 日刊（土曜、日曜、祝日は除く）

特許ニュース®

令和７年
(2025年) 12月 10日（水）

No. 16523 １部377円（税込み）

発行所

一般社団法人 発明推進協会

東京都港区虎ノ門２－９－１
虎ノ門ヒルズ 江戸見坂テラス

郵便番号 105－0001

[電話]03－3502－5493

発明推進協会ウェブサイト https://www.jiii.or.jp

特許ニュースは

●知的財産中心の法律、判決、行政および技術開発、技術予測等の専門情報紙です。

定期購読料 １カ年75,090円 ６カ月39,165円（税・配送料込み）

目 次

知財の常識・非常識 ㊾

生成AI利用とデータ利活用／営業秘密管理（2025年11月時点）

桜坂法律事務所
弁護士 林 いづみ

1．はじめに―生成AI利用の普及と不確実性

（1）生成AIの利用は、世界中で、企業および個人レベルの社会生活において普及し始めている[1]。最近では単なるチャットにとどまらず、RAG（検索拡張生成）技術を使って社内情報に回答するチャットボットを開発したり、議事録作成や要約、画像生成、さらには人に代わって業務を実行してくれるAIエージェントなどのサービスを導入・活用したりする企業も増えている。大久保敏弘・NIRA総合研究開発機構(2025)「第３回デジタル経済・社会に関する就業者実態調査（速報）」によれば、2025年７月時点の生成AIの利用状況をみると、2023年10月以降、仕事での生成AI利用者は着実に増加してお

り、2024年12月時点と比較すると、特に情報収集・検索での利用が増加している[2]。

（2）AI（人工知能）技術の利活用に向けた制度整備が世界的に進む中、我が国も2025年５月28日に「人工知能関連技術の研究開発及び活用の推進に関する法律」（AI法）が成立（同年９月１日全面施行）し、政府にAI戦略本部が設置されてAI基本計画及び指針の策定に向けた作業が進められている[3]。知的財産戦略本部にも「AI時代の知的財産権検討会」が設置され、「中間とりまとめ」（2024年５月）[4]及び「中間とりまとめ－権利者のための手引き」（2024年11月）[5]が公表されており、前記AI戦略本部と連携して、2025年10月24日（第８回会合）から、論点整理及び検討が継続されている[6]。

（3）AI制度をめぐっては、広島AIプロセスをはじめとする国際枠組みでの共通規範形成努力は進められつつも、具体的制度の在り方についての収斂の見通しは立っておらず、AI利活用をめぐる環境は「かつてない不確実性に特徴づけられて」いる。我が国のAI法は、そのような不確実性の中で斬新的な制度構築を進めるための枠組みの一つとして理解すべきといわれる[7]。

現在（2025年11月）、AI技術開発の中心地である米国では、第二期トランプ政権が、バイデン政権施策を否定し、EUおよびカリフォルニア州に代表される州ごとのAI規制立法に対する影響力行使や、2025年７月「AI行動計画」及び関連する大統領令において中国との覇権競争を含む施策を示している。EUにおいては包括的なAI規制法であるEUAI法の段階的な適用開始、具体的な行動規範や整合規格、ガイドライン等の実務的対応のフェーズに移行しているものの、EU内部の政治的要請とビッグテックへの法適用にかかわる米国（第二期トランプ政権）からの影響力行使への対応が、AI規則の見直しや産業振興を含むAI政策にいかなる影響を与えるか、今後の推移を注視する必要がある。

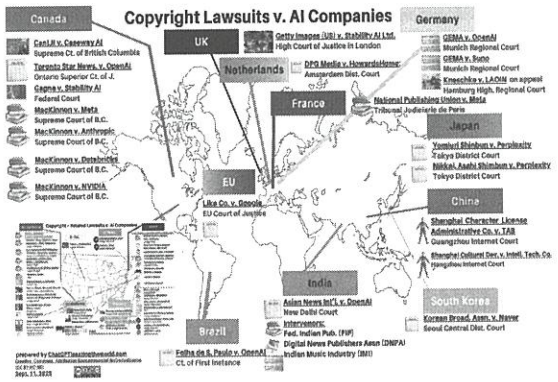
【脱稿後追記：2025年11月19日、欧州委員会は、AI規制の緩和案を発表した。自動車などに使われる「高リスク」のAIに関する規制の導入時期を最大16ヶ月遅らせる。】

（4）本稿においては、AI制度をめぐる共通規範（ハードロー・ソフトローを含め）や具体的制度の在り方が、国際的に不確実な一方で、普及が進む生成AIの利活用に関して、市場構造（AI開発者（AIシステムを開発する事業者）、AI提供者（AIシステムをアプリケーションや製品に組み込んだサービスを提供する事業者）、AI利用者（AIシステム・サービスを利用する事業者））の実態と課題を概観し、生成AIの鍵を握るデータガバナンスの重要性について検討する。なお、誌面の制約のため、生成AI利用に係るサイバーセキュリティについては別稿に譲る。

２．生成AIに関する訴訟提起の状況

生成AI利用の普及に伴い、生成AIの学習データとしての著作物、肖像、声の無断利用に対して、世界中で（日本も含めて）訴訟が多発しているが、現時点では、いまだ司法判断は定まっていない[8]。

【図１：世界における生成AIに関する訴訟マップ】



出典：Updated World Map of Copyright Suits v. AI (Sept. 11 2025) 71 total – Chat GPT Is Eating the World[9]

