク情報の投稿等によって、たやすく不正使用され、日常、重大な権利利益の侵害が引き起こされている。このような現代社会が置かれた状況を踏まえて、個人情報保護法は、「個人情報の有用性に配慮しつつ、個人の権利利益を保護する」ものとして制定されたのである。

個人情報の保護は、従来、プライバシー権や自己情報コントロール権という個人の権利利益の侵害に対する損害賠償や差止による救済という形で行われてきた。しかし、一旦社会に流出した個人情報は、回収することが困難であり、しかも、それによって生じた権利利益の侵害は、損害賠償や差止によっては救済されない深刻な爪痕を残すことが珍しくない。そこで、個人情報保護法は、このような権利利益の侵害発生の原因をなす個人情報自体の取扱いを規制することによって、発生した侵害の事後的な救済ではなく、侵害の発生を未然に防止しようとする法制なのである。

II 個人情報保護法制形成の経緯

個人情報保護法は、次のような経緯を経て、現行法に至っている。

1 OECD勧告

コンピューターによって大量の個人情報が処理され、また、それがインターネットによって国内外に頻繁に伝達される社会が出現する

中で、個人情報そのものの取扱いに関する法的規制が必要になり、海外では、各国で、個人情報に関する法制を整え始めた。

しかしながら、国によって法制が異なるのは、国際取引で、種々個人情報に関するトラブルが発生することは必至であるため、1980年、OECDが、「プライバシー保護と個人データの国際交流についてのガイドラインに関するOECD理事会勧告」(以下「OECD勧告」という。)を発し、その中で、OECD8原則が定められた。

このOECD8原則は、①収集制限の原則、②データ内容の原則、③目的明確化の原則、④利用制限の原則、⑤安全保護の原則、⑥公開の原則、⑦個人参加の原則及び⑧責任の原則である。上記各原則の内容は、後記「OECD8原則と個人情報取扱事業者の義務規定の対応表」中で説明する。

2 個人情報保護法の制定・改正

OECD勧告の影響を受けて、我が国でも、地方公共団体毎に、個人情報保護条例が制定され、1988年に、国の行政機関を対象とする「行政機関の保有する電子計算機処理に係る個人情報の保護に関する法律」(以下「旧行個法」という。)が制定された。

これに対し、民間部門を対象とする包括的な法律はなく、私人間における個人情報保護は、自主規制に委ねられていた。

ところが、1995年に「EU個人データ保護指令」(以下「EU指令」という。)が制定され、このEU指令には、個人データの第三国への移転は、十分性(当該第三国が十分な保護措置を確保していること)が認定された場合に限って行うことができるとの条項(25条)が定められていた。

加えて、我が国では、この当時、住民基本台帳ネットワークの導入が計画されていたが、その導入に、民間部門での個人情報の規制が条件とされていたことから、2003年に、民間部門を対象とする個人情報保護法(以下「旧個人情報保護法」という。)が制定された。これと相前後し

て、旧行個法の改正が行われ、さらに独立行政法人等個人情報保護法(以下「独個法」という)が制定された。

その後、インターネットの飛躍的な発達により、大量な個人データの蓄積と利用、個人情報のグローバルな流通が生じたことを背景として、2016年にEU一般データ保護規則(GDPR)が制定された。この規則は、適用対象諸国に直接適用されるものであった。このような中で、2021年に個人情報保護法の抜本改正が行われた。

この改正は、旧個人情報保護法、改正旧行個法及び独個法を、個人情報保護法一本に統合し、個人情報保護委員会を置き、同委員会により、民間、行政及び独立行政法人の監視監督を行うというものであった。

