

生成AIビジネス活用における米国法規制と法的リスク



日系企業グループパートナー弁護士

山本 真理



ビジネス・トランザクション・アドバイザー

田中 剛

Barnes & Thornburg LLP

米国で事業展開する日系企業とその親会社に対して様々な法務サービスを提供する総合法律事務所です。日常の法務のみならず社内教育などの法務ソリューションも提供しています。以下の連絡先にお問い合わせ下さい。

One North Wacker Dr., Suite 4400

Chicago, IL 60606

Website: www.btllaw.com

連絡先

日系企業グループパートナー弁護士

山本 真理

Phone : 312-214-8335

E-mail: mari.regnier@btllaw.com

はじめに

生成AI (Generative AI) の急速な普及に伴い、そのビジネス利用が企業規模を問わず拡大している。しかしその一方で、生成AIの利用には様々な法的リスクが存在し、米国でビジネス展開する日本企業も無視できない課題となっている。ここでは、米国における生成AI関連の法規制の現状と、企業が実務で直面し得る主な法的論点を紹介する。

現行の米国法規制の枠組み

現在、連邦レベルでは生成AIやAI全般を直接規制する包括的な法律は制定されていない。そのため既存の法律（例えば著作権法、消費者保護法、差別禁止法など）をAI利用の文脈に当てはめて対応している状況である。もっとも、米連邦取引委員会 (FTC)や雇用機会均等委員会 (EEOC)、消費者金融保護局 (CFPB)、司法省 (DOJ) など各分野の規制当局は2023年4月の共同声明で、自らの管轄権はソフトウェアやアルゴリズム処理 (AIを含む) にも及ぶと明言しており、生成AIについても既存法に基づく執行を強める姿勢を示している。

連邦法が未整備な中、米国各州や特定分野で個別のAI関連規制が動き出している。

コロラド州は2024年5月、同州では初の包括的なAI法となる「コロラド州AI法 (Colorado AI Act)」を制定した。同法は高リスクAIシステム (人の重要な決定を自動化するもの) を開発・利用する事業者に対し、差別回避のための合理的措置やリスクアセスメント実施などの義務を課している。また、イリノイ州は、2024年8月に州差別禁止法 (Illinois Human Rights Act) を改正して雇用におけるAI利用を規制した。同改正法 (州法HB 3773) では、雇用主が人事評価や採用

にAIを用いる際に結果的に差別を生じさせることを禁じ、さらにAI利用について応募者・従業員への通知義務を課している。これにより、企業はAIツールによる人事判断が人種・性別等に与える影響を監視・軽減し、透明性を確保することが求められる。さらにイリノイ州は2024年5月、生成AIによる人物のデジタル複製 (いわゆるディープフェイク) から著名人の肖像権等を保護するため、州のパブリシティ権法を改正する「デジタル・レプリカ法」(HB 4875) も可決した。これは他人の画像や声を無断でAI生成することを禁じるものである。

このように米国内では州ごとに個別のAI関連法が生まれており、既存の連邦法の適用とも相まって、複雑な規制環境が形成されつつある。

生成AI利用に伴う主要な法的リスク

以上の規制動向を踏まえ、企業が生成AIを業務で活用する際に留意すべき主な法的リスクを整理する。

- **著作権に関わるリスク:** 生成AIが出力する文章や画像等が既存の作品と酷似し過ぎていた場合、ユーザー企業がその出力を利用および公開することで著作権侵害の責任を問われ得る。例えば、AIが既存の文章をほぼそのまま生成したり、有名キャラクターに酷似した画像を生成したりした場合が考えられる。したがって、企業としては、AI生成物をそのまま商用利用する場合、元データや類似作品の権利クリアランスが取れているか慎重に確認する必要がある。また、企業側の視点では、AIが生成した成果物には著作権が認められない場合がある点にも注意が必要だ。米国の著作権法制では一貫して「人間による創作性」を



保護の要件としており、完全に自動生成された作品は原則として著作物にならないと解されている。よって、企業が例えばAIに商品ロゴやデザインを丸ごと作らせた場合、それらには独占的権利を主張できない恐れがあることから、AI生成物を利用する際は必ず人による創意工夫（編集や選択など）を加えることで法的保護を確保することが望ましい。