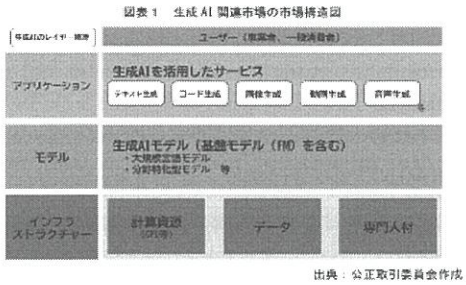
【図２：米国における生成AIに関する訴訟マップ】

出典：Map of Copyright Litigation v. AI companies in United States[10]

３．生成AIの開発をめぐる市場構造と実態調査

（１）公正取引委員会の令和７年６月「生成AIに関する実態調査報告書ver.1.0」によれば、生成AIの開発をめぐっては以下のような市場構造と実態がみられる[11]。

【図３：生成AI関連市場の市場構造】



出典　令和７年公取報告書

A．アプリケーションレイヤーについて

アプリケーションレイヤーにおいては、ビッグテック企業からスタートアップ企業まで、多様な事業者が様々な生成AIプロダクトを提供しており、多彩な需要に対応するため、活発な競争が行われている。日本国内においても、社内・社外向けチャットボット、検索システム、テキスト生成、画像生成、音声生成など、様々な生成AIアプリケーションサービスが商用化され、市場における活用が進んでいる[12]。

B．モデルレイヤーについて

現時点においては、ビッグテック企業等を中心に、生成AIモデルの開発競争が活発に行われている状況にあり、国内事業者は、日本語性能が高い汎用モデルや特定用途へ特化したモデルなどを開発することで、ビッグテック企業の汎用モデルと差別化を図る動きを見せている。一方で、モデルの小型化・軽量化・効率化を目的とした様々な開発手法が注目されており、今後、競争状況が一新される可能性もあり得る。

C．インフラストラクチャーレイヤーについて

①計算資源（GPU等）：GPU市場においては、NVIDIA製GPUがグローバル市場で高いシェア（約80%）を有しており、学習段階の市場では引き続き優位性を持つ可能性が高い。一方、推論段階の市場では、新規参入者の台頭等により、学習段階と比べて競争が活発化しており、多様なプレイヤーによる革新が進む段階にある。

②データ：前回報告書でも、生成AIモデルの開発においては、大量の学習データを使用して事前学習を行う必要があり、さらに、特定のタスク等に合わせて調整するためには、追加の学習データを使用してファインチューニングを行う必要があること、特に海外を中心に、データ保有者と生成AIモデル開発事業者との間でデータの利用を巡って問題が発生していること（例えば、基盤モデル開発事業者に対して、インターネット上に公開されているあらゆる情報を事前学習に使用することに関連して、著作権侵害等を理由に訴訟が提起されている状況となっていること）が指摘されていたが、今回の報告書における指摘では、生成AIの開発や利用において、質の高い独自データの重要性が増していることが注目される[13]。また、データ利用には権利処理、アクセス環境、知的財産権制度への対応が必要であるとして、公表済みの各種ガイドライン等を紹介している[14]。

（２）マルチモーダルAI、蒸留など

近年、生成AIの応用範囲が大幅に拡大した結果、大規模言語モデルから、テキスト、画像、音声、動画等の異なるタイプのデータを統合して処理するマルチモーダルAIへと主流が進化している。マルチモーダルAIの登場により、医療・創薬・教育・エンターテインメントなどAIの活用範囲が広がることや、推論・分析など一般的なタスクにおける処理能力も向上すること等が期待されている。開発の効率化アプローチとして、例えば、低コストで高性能な生成AIモデルを開発したとされるDeepSeek社は、「蒸留」[15]や「MoE」[16]の技術を取り入れ、計算効率の最適化を図っていると公表している[17]。こうした効率化の取組は、GPUなどの計算資源に対する依存度を相対的に下げる可能性があるとされる。

（３）生成AIクラウド市場、関連サービス事業者、

パートナーシップ状況など

ビッグテック企業を中心とする海外のクラウドサービス事業者は、豊富な資金力を背景に計算資源の確保を進め、図表４のとおり、生成AI開発に最適化されたクラウドサービスを提供している[18]。

【図４：大手クラウドサービス提供事業者３社の主な生成AI関連サービスの概要】

図表４　大手クラウドサービス提供事業者３社の主な生成AI関連サービスの概要

クラウド	主な半導体チップ	主な生成AI関連サービス
Amazon Web Services（AWS）	・Trainium ・Inferentia ・NVIDIA H100 等	・Amazon Q ・Amazon Bedrock ・Amazon SageMaker 等
Microsoft Azure	・NVIDIA H100 等	・Azure AI Foundry ・Azure Machine Learning ・Azure OpenAI Service 等
Google Cloud	・TPU v5p/v5e ・NVIDIA H100 等	・Vertex AI ・Cloud AutoML ・Gemini 等

出典：各種公開資料を基に公正取引委員会作成

出典：令和７年公取報告書―図表４　大手クラウドサービス提供事業者３社の主な生成AI関連サービスの概要

また、生成AI関連市場における開発事業者間のパートナーシップに着目すると、半導体チップ提供事業者と生成AIモデル開発事業者間、生成AIモデル開発事業者間同士、生成AIモデル開発事業者と生成AIプロダクト開発事業者間のパートナーシップなど、国内外でレイヤーをまたいだ形でのパートナーシップの形成が活発に行われている。また、既存のデジタルサービスを提供するビッグテック企業と生成AIモデルを開発するスタートアップ企業との間でパートナーシップを締結している例なども複数みられる。