3 個人情報保護法の内容

個人情報保護法の民間部門における規制内容は、下記表のとおり、OECD8原則に対応する個人情報取扱事業者の義務として定められている。

「OECD8原則と個人情報取扱事業者の義務規定の対応表」⁸

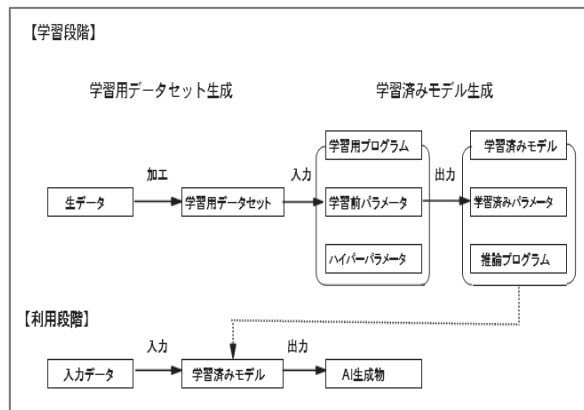
OECD8 原則	個人情報保護法
③目的明確化の原則(収集目的を明確にし、データ利用は収集目的に合致すべき)	15 条(利用目的をできる限り特定) 16 条(利用目的の達成に必要な範囲を超える取扱不可)
④利用制限の原則(データ主体の同意ある場合や法律の規定による場合以外は目的以外に利用してはならない)	23 条(本人の同意得ずに第三者提供不可)
①収集制限の原則(適法・公正な手段により、かつ情報主体に通知または同意を得て収集されるべき)	17 条(偽りその他不正手段による取得不可)
②データ内容の原則(利用目的に沿ったもので、	19 条(正確かつ最新の内容を保つよ

かつ、正確・完全・最新であるべき)	う努める)
⑤安全保護の原則(合理的安全保護措置により、紛失・破壊・使用・修正・開示等から保護すべき)	20 条(安全管理のために必要な措置) 21 条(従業員・委託先に対する必要な監督)
⑥公開の原則(データ収集の実施方針等を公開し、データの存在、利用目的、管理者等を明示するべき)	18 条(取得したとき利用目的を通知又は公表) 24 条(利用目的を本人の知り得る状態に置く)
⑦個人参加の原則(自己に関するデータの所在及び内容を確認させ、又は異議申立てを保障すべき)	25 条(本人の求めに応じて保有個人データを開示) 26 条(本人の求めに応じて訂正等) 27 条(本人の求めに応じて利用停止等)
⑧責任の原則(管理者は諸原則実施の責任を有する)	31 条(苦情の適切かつ迅速な処理に努める)

第2 生成AIで個人情報保護法が問題となる局面

I 生成AIの生成・利用過程

生成AIには、「生データ」を加工して「学習用データセット」を作成し、これを「学習用プログラム」に入力して、「学習済みモデル」を生成する開発(学習)段階と、生成された「学習済みモデル」に「入力データ」を入力して、「AI生成物」を出力させる利用段階がある(下図参照)。



例外はあるが、原則的には、学習段階を担う者は、AI 開発者と AI サービス提供者であり、利用段階を担う者は、AI 利用者である。

1 学習段階

(1) 学習段階での生成過程

学習段階では、①クロウリングにより収集したデータや、ユーザやベンダが一次的に取得したデータを「生データ」とし、②これに、欠損値や外れ値の除去、ダミー変数変換等の前処理や、ラベル情報の付加等の別個情報の付加等の変換・加工処理を施して学習用データセットを作成し、③これを「学習前パラメータ」（学習用データセットの中から一定の規則を見出し、その規則を表現するモデルを作成するためのアルゴリズムを実行するプログラム）と「ハイパーパラメータ」（アルゴリズムの挙動を制御する）から成る「学習用プログラム」に入力して、「学習済みパラメータ」（一定の目的のために機械的に調整されたパラメータ）と「推論プログラム」（学習済みパラメータを適用することで、入力に対して一定の結果を出力することを可能にするプログラム）から成る「学習済みモデル」を生成するという作業が行われる（平成30年6月経済産業省「AI・データの利用に関する契約ガイドライン-AI 編-」「第2 AI 技術の解説」3 想定する AI 技術の実用化の過程」）。