- **機密情報・個人情報の漏洩リスク:** 社内機密データや顧客の個人情報扱う企業にとって、生成AI利用による情報漏洩リスクは重大な懸念である。まず、従業員がチャット型の生成AI（例：ChatGPT等）に業務上の機密事項や個人データを入力した場合、その情報がAIサービス提供者のサーバーに保存・分析され、第三者に漏洩する可能性がある。

また、企業がクラウド型AIサービスを利用する場合、サービス提供企業との間でデータ処理契約や秘密保持契約を結ぶのが一般的だが、生成AIはその性質上、入力データをモデル改善等に使用するケースがあり、契約で明確に禁止しておかないと知らぬ間に提供データが二次利用されかねない。特に顧客情報や従業員情報を扱う場合、AIベンダーとの契約でデータの利用目的および範囲、保存期間、第三者提供の有無などを厳格に規定しないと、自社がプライバシー違反の責任を問われるリスクがあるといえる。

- **誤情報・差別的アウトプット等に対する責任リスク:** 米国の消費者保護法制では、FTCが管轄する連邦取引委員会法第5条に基づき「不公平または欺瞞的な事業慣行」が禁止されている。生成AIを使って消費者を誤導したり操作

した場合、この条項に抵触するリスクがある。例えば、AIチャットボットがあたかも人間のように振る舞い信頼を得た上で特定の商品購入を誘導した場合、利用者に不利益を与えれば不公平なプラクティスと見なされる恐れがある。

また、差別的アウトプットに関しても既存の連邦法が適用される（差別禁止法や住宅公正法など）。企業がAIツールを利用した結果、特定の人種や性別に不利益を与えれば従来通り企業が責任を負うことになる。また、上記のとおり、コロラド州やイリノイ州では、AIによる間接的な差別を明確に禁じているところであり、企業はAI導入前に十分なテスト（バイアス監査）を行い、結果に人間のレビューを挟むなどして、差別的取扱いとならないようにする必要がある。

企業が取るべき対応策・ガバナンス

以上のリスクを踏まえ、生成AIを業務で利用する企業としては、以下のような対応策を講じることが望ましい。

- **社内ポリシー整備と社員教育:** ポリシーには、どういった用途でAI利用を許可するか、扱ってよいデータの範囲、成果物の取扱いを定める。また、社員がAIツールの仕組みとリスクを正しく理解することも不可欠であり、定期的な研修やポリシー共有を行うことが重要だ。
- **利用フローの管理・承認:** 社内ポリシーと連動して、AI利用の事前承認フローを設けることも有益といえる。例えば、新たに生成AIツールを業務導入する際は必ず法務またはIT部門の承認を得るプロセスを作ることが考えられる。また、プロンプト（AIへ

の入力内容）に機微情報を含める必要がある場合、上長や情報管理責任者のチェックを義務付ける等、人の目による制御を組み込むことも有効である。

- **テストと検証の実施:** 実運用の前に、生成AIツールの出力精度・バイアス傾向をテストすることも効果的な手続といえる。社内のデータやシナリオを用い、誤情報が出ないか、有害な内容を生成しないかなどを継続的に検証する。例えば、採用に利用されるAIであれば男女や人種で不利な結果が出ないかモニタリングし、もし偏りが検出されたらベンダーと協力してモデル調整や追加フィルターを講じるといった対応を行うことが考えられる。
- **最悪の事態への備え:** 万が一生成AIの利用に伴うインシデントが発生した場合の行動を予め想定しておくことも必要である。まず事実確認、ログ収集、利用停止など初動で被害拡大を防ぎ、法務、IT部門などで対応チームを組成する。続いて詳細な調査を行い、法律専門家も交えて、どのような法令に抵触する可能性があるのかを評価し、求められる対応をとる。そして、最終的に当該インシデントを踏まえた再発防止策を立てるといった流れが考えられる。

生成AIのビジネス活用は企業にとっても業務効率化やイノベーション促進の大きなチャンスである。しかし、AI活用の恩恵を享受するためには、そのリスクを制御する枠組みを備えることが不可欠である。米国においても生成AIに対する法規制は発展途上であるが、その動向に注意しながら、この新たな波を乗りこなしていただきたい。