【図５：パートナーシップ一覧】

図表５　パートナーシップ一覧
生成AIサービス関連企業

出資企業 ＼	OpenAI	Anthropic	Hugging Face	sakanaAI
NVIDIA	連携		○ 2023/8	○ 2024/9
Microsoft	○ 2019/7		連携	
Amazon		○ 2023/9	○ 2023/8	
Google		○ 2023/2	○ 2023/8	
Apple	連携			
ソフトバンクグループ	○ 2025/2			

※○は、出資を伴うパートナーシップを示す。
出典：2025年３月末時点の各種公表情報を基に公正取引委員会作成

４．生成AI関連市場における主な海外当局等の動き

（１）各国当局は、生成AIの開発と利用に伴う課題に対して、以下のような様々な対応を続けている。

関係機関／規制・ガイドライン名／発表・改訂年／URL
欧州委員会：2024/European Union AI Act（欧州AI規制法案　最終案） https://artificialintelligenceact.eu/ 欧 州EDPB：https://edpb.europa.eu/news/news/2024/edpb-publishes-guidelines-generative-ai-and-data-protection_en AIと営業秘密・学習データに関するFAQ： https://ec.europa.eu/info/law/law-topic/data-protection_en
中国国家インターネット情報弁公室/2023年７月施行・2025年改訂 生成型人工知能サービス管理暫行規定 http://www.cac.gov.cn/2023-07/10/c_1684138752107111.htm 2025年／生成型AIガバナンス指針 http://www.cac.gov.cn/2025-01/15/c_1700109557123456.htm 中国最高人民法院：AIデータ利用と営業秘密保護に関する司法解釈 http://www.court.gov.cn/fabu-xiangqing-403812.html
米国NIST（2024）：AI Risk Management Framework https://www.nist.gov/itl/ai-risk-management-framework Risk Management Framework https://csrc.nist.gov/projects/risk-manegement/about-rmf 米国政府（2023年11月）： Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/ 米国FTC: https://www.ftc.gov/news-events/data-privacy-artificial-intelligence

（２）前記公取令和７年報告書でも「（別紙）生成AI関連市場における主な海外競争当局等の動き」において整理されているが、以下においては、主に第二期トランプ政権以後の直近の事象[19]に焦点をあてて国際的動向を整理する。

➢2024年７月23日、欧州委員会、CMA（英国競争・市場庁）、DOJ（米国司法省反トラスト局）及びFTC（米国競争当局）の連名で、生成AI基盤モデル及びAI製品の競争における共同宣言が発表された[20]。

➢2024年８月１日、EUのAI法が発効し、段階

的な適用が開始された（11条）。関連ガイドライン[21]も公表されているが執行は１年留保されている。

➢2024年９月19日、欧州委員会は「生成AIと仮想世界における競争に関する政策概要（ポリシーブリーフ）」を発表した[22]。

➢2024年10月３日及び４日、イタリア（ローマ）において、G７の競争当局及び政策立案部局のトップ等が出席する「G７競争サミット」が開催され、成果文書として「デジタル競争共同宣言」が採択された[23]。

➢英国CMA（競争・市場庁）は、競争政策・消費者保護政策の観点から、AI基盤モデルを対象とした調査を実施し、2023年９月18日に生成AI基盤モデルに関する調査報告書を公表し、2024年４月11日に同報告書のアップデート版を公表した[24, 25]。

➢2025年１月17日、米国FTC（連邦取引委員会）は、2024年１月25日、Alphabet、Amazon、Anthropic、Microsoft及びOpenAIの５社に対して発令した、生成AI企業及び大手クラウドサービスプロバイダーが関連する最近の投資や提携に関する情報提供命令（FTC法第６条に基づく）によって入手した情報等を踏まえ、「AIパートナーシップと投資」についてのスタッフレポートを公表し、大規模クラウドサービスプロバイダー（Alphabet、Amazon及びMicrosoft）と生成AI開発事業者（Anthropic及びOpenAI）間のパートナーシップによって、投入物へのアクセス制限や優先的アクセス、スイッチングコストの上昇及び機密情報の入手等の競争政策上の問題が生じる懸念を指摘した[26]。

➢2025年１月、中国のAIスタートアップ企業であるDeepSeekが少ない資金で米国大手AI企業のモデルと遜色のない生成AIを開発したことから、対中国の競争力強化の観点から規制緩和へと大きく方針転換した[27]。

➢2025年１月23日、トランプ大統領は大統領令「AIにおける米国のリーダーシップに係る障害の除去」を発表し、180日以内のAI行動計画の策定や、バイデン政権時代に定められた政府によるAI利用と調達に係るOMB（行政管理予算局）覚書の改訂などを命じた。

➢2025年４月23日、ホワイトハウスは大統領令「米国の若者のためのAI教育の推進」を発表、同月28日には、メラニア大統領夫人が被害女性らを支援した、テイク・イット・ダウン法（ディープフェイクによるものを含む非同意親密画像の故意の公開の違法か、削除の義務付け等）が連邦議会で超党派で可決され、トランプ大統領が５月19日付けで署名した。

➢2025年２月11日、パリで開催されたAIアクションサミットの基調講演において、ヴァンス米国副大統領は、欧州のデジタル・AI関連の規制について、過剰な規制であるとともに、検閲による言論統制であると強く非難した。