(2) 学習段階で生ずる個人情報保護法上の問題

学習段階では、次のような、個人情報保護法上の問題が生ずる。

① 利用目的規制適用の有無

個人情報保護法には、個人情報取扱事業者が、個人情報を取り扱う⁹⁾に当たっては、利用目的をできる限り特定しなければならない（17条1項）、個人情報を取得した場合は、予め利用目的を公表している場合を除き、速やかに、その利用目的を本人に通知又は公表しなければならない（21条1項）、予め本人の同意を得ないで、利用目的の達成に必要な範囲を超えて個人情報を取り扱ってはならない（18条1項）という「利用目的規制」が定められている。

学習用モデルの生成に、「利用目的規制」が適用されるとすると、取得したデータに、個人情報が含まれている場合には、そのデータを使って「学習済みモデル」を生成するに当たって、取得時に特定した利用目的の達成に必要な範囲に、AI モデルの開発を行うことが含まれるのであれば、そのまま、「学習済みモデル」を生成することができるが、これが含まれない場合には、本人の同意を得なければならないことになる。

しかしながら、「学習済みモデル」を生成する過程には、利用目的規制が適用されることはないとする有力説がある（中井杏「AI 開発における学習用データの利用目的と学習済みパラメータの取扱い」NBL1254号46頁（以下「中井論文」という。））、岡田淳・北山昇・小川智史「AI と個人情報・プライバシー」NBL1244号75頁）。

中井論文は、「学習済みモデル」について論じる前に、まず、参考として、「統計情報の作成」について論じ、個人情報から統計情報を作成することも「取扱い」に含まれるから第17条1項に基づき利用目的を特定しなければならない筈だが、『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（以下「ガイドラインQ&A」という。）2-5は、個人情報を特定の個人を識別することができない態様に統計処理して利用する場合、利用目的として特定する必要があるかという問いに対して、「利用目的の特定は『個人情報』が対象であるため、個人情報に該当しない統計データは対象とな

りません。また、統計データへの加工を行うこと自体を利用目的とする必要はありません。」と回答していることを挙げて、これは、統計データの「特定の個人を識別することができない」という性質に着目して、利用目的を不要とするものであるとする(その理由付けの詳細は脚注 10 参照)。¹⁰

そして、「個人情報の保護に関する法律についてのガイドライン(仮名加工情報・匿名加工情報編)3-1-1」が、「統計情報は、特定の個人との対応関係が排斥されている限りにおいては、法における「個人に関する情報」に該当するものではない」としていることを指摘した上で、「学習済みモデル」についても、「ガイドライン Q&A1-8」が、複数人の個人情報を機械学習の学習用データセットとして用いて生成した学習済みパラメータ(重み係数)は、学習済みモデルにおいて、特定の出力を行うために調整された処理・計算用の係数であり、当該パラメータと特定の個人との対応関係が排斥されている限り、「個人に関する情報」に該当するものではないため、「個人情報」にも該当しないとしていることを指摘し、したがって、出力に至るまでの全過程において、特定の個人との対応関係が排斥された非個人情報である学習済みパラメータを利用するために学習用データを利用するのであれば、利用目的規制の対象外であるとしている。

中井論文に対して、a「学習済みパラメータ」、それに基づいてプロファイリングが行われる等個人(本人に限らない)の評価に用いられる場合がある点で、統計データとは必ずしも同じでないこと、b 令和 2 年改正で導入された「仮名加工情報」(個人情報に含まれる記述の一部を削除する等して、他の情報と照合しない限り特定の個人を識別することができないように個人情報を加工して得られる個人に関する情報)の代表的な利用例として、「機械学習モデル」の「学習用データセット」が想定されたこと、c「学習済みパラメータ」の作成に、利用目的の