➢2025年２月21日、トランプ大統領は、欧州等を念頭に、デジタルサービス課税を課す国に対して関税を課すとの覚書に署名した。また、同年４月後半には、米国の在欧州代表部が、欧州AI法における汎用目的AI（GPAI）規制に係る実戦規範（COP）の採択に反対する旨の書簡を送付した。

➢2025年４月９日、欧州委員会は「AI大陸行動計画」を発表し、AIの分野でEUが世界的リーダーになることを目標としている。なお、2024年９月のDraghi Report[28]において、デジタル規制によりEUのテック産業の発展が阻害されており、ルールをシンプルにすべきとされたことを受け、デジタル分野についても、規制の簡素化に向けた検討が進行中という。

➢2025年７月23日、トランプ政権は、第二期政権の全体的なAI戦略となる「競争に勝つ―米国のAI行動計画」を発表した[29]。特徴的なのは、トランプ政権の価値観の反映（DEIの排除[30]）とAI技術の輸出促進（中国のAIモデルにおける中国共産党の検閲状況の調査など）の点である。また、同計画では、AI規制の強い州への補助金削減方針を記載している（今後、連邦通信委員会（FCC）が、既存法に基づき、州のAI規制を評価する）。

➢2025年８月４日に開催されたAPECデジタルAI大臣会合に参加した米国OSTPのクラチオス局長は、各国に対し米国のAI輸出をPRしつつも、各国

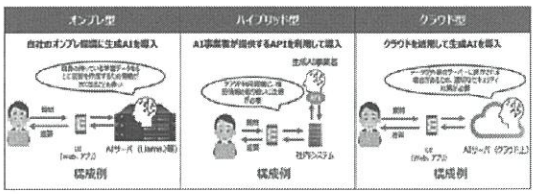
が正当に要求するAI主権、データプライバシー、技術的なカスタマイズを提供するとコメントした。

５．AI時代におけるデータガバナンス：生成AIの学習データに営業秘密や個人情報等が含まれる場合の情報漏洩リスク

（１）生成AIが急速に活用される現代において、ユーザーがAIに入力する情報には企業の営業秘密や従業員・顧客の個人情報など、秘匿性の高いデータが含まれることも多く、これらの情報は、AIモデルが「学習データ」として蓄積・解析する際、モデルの応答に利用されるリスクがある。IPA「テキスト生成AIの導入・運用ガイドライン」（以下、「IPAガイドライン」という。）[31]の巻末（P84, 85）の言葉は示唆に富む。「ビジネスにおいて重要な要素は自社と他社と間で違いを生むこと、つまり差別化です。他社との差別化を可能とするAIを開発するには、学習データの広さよりも深い専門性や秘匿性、つまり他社が活用できない情報が重要となります。そのため、今後ビジネスにおける生成AIの活用については、“業界や会社に特化した生成AI”が鍵を握ると考えます［61］。各企業で業界に特化した生成AIを導入するには、自社が所属する業界の特性を分析し、学習させる自社のデータを分類するなどの準備が必要です。現時点のデータを整理することは、“将来的に業界に特化した生成AIの構築をスムーズに行うことに繋がる”と見込まれます。この事前準備を念入りに行うことが業界に特化したAIを用いて業務効率化を図るための第一歩となるため、今一度、自社が持つデータの利活用について検討をすることをお勧めします。」「法規と安全な利用：各国で行ったAIに対するアンケート結果によると、（中略）「日本はAIに対する深い理解はないが、楽観的に捉えている」という結果が得られたと言えます。この結果からは、AIに対し、先進的な技術であるというイメージが先行し、それに関するリスクが認識されていないことが危惧されます。リスクは例えば、AIが行う「推論」によって作られたハルシネーションや潜在的思考への影響、過失によるもの（情報漏洩など）に加えて、悪意によるもの（ディープフェイクによる個人の尊厳を汚す行為、フェイクニュースを作成し大衆を混乱に陥れる行為など）です。（中略）組織において利用する際には継続的なAIの教育を行い、“もっともらしいAIの出力の正しさ”を確認する習慣を根付かせることが重要です。情報の真偽性を確認する習慣を浸透させ、AIの持つ利便性や有効性を最大化し、業務効率と企業価値の最大化を図っていきましょう。」

（２）IPAガイドラインは、生成AIの構築環境ごとにメリットとリスクを解説している。

【図６：生成AIの構築環境】



出典：IPA「テキスト生成AIの導入・運用ガイドライン」P30　図３－３

クラウド型とは、クラウドサービスを利用して組織に生成AIを導入する方式のことで、現在、各クラウドプロバイダーから生成AIを導入するためのさまざまなサービスが提供されている。オンプレ環境に生成AIを導入する場合と比べて導入難易度が低く、管理の手間も少なく済む一方、入出力データが外部サーバーに保存されるなどのセキュリティリスクがあり、入力データを学習許可させないオプトアウト申請などのセキュリティの検討が必要となる。また、サービスごとに設定できる内容も異なるため、導入前に各サービスの仕様や制約をしっかりと確認することも必要である。なお、LLMが学習していないデータに関する回答の精度が大きく低下する課題（例えば、インターネットに掲載されていない社内ドキュメントのようなデータ、専門性の高いデータ、LLM作成時点では公開されていない最新のデータなどに関する質問に正確に回答することは困難）に対応する技術として、現在「ファインチューニング」と「RAG（Retrieval-Augmented Generation）が採用されている。セキュリティとプライバシーの観点から、RAGに使用するデー

タに機密情報や個人情報が含まれる場合、適切なアクセス制限やデータの定期的な棚卸が重要である。特に、クラウド環境を利用した環境構築において、RAG環境を構築する場合、割り当てられた担当者の権限によっては、利用が制限される機能が存在するため、円滑な生成AIシステムの導入にあたり、担当者への権限付与の設定が重要となる[32]。もとより、RAGをはじめとする生成AIに関する技術は、その進化が著しいため、常にその動向を注視することが重要である。

（３）生成AIサービス導入に当たっては、生成AIサービス提供契約において、①情報流出リスク軽減のための安全設計[33]が採用されているか、②生成AI提供サービスの契約書におけるNDA条項・管理条項[34]を、確認する必要がある。そのうえで、生成AIを安全に運用するためには、①利用ツール（生成AIサービス）ごとの社内での利用規定の設定[35]、②従業員教育の徹底[36]、③継続的な監督と改善[37]を継続的に実践することが必要である。

６．おわりに

生成AI技術の進歩は早く、AI制度の将来像は不確実である。日本社会における生成AI関連サービス提供者がもっぱら外国企業で占められている現状に鑑みると、今後、我が国が精緻な規制・規範を策定したとしても、それを生真面目に守るのはもともと慎重な日本企業だけかもしれないことが懸念される。前記のとおり「AIに対する深い理解はないが、楽観的に捉えている」日本社会においては、よくわからないうちに生成AIの利用が個人及び企業の間で普及し始めているようだ。利用の太宗を占めているChatGPT（OpenAI）、Gemini（Google）、Copilot（Microsoft）、Refus（Amazon）、Apple Intelligence（Apple）、Grok（X）などでは、無料の生成AIの利用規約も有料の生成AIの利用規約も、正文はIT約款特有の表現で書かれた長文の英語であって日本語は参考訳にすぎない[38]。FAQもあるが機械翻訳のような和訳を一般人がどこまで理解できているだろうか。利用者は、利用規約において、無料版や個人プランでは入力データがAIの学習に利用されることがあるのか、法人向けのプランではデフォルトで学習利用がオフになっているのか、個人プランでも設定によってオプトアウトが可能なのか、を本当に理解したうえで使用しているだろうか。

利用者の入力データがAIの学習に利用されることが有るか無いか、簡単に利用されない設定にできるか、利用者が入力したデータが第三者への出力に含まれる可能性が有るか無いか、簡単に出力に含まれないような設定にできるか、わかりやすい日本語で利用者に対して説明表示すること、また相談窓口の整備は、最低限の消費者保護として必要ではないか。まずは、こうした観点での「利用者のための手引き」の整備を、サービス提供者に義務付けることが急務であると考える。

1　https://www.nikkei.com/article/DGXZQOGN20EDF0Q5A220C2000000/　ChatGPTの全世界の利用者数は2025年２月に４億人に到達している（日本経済新聞「OpenAI『ChatGPT』利用者、世界４億人に２カ月で３割増」（2025年２月21日）なお、2024年12月時点での利用者は、３億人であり、利用者数が２億人から３億人に達するまでに３か月を要したのに対し、３億人から４億人への増加は２か月余りと、利用者数の増加スピードが加速している。

2　総務省「令和６年版情報通信白書」（2024年７月）の「生成AIの活用方針策定状況」https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r06/html/nd151120.html#f00061においては、日本で「生成AIについて活用する方針を定めている」と回答した割合は42.7％であり、約８割以上で活用する方針を定めていると回答した米国、ドイツ、中国と比較するとその割合は約半数であった。

3　AI基本計画の骨子（たたき台）の概要についてsanko4-1.pdf；AI法に基づく適正性確保に関する指針の整備についてsanko5.pdf（同資料P３　この時点までに関係省庁が公表している各種ガイドライン（合計15）の一覧表）

4　0528_ai.pdf

5　2411_tebiki.pdf「AI技術の進歩の促進と知的財産権の適切な保護が両立するエコシステム」の実現に向け、権利者（クリエイター等）に期待される取組事項例を紹介。生成AIと知財をめぐる懸念・リスクへの対応等については、法・技術・契約の３つの手段を適切に組み合わせて対応することが必要であるとして、「知っておきたい法・技術・契約の概要」を要約している。

6　2025年10月24日開催の同検討会の資料３　shiryo3.pdf

では以下の３つの論点が掲げられている。①データの収集や、生成AIに係る開示・表示、保護データに係る対価還元、保護データに係る侵害防止技術、海賊版・偽情報・誤情報のスクリーニングに係る技術など、データの信頼性・安全性を含め生成AIに係る開示に向けた各種の対応が必要と考えられるところ、どのような方向で検討を進めるべきか。②法・技術・契約の各手段を適切に組み合わせながら、連携した取組が重要であるところ、データ利活用に伴う対価還元を進めていくため、どのような課題を特定しつつ、取組を進めていくべきか。③直近の生成AIと知的財産をめぐる技術動向や、国内外の裁判例等も踏まえつつ、AIとデータの取扱いについて、どのような将来像を想定しておくべきか。また、参考資料10「AIと著作権に関する関係者ネットワークの総括―令和７年５月30日　文化庁・経済産業省」sanko10.pdfにおいては「６．ネットワークを通じて明らかになった課題」として、学習用データセットに関する契約についての留意事項等の整理、権利者への適切な対価還元に向けた学習用データセット構築の在り方、クリエータが安心活実用的に活用できる生成AIの在り方（サービスに関する説明の在り方、学習用データセットの在り方、機能等）がまとめられている。