特定が不要だとすると、その行為は、第 17 条 1 項の個人情報の「個人情報を取り扱う」ことに該当しないことになり、漏えい等の報告(26 条)や不適正利用の禁止(19 条)のではないかという疑問が出てくるという問題点が指摘されている(中井論文に付加された「曾我部教授からのコメント」NBL1254 号 52 頁)。

「学習済みモデル」生成に、利用目的規制が適用される場合(適用説を取った場合、又は、不適用説でも、出力までの全過程で、特定の個人との対応関係が排斥されていない場合)、利用目的は、最終的に達成しようとする目的を特定すれば足りるが、「個人情報の保護に関する法律についてのガイドライン(通則編)(以下「ガイドライン通則編」という。)3-1-1」は、最終的にどのような事業の用に供され、どのような目的で個人情報を利用されるのかが、本人にとって一般的かつ合理的に想定できる程度に特定することが望ましいとし、プロファイリングの事例を念頭に、「取得した閲覧履歴や購買履歴等の情報を分析して、趣味・嗜好に応じた新商品・サービスに関する広告のために利用いたします。」「取得した行動履歴等の情報を分析し、信用スコアを算出した上で、当該スコアを第三者へ提供いたします。」との特定の事例を示している。前者は、取得した個人情報を、学習済みモデルで分析する場合、後者は、取得した個人情報を学習用データとして使用する場合を示している。

② 要配慮個人情報の取得

前記 EU 一般データ保護規則(GDPR)は、第 6 条で、個人情報の「取扱い」の適法性の根拠を定めており¹¹、その適法性根拠の一つとして、「同意」を定めている。

これに対して、我が個人情報保護法は、個人情報の「取扱い」に、一般的に、適法性根拠を求めておらず、一定の場合にだけ、本人の同意が必要としている。

その一つが要配慮個人情報であり、第 20 条 2 項で、個人情報取扱事業者は、同項に定められ

た例外の場合を除いては、あらかじめ本人の同意を得ないで要配慮個人情報を取得(「取得」は、「取扱い」の一つ。脚注9参照)してはならないとされている(20条2項)。

要配慮個人情報とは、本人の人種、信条、社会的身分、病歴、犯罪の経歴、犯罪により害を被った事実その他本人に対する不当な差別、偏見その他の不利益が生じないようにその取扱いに特に配慮を要するものとして政令で定める記述等が含まれる個人情報である(2条3号)。

生成AIの学習段階では、大量の「生データ」が必要になるため、これを新たに取得する場合には、ウェブで公開されている情報のクロールが行われるが、そこで取得する情報の中に要配慮個人情報が含まれていることは多々あり、これを避けることは容易でない。

その情報が、本人がSNS等で公開したものであったり、国の機関、情報機関等が、ウェブサイトで公開しているものであったりすれば、第20条2項7号の除外事由に該当することになるが、それ以外の除外の事由該当性の判断は難しく、個人情報保護法上は、本人の同意を得ることが必要となる場合が多いであろうが、クロールで収集した個人情報につき、本人に同意を得ることは、実際には不可能に近く、法の形式的な適用は躊躇されるところである。

これに関連して、個人情報保護委員会は、令和5年6月1日付けで、OpenAI, L.L.C. 及び OpenAI OpCo, LLC に対し、個人情報保護法に基づき、注意喚起を行っているが、その中で、あらかじめ本人の同意を得ないで、ChatGPTの利用者及び利用者以外の者を本人とする要配慮個人情報を取得しないよう注意喚起しており、機械学習のために情報を収集することに関する遵守事項として、a 収集する情報に要配慮個人情報が含まれないよう必要な取組を行うこと、b 情報の収集後できる限り即時に、収集した情報に含まれ得る要配慮個人情報をできる限り減少させるための措置を講ずること、c 上記a及びbの措置を講じてもおお収集した情報