7 ジュリストNo.1616　池貝直人「特集　AI利活用の方向性―特集にあたって」

8 例として、①　Stable Diffusion AI事件（2024年欧州司法裁判所）画像生成AIの学習過程で著作権・秘密データの利用可否が争われた。欧州裁判所は「営業秘密の社会的価値とAI開発のバランス」を明示し、一部に違法利用を認定した。https://artificialintelligenceact.eu/

②　OpenAI訴訟（2024年連邦地裁）著作権者が訓練データに自身の著作物が不正使用されたとして提訴。AIモデルのフェアユースの判断基準、営業秘密と“学習の限界”が争点となり、裁判所は「著作権者に追加的救済の余地あり」としつつ、AIのフェアユース性判断を示した。

https://www.thomsonreuters.co.jp/ja/products/westlaw-japan/case-law.html

③　Salesforce v. Google AI（カリフォルニア州、2025年４月判決）営業秘密を含む企業データがGoogleの生成AIの学習に用いられたことについて、判決は「企業秘密の一部漏洩を認定」し、損害賠償の一部を認めた。

④　杭州AI技術事件（2025年最高人民法院判決）企業間で営業秘密がAI学習データとして不正提供された事例。判決は「営業秘密性とAIモデルの社会的利益」を比較考量し、制限的救済を容認。http://www.court.gov.cn/fabu-xiangqing-403812.html

9 https://chatgptiseatingtheworld.com/2025/09/11/updated-world-map-of-copyright-suits-v-ai-sept-11-2025-72-total/

10 htts://chatgptiseatingtheworld.com/wp- content/uploads/2025/06/Map-od-Copyright-Litigation-v.-AI-companies-in-United-States-June-12-2025.pdf

11 公正取引委員会「ディスカッションペーパー『生成AIを巡る競争』」（2024年10月）に続くものである。https://www.jftc.go.jp/houdou/pressrelease/2024/oct/241002_generativeai.html

12 例えば、OpenAIによると、ChatGPTの日本における利用者数は2024年に、前年比２倍の600万人に達したとされている。

13 生成AIモデル開発や利用においては、RLHFやRAGなどの技術により、応答精度や外部知識活用が向上すること/事前学習には大量の言語データが求められ、ファインチューニングでは目的別の応答精度向上データが必要であり、特化型モデル構築には業界固有の高品質データが不可欠であること。/データはウェブ公開、オープンデータ、事業者保有、行政機関保有など多様であるが大規模モデル開発には膨大なデータ量が要求されるが、質の高いオープンデータの不足が懸念されていること。/生成データの活用やデータ品質向上の取り組みが進行中であり独自データの重要性が増し、ビッグテック企業が競争優位となる事例が見られること。

14 文化庁「AIと著作権に関する考え方について」（2024年３月）
（https://www.bunka.go.jp/seisaku/bunkashingikai/chosakuken/pdf/94037901_01.pdf）

・同「AIと著作権に関するチェックリスト＆ガイダンス」（2024年７月）
（https://www.bunka.go.jp/seisaku/bunkashingikai/chosakuken/seisaku/r06_02/pdf/94089701_05.pdf）

・内閣府知的財産戦略推進事務局「AI時代の知的財産権検討会『中間とりまとめ』－権利者のための手

引き－」（2024年５月）（https://www.kantei.go.jp/jp/singi/titeki2/chitekizaisan2024/0528_ai.pdf）
・経済産業省「コンテンツ制作のための生成AI利活用ガイドブック」（2024年７月）（https://www.meti.go.jp/policy/mono_info_service/contents/aiguidebook.html）
・総務省・経産省「AI事業者ガイドライン〔第1.1版〕（2025年３月28日）https://www.meti.go.jp/shingikai/,pmp_omfp_service/ai_shakai_jisso/20240419_report.html
・個人情報保護委員会「生成AIサービスの利用に関する注意喚起等」（2023年６月２日）https://www.ppc.go.jp/news/careful_information/230602_AI_utilize_alert/

15 蒸留（知識蒸留）とは、一般的には、事前学習済み生成AIモデル（教師モデル）が学習した豊富な知識を、小型で効率的な別の生成AIモデル（生徒モデル）に転送する手法である。通常、教師モデルは膨大なパラメータと計算資源を必要とする一方、蒸留された生徒モデルは、教師モデルと同等あるいは近い性能を、低コストかつ高速な推論環境で実現できる点が大きなメリットであるといわれている。

16 Mixture of Experts（MoE）とは、１つの巨大モデルを、複数の「専門家（Expert）と称するサブネットワークに分割し、各入力に対して最も適切な専門家を選択して出力を生成する手法である。生成AIモデルの学習・推論に伴う計算コストを削減し、大規模化、省電力化、高速化を実現する。この仕組みにより、各専門家は入力の特定の領域や特徴に特化し、全体として高い表現力を保ちつつ計算量は抑えられるといわれている。

17 https://github.com/deepseek-ai/DeepSeek- R1/blob/main/DeepSeek_R1.pdf

18 GPUクラウドの日本市場シェア（2023年実績）は、アマゾンウェブサービスジャパン 55.0％、日本マイクロソフト 18.7％、グーグル・クラウド・ジャパン 13.4％、さくらインターネット 1.0％、その他 12.0％と推定されている（富士キメラ総研「2025生成AI/LLMで飛躍するAI市場調査」（2024年11月）188頁）。

19 出典：前掲ジュリストNo.1616「特集　AI利活用の方向性」から市川類「第二期トランプ政権における米国のAI政策の動向」及び石川智也「EUのAI法の実務対応と今後の展望」

20 https://competition-policy.ec.europa.eu/about/news/joint-statement-competition-generative-ai-foundationmodels-and-ai-products-2024-07-23_en

21 European Commission, Annex to the Communication to Commission “Approval of the Content on the Draft Communication from the Commission-Guidelines on the Scope of the Obligations for General-purpose AI Models Established by Regulation (EU) 2024/1689 (AI Act)”, C (2025) 5045 final (Jul.18, 2025

22 https://digital-strategy.ec.europa.eu/en/news/commission-publishes-policy-brief-competition-generativeai-and-virtual-worlds）同政策概要では、主要なリソースへのアクセス制限、市場支配力を活かした排除行為、ネットワーク効果等の競争上の懸念を指摘している。

23 https://www.jftc.go.jp/houdou/pressrelease/2024/oct/241007_G7_result.html　同サミットにおいては、AIバリューチェーンにおける競争上の懸念（AIの鍵となる投入物及びパートナーシップ）、AIに関する競争上等の懸念（AIの下流及び隣接市場並びにアルゴリズムを利用した共謀等）、AI市場に対する規制・政策アプローチ等の議題について議論が行われ、当該共同宣言では、AIによるイノベーションの創出、AIに関する競争上の懸念、競争とイノベーション促進のための主導原則、競争当局等の役割（厳正な法執行、国際協力の強化等）などについての考え方を示している。

24 https://www.gov.uk/government/publications/ai-foundation-models-update-paper　同報告書では、競争の公平性、効率性及び開放性の観点から懸念がみられる旨が示されている。

25 CMAは、複数のビッグテック企業と生成AIスタートアップ企業とのパートナーシップ等について企業結合審査を行っていたところ、全てのパートナーシップ等で第２次審査へ移行しない旨決定した。MicrosoftとMistral AI（2024年５月17日に審査終了）、MicrosoftとInflection AI（同年９月４日に審査終了）、AmazonとAnthropic（同年９月27日に審査終了）、GoogleとAnthropic（同年11月19日に審査終了）、MicrosoftとOpenAI（2025年３月５日に審査終了）

26 https://www.ftc.gov/news-events/news/press-releases/2025/01/ftc-issues-staff-report-ai-partnershipsinvestments-study　同情報提供命令は、生成AI開発企業とクラウドサービスプロバイダーとの

間に形成された投資や提携が、競争環境にいかなる影響を与えるかについて理解を深めるため、数十億USドル規模の投資が行われている３つのパートナーシップに関わる企業（Microsoft-OpenAI、Amazon-Anthropic及びGoogle-Anthropic）に対して行われた。なお、同レポートについて、アンドリュー・N・ファーガソン委員長（同報告書公表時は委員）とメリッサ・ホリョーク委員は、同レポートの公表自体には賛意を示しつつも、第５章（AIパートナーシップの潜在的な影響について注目すべき分野）については、読み飛ばすか、懐疑的な目で読むべき等の意見を表明している（前掲ジュリスト・市川類P23～26参照）。

27 前掲ジュリスト・市川類P23～26によれば、2024年12月、第二期トランプ政権は、ホワイトハウスの科学技術政策の司令塔である科学技術政策局（OSTP）の局長に、マイケル・クラチオス氏（文系学士卒の30代後半の人物）を異例の抜擢をし、また、シリコンバレーの実務家を、AI・暗号特別顧問、かつ科学技術政策の中核的アドバイザーとして指名した。また、トランプ大統領は就任日翌日にホワイトハウスで、ソフトバンク、OpenAI等による米国内に5000億ドルを投資するとするスターゲートプロジェクトを発表した。

もともと、米国では、連邦政府におけるAI規制が進まない中で各州政府において数多くのAI関連規制法が成立していた。例えば、コロラド州の包括的AI規制法、テネシー州のELVIS法（AI生成による声の模倣や肖像の不正司法を防ぐ目的。「声の肖像権」を明記）、カリフォルニア州の肖像権、透明性確保義務、コンテンツ規制を含む18の関連法案、ニューヨーク州は2025年２月に州政府におけるAI利用に関し、自動化された意思決定ツールの使用についての一部禁止や評価・透明性確保を義務付けた法案が成立している。これに対して、DeepSeekショックの後、国内サービス展開にあたり、全ての州法に対応せざるを得なくなることに大手AI企業は危機感を深め、「大きく美しい１つの法案」に州政府によるAI規制を10年間禁止する条項（州AI規制モラトリアム条項）を盛り込んで５月22日下院で可決したが、７月１日上院で同条項が削除された、といった攻防の経緯がある。

28 The Draghi report on EU competitiveness

29 The White House, “Winning the Race: America's AI Action Plan”, Jul. 23, 2025

30 大統領令「連邦政府におけるWoke　AIの防止」The White House, “Preventing Woke AI in the Federal Government”, Jul, 2025 「Woke（ウォーク）」とは、社会正義に目覚めた状態を指す英語のスラングであるが、近年では「過度な意識の高さ」や「急進的な価値観の押し付け」を揶揄する否定的な文脈で使われている。

31 https://www.ipa.go.jp/jinzai/ics/core_human_resource/final_project/2024/f55m8k0000003spo-att/f55m8k0000003svn.pdf