に要配慮個人情報が含まれていることが発覚した場合には、できる限り即時に、かつ、学習用データセットに加工する前に、当該要配慮個人情報を削除する又は特定の個人を識別できないようにするための措置を講ずること、d 本人又は個人情報保護委員会等が、特定のサイト又は第三者から要配慮個人情報を収集しないよう要請又は指示した場合には、拒否する正当な理由がない限り、当該要請又は指示に従うことの4点を定めている¹²。

2 利用段階

(1) 利用段階での生成過程

利用段階では、①AI利用者が保有するデータを「入力データ」とし、②これを「学習済みモデル」に入力して、③「AI生成物」としてのデータを出力するという作業が行われる。

(2) 利用段階で生ずる個人情報保護法上の問題

利用段階では、次のような、個人情報保護法上の問題が生ずる。

① 利用目的規制

利用段階では、個人情報を「学習済みモデル」に入力して、データを出力するのに、利用目的規制の適用があることについて、異論はない。

個人情報保護委員会令和5年6月2日作成の「生成AIサービスの利用に関する注意喚起等について」の「別紙(1) 生成AIサービスの利用に関する注意喚起等」の「(1) 個人情報取扱事業者における注意点」①には、「個人情報取扱事業者が生成AIサービスに個人情報を含むプロンプトを入力する場合には、特定された当該個人情報の利用目的を達成するために必要な範囲内であることを十分に確認すること。」との注意喚起があるが、これは、利用段階における利用目的規制を前提とする注意喚起である。

② 要配慮個人情報の取得

前述のとおり、要配慮個人情報は、第20条2項で、個人情報取扱事業者は、同項に定められた例外の場合を除いては、あらかじめ本人の同意を得ないで取得することができないとされ

ている。

しかしながら、要配慮個人情報に該当しない個人情報を「学習済みモデル」に入力して、プロファイリングにより、「AI 生成物」として、要配慮個人情報を出力させれば、同意を得ないで、要配慮個人情報を入手できることになる。

この場合、AI によるプロファイリングにより、要配慮個人情報を生成することを、第 20 条 2 項の「取得」に当たり、本人の事前の同意がない限り、同条違反を構成するという説(山本龍彦「プライバシーの権利を考える」(信山社 2018)266 頁)と、これを「取得」とすることは、一般的には難しく、実際には、出てきた結果は、第 20 条 2 項の例外で読めてしまうものが多いとする説(宇賀克也—藤原静雄—山本和徳「(鼎談) 個人情報保護法改正の意義と課題」行政法研究 13 号(2016)11 頁藤原発言)がある。

プロファイリングにより出力された情報は、生成 AI による推測に過ぎないが、元々、本人と個人情報の結び付きも、一定の根拠に基づく認定であって、その差は相対的なものに過ぎず、この点で、プロファイリングによる要配慮個人情報の入手への第 20 条 2 項の適用を否定することはできない。ただ、プロファイリングにより出力される個人情報は、精度のかなり低いものまで含まれるのであるが、これが、本人の属性として出力される以上、未だ、本人にとって自己でコントロールする必要のある情報ということができ、要配慮個人情報が他人に入手されることによって、極めて深刻な利益侵害が生じ得ることも考え併せれば、この場合も、第 20 条 2 項の適用があると考えるのが相当であろう。

なお、プロファイリングにより生成されるのが、本人の信条等、不当な差別、偏見を生じさせる個人情報を含む記述であっても、その個人情報が、本人の属性でなく、それを推定させる事実に残る場合には、第 20 条 2 項の問題は生じない。ガイドライン Q&A1-27 は、そのことを示している。

③ 第三者提供規制

個人情報保護法第 27 条 1 項は、個人情報取扱業者が、個人データを第三者に提供する場合には、同項の定める除外事由に該当する場合を除き、あらかじめ、本人の同意を得ることが必要であるとする。