32 クラウド型には利用するクラウドの形式によって、さらにPaaS型（例：Amazon Bedrock（AWS）、Azure OpenAI（Azure）、Vertex AI（GCP））SaaS型の２種類が存在する。

SaaS型（例：ChatGPT Enterprise（Open AI）、Claude 3 Opus（Anthropic）、Copilot for Microsoft 365（Microsoft）、Gemini Advanced（Google））は、各社が構築した生成AIのサービスをネットワーク経由で利用する方式のことであり、生成AIのサービスをインターネット経由で即座に利用開始でき、サービスの管理やセキュリティ対策も提供者側が行うため、ユーザー側の管理負荷を抑えながら、常に最新の機能を利用できる。一方、SaaS型のサービスは標準化された機能セットを提供するため、一般的には自社のニーズに合わせたカスタマイズが難しいとされている。また、利用するサービスやその設定内容によっては入出力データがサービス提供者側の生成AIに学習される可能性があり、SaaS型を利用する際は特に利用規約やセキュリティについて留意することが重要である。

PaaS型は、モデルの開発や既存モデルの利用・デプロイを簡素化するためのプラットフォームを提供するサービス。海外リージョンを利用する場合、データベースが海外に設置されていることから、データの格納が安全保障貿易管理（輸出管理）の対象となる可能性があるため注意が必要である。利用するサービスや設定によっては自社のデータが外部に漏洩するリスクも存在するため、利用する際には適切なセキュリティ設定が求められる。

ハイブリッド型とは、AI提供者が提供しているAPIを利用して、組織に生成AIシステムを導入する方法。自社のシステムからAPIを経由して生成AI機能を呼び出して利用することで、自社システムとの連携が容易となる点が特徴。クラウド型と同様、入出力データが外部サーバーに保存される場合があるなどのセキュリティリスクもあり、利用する際には適切なセキュリティ

設定が必要。利用するモデルやAPIごとにサービスの仕様や制限をしっかりと確認することが重要。

[33] 例：情報流出リスクを軽減するために、アクセス制御、暗号化（送信データ・保存データ双方をTLS/SSLやAES等の方式で暗号化。API連携で機密データをやり取りする際にも、データ漏洩の危険性を低減）、監査ログの記録、API連携の分離管理（社外・社内システムとの連携部分に追加認証やIP制限を設け、機密データの漏洩経路を遮断）等の安全設計が採用されているかどうか。

[34] 条項例:「第●条（秘密保持）1．契約当事者は、本サービスの利用に際し知り得た営業秘密、個人情報等の機密情報について、契約期間中および終了後も第三者に漏洩してはならない。2．サービス提供者は、学習データの保管・処理について適切なアクセス制御・暗号化措置を実施するものとし、本契約にてユーザー情報の再利用を禁止する。3．サービス利用者は、本サービス利用時に機密情報をプロンプト入力してはならない。事前に社内管理基準および公開・非公開ルールを遵守するものとする。」

[35] ユーザーに生成AIを安全かつ効率的に利用してもらうため、利用する上での禁止事項や入出力内容の取扱いに関する注意点、目的の出力を生成するために考慮すべき点などを盛り込む。IPAガイドラインやクラウドサービスの利用規約では「機密情報や個人情報をプロンプトに入力しない」ことが原則とされており、AIを利用する企業・団体も社内規定としてこれを厳格に運用する必要がある。例：利用可能／禁止データ項目を明示した管理基準表の策定/営業秘密（新製品の技術詳細、設計情報、業務ノウハウ）、個人情報（氏名、生年月日、メールアドレス、社員番号等）は、AIのプロンプトに入力しない/経営戦略資料や顧客リストは一律公開禁止、社外向けプレスリリースは一部入力許可/利用ツールごとに公開・非公開ルールを文書化し周知徹底/利用申請・承認フローの組織内整備/不特定多数が利用できるサービスにおいては、情報特定可能なデータや連絡先・契約書面類の記載禁止/など。

[36] 例：生成AIサービスの入力禁止事項（営業秘密、個人情報等）を明示した教育プログラム・eラーニングの実施、実際の事例や過去の漏洩事件を用いたリスク啓発、研修後の理解度テストや定期的な再学習

[37] 例：利用ログの定期監査（アクセス記録のモニタリング）、AI利用担当者との定期レビュー会議を開催し運用ルールの見直しを図る、社外の法規制・事故事例を随時収集し、社内ガイドラインへ反映（「ChatGPTで個人情報流出事故」等のニュース共有など）、参考URL掲載の教育資料等を用いて、従業員教育をする等

[38] GPT-Enterprise 利用規約（英語）https://openai.com/enterprise-privacy 「OpenAIのモデル学習用データの入手先はどこですか？：OpenAIは、公的情報源、第三者から許諾を受けて取得したデータ、人間による評価から作成された情報など、様々な所から入手してたデータを用いています。また、個人利用のChatGPTとDALL・Eの各バージョンからのデータも使います。デフォルトでは、ChatGPT Business、ChatGPT Enterprise、ChatGPT EduおよびAPIプラットフォーム（2023年３月１日以降）のビジネスデータは、OpenAIのサービス向上のためにユーザーが自身のデータ開示について明示的にオプトインした場合を除き、当社モデルの学習に使用されません」

Microsoft Azure OpenAI 利用規約 https://learn.microsoft.com/en-us/legal/cognitive-services/openai/data-privacy

－つづく－

※㊽は10月10日付掲載

※次回は2026年２月掲載予定