利用段階では、プロンプトとして入力された個人データが、機械学習に利用される場合には、それが新たに「学習用データセット」に組み込まれることによって、AI サービス提供者に「提供」されることになる。

個人情報保護委員会令和 5 年 6 月 2 日作成の「生成 AI サービスの利用に関する注意喚起等について」の「別紙(1) 生成 AI サービスの利用に関する注意喚起等」の「(1) 個人情報取扱事業者における注意点」②は、「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。」と注意喚起しているが、それは、このことを言っているものと考えられる。

なお、ガイドライン Q&A7-53 では、個人情報取扱事業者がクラウドサービスを利用している場合、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ときには、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ず、本人の同意を得る必要はないとしている。

第 3 章 AI と不正競争防止法

1 総論

(1) 不正競争防止法は、事業者間の公正な競争等を確保するため、不正競争の防止及び不正

競争に係る損害賠償に関する措置等を講じ、もっても国民経済の健全な発展に寄与することを目的としており（1条）、「不正競争」となる様々な行為を定義している（2条）。不正競争によって営業上の利益を侵害され又はそのおそれがある場合には差止請求権（3条）、故意又は過失により不正競争を行って営業上の利益を侵害した場合には損害賠償請求権（4条以下、また故意又は過失により不正競争を行って営業上の信用を害された場合には信用回復の措置請求（14条）など民法上の不法行為の特別法として定められている。

（2）生成AIとの関係では、生成段階と利用段階とに分けて検討する必要があるが、他の事業者との問題になるのは主に利用段階と思われる。そこで、生成AIの利用段階として思われる4つの「不正競争」行為について検討していく。

2 形態模倣商品の提供行為（2条1項3号）

（1）「他人の商品の形態を模倣」した商品の譲渡等をする行為を「不正競争」として禁止されている（同号）。

（2）「商品の形態」とは、「需要者が通常の方法に従った使用に際して知覚によって認識できる、商品の外部及び内部の形状並びに形状に結合した模様、色彩、光沢及び質感」を言うと言われている（同条4項）。これに関して、ソフトウェアが「商品」に当たるとしたうえで、ソフトウェアを操作して表示される画面の形状、模様、色彩等は「形態」に当たり得るとした判示がある（東京地判H30.8.17）。そのため、AIが生成したソースコードに基づいて作成したソフトウェアやWebサイトの表示について、それが模倣するものであれば不正競争として禁止される行為となる。

また、生成AIを用いて他者の製品自体の形態を模倣するものであれば、同様の禁止行為となる。

（3）「模倣する」とは、他人の商品の形態に依拠して、これと実質的に同一の形態の商品を作り出すことをいう（同条5項）。この依拠性につ

いては、著作権法と同様の問題となる。

この依拠性については、人自らがソフトウェア等の表示等の商品を作るときは、依拠するものがあるかどうか当然認識することができるが、生成AIを利用する場合には、そもそも依拠するものの内容が分からないばかりか、実質的同一性の判断もしようがない状況にある。それゆえ、生成AIを利用したソフトウェア等の表示等の商品が知らないうちに模倣してしまい、不正競争としての禁止行為に抵触してしまっていることが十分想定される。

この依拠性の認識の有無・程度といった主観的要件について見解が分かれると思われるが、「不正競争」の定義の仕方からすると、基本的には主観要件は想定されていないと考えられ、著作権法における依拠性の考え方と必ずしも合わせる必要はなく、依拠性の認識は不要であると考ええる。形態模倣商品の提供行為をした者が、損害賠償や措置回復の責任を負うかは故意又は過失が必要となるので、行為者の主観性はここで検討されるべきである。もっとも、生成AIをどのように利用した場合に過失が認められるかについて、事例判断によるが、生成AIが膨大なデータ量から既存商品を模倣した可能性が考えられるところ、この可能性をもって直ちに過失を認めることは難しいと思われる。

（4）生成AIを利用した商品については、事業として譲渡等をする場合には特に注意が必要である。一方で、生成AIを活用した商品開発を抑制する働きになってしまう。現在、「生成AIを巡る競争」について公正取引委員会が検討を始めたところである（令和6年10月、ディスカッションペーパー）。

3 「営業秘密」の侵害（2条1項4号ないし10号）

（1）窃取等の不正の手段によって営業秘密を取得し、自ら使用し、もしくは第三者に開示する行為等は、「不正競争」として禁止されている。

（2）「営業秘密」とは、秘密として管理されている生産方法、販売方法その他の事業活動に有

用な技術上又は営業上の情報であって、公然と知られていないものをいい(同条6項)、秘匿されるべき営業上の秘密が保護されている(①秘密管理性、②有用性、③非公知性)。

(3) 生成AIとの関係では、例えば、管理権限のない従業員が営業秘密の情報を生成AIに入力をして利用する場合が想定される。そのように生成AIの利用がされると入力された情報(営業秘密)が蓄積されていて、他人が生成AIを利用した際にその営業秘密である情報を知ってしまうことになる。

(4) このような場合、従業員が秘密情報を生成AIに入力して利用した時点で、①秘密管理性が失われると指摘されることもあるが、この要件は管理の問題であって従業員の問題行為によって直ちに秘密管理性が失われることにはならないと考える。また、③非公知性については、他人が生成AIを通じて営業秘密を知ることになるので公知になると考えられるが、生成AIにより作成されたもの又はその一部が営業秘密であるかどうかは判別が難しいことを考えると直ちに公知になるとは言いきれないと思われる。

ここでの問題は、営業秘密が窃取等の「不正の手段」によって取得されて、第三者に開示する行為等が不正競争とされているのであるから、従業員が誤って生成AIに営業秘密を入力して利用し、その後に生成AIを利用した他人が営業秘密を知ることになり利用したとしても、その過程には窃取等の不正の手段はない。そのため、結果として「不正競争」に当たらず、不正競争防止法上の差止請求等はできないことになると考えざるを得ないであろう。

これについては、生成AIを活用した競争が想定される以上、立法による対応等が期待される。

(5) 実際の対処としては、事業者内の営業秘密の取り扱いを厳格にして、生成AIの利用がされないようにするか、生成AIを利用した際に情報(営業秘密)が蓄積されない方法にして

おく必要がある。

4 誤認惹起行為(2条1項20号)

(1) 商品・役務又はその広告等に、その原産地、品質・質、内容等について誤認させるような表示をする行為、またはその表示をした商品を譲渡等する行為は、「不正競争」として禁止されている。

(2) 例えば、地域とは何ら関係がないのに原産地の名称が商品名に使われている場合、実際には入っていない原材料が入っているかのような表示されている場合などがある。

生成AIを利用した場合、知らずにこのような誤認を惹起させる内容になっていてそのまま商品に表示したり、またはその表示された商品を譲渡等したりすると、不正競争として違反となる。

(3) 当然であるが、生成AI自体は、誤認惹起にあたるかどうかの判断はしないのであるから、利用する側が十分に気をつけなければならない。また、誤認惹起行為は、表示の問題であるから、利用者はその表示を認識することができるのであって、生成AIが作成したことをもって責任を免れる理由とはならないはずである。

5 信用毀損行為(2条1項21号)

(1) 競争関係にある他人の営業上の信用を害する虚偽の事実を告知し、または流布する行為は、「不正競争」として禁止されている。

(2) 「競争関係」とは、双方の営業につき、その需要者又は取引者を共通にする可能性があることで足りる。なお、非競争者間での誹謗行為等は、一般不法行為の問題となりうる。また、「他人」とは、他人の名称自体が明示されていなくても、告知等の内容および、業界内の情報等から、告知の相手方において「他人」が誰を指すのか理解できれば足りる。

(3) 生成AIを利用したところ、競争関係に他人の営業上の信用にかかわる内容が含まれている場合には、利用者にはその内容が虚偽であるかの判断は一見困難であるから、そのまま対

外的に表示する告知等に十分気をつけなければならない。

これに関して、生成 AI が作成した虚偽事実を含む内容を真実であると信じて告知等をした場合に、責任を免れることができるかが問題となり得る。生成 AI は必ずしも真実の内容を作成するとは限らず、生成 AI 自体に虚偽内容を排除するプログラムがされているわけではないことを考えると、社会通念の観点からして、生成 AI による作成をもって信じるに相当な理由があるとは言えないと考える。したがって、生成 AI をもって責任を免れるのはかなり難しいはずである。

¹ (参考) 文化庁著作権課「令和5年度著作権セミナー AIと著作権」(R5.6)

² 文化庁著作権課「デジタル化・ネットワーク化の進展に対応した柔軟な権利制限規定に関する基本的な考え方(著作権法30条の4、47条の4及び47条の5関係)」R1.10.24

³ 上記9頁第9問

⁴ 文化庁「著作権審議会 第2小委員会(コンピュータ関係) 報告書」S48.6

⁵ 文化庁「著作権審議会 第9小委員会(コンピュータ創作物関係) 報告書」H5.11

⁶ 知的財産戦略本部「次世代知財システム検討委員会報告書」H28.4

⁷ 知的財産戦略本部「新たな情報財検討委員会報告書」H29.3

⁸ 内閣府国民生活局個人情報保護推進室作成「個人情報の保護に関する法律」説明資料5

⁹ GDPR第4条2項には、『『取扱い』とは、自動的手段によるか否かを問わず、収集、記録、編集、構成、記録保存、修正若しくは変更、検索、参照、使用、送信による開示、配布、又は、それら以外に利用可能なものとする、整理若しくは結合、制限、消去若しくは破壊のような、個人データ若しくは一群の個人データに実施される業務遂行又は一群の業務遂行を意味する。』と定められている。

¹⁰ 中井論文は、その理由を、①ガイドラインQ&A公表前にあった『『個人情報の保護に関する法律』についての経済分野を対象とするガイドライン』等に関するQ&Aは、ガイドラインQ&A2-5と同様の問題について、同様の回答をするのに、「最終的な利用目的を特定すれば足りる」、「統計データへの加工の過程を特定す

る必要はない」と明言していたが、ガイドラインQ&A2-5では、そのような文言がなくなったこと、②Aという目的で統計データを作った後、その統計データをBの目的で利用する場合に、Bを利用目的として特定することは義務付けられておらず、当初のAだけ利用目的として特定しなければならないとすることは、個人情報保護法第1条の「個人の権利利益を保護すること」との関係で合理性がないこと、以上の2点から、ガイドラインQ&A2-5において、統計データへの加工を行うこと自体を利用目的とする必要がないとされているのは、最終的な利用目的を特定すれば足りるからではなく、統計データの性質自体に着目したものであると説明している。

¹¹ 前記EU一般データ保護規則(GDPR)では、第6条で、取扱いの適法性の根拠として、同意、契約の履行又は締結前のデータ主体の要求に際しての手段、管理者の法的義務の遵守、データ主体又は他の自然人の生命に関する利益保護、公共の利益又は管理者に与えられた公的な権限の行使における職務の遂行、管理者によって、又は、第三者によって求められる正当な利益前記EU一般データ保護規則(GDPR)では、第6条で、取扱いの適法性の根拠として、同意、契約の履行又は締結前のデータ主体の要求に際しての手段、管理者の法的義務の遵守、データ主体又は他の自然人の生命に関する利益保護、公共の利益又は管理者に与えられた公的な権限の行使における職務の遂行、管理者によって、又は、第三者によって求められる正当な利益

¹² 個人情報保護委員会作成令和5年6月2日付け「OpenAIに対する注意喚起の概要」