Miura&Partners

Data and Digital Insights Vol.6

生成 AI の活用と法整備の現在

2025 年 12 月 12 日

弁護士 南みな子
弁護士 中山貴博

目次

1. はじめに

生成 AI の性能は飛躍的に向上しており、ビジネスにおいて多かれ少なかれ生成 AI を利用する企業が日々増加していることには多言を要しません。特に、2022 年 11 月 30 日に OpenAI による ChatGPT が出現して以降、生成 AI の社内導入というトピックが様々な場面で論じられています。

このような中、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（以下「AI 新法」といいます）が 2025 年 5 月 28 日に成立し、同年 9 月 1 日に全面施行されると同時に、人工知能戦略本部が内閣に設置されました。本稿では、AI 新法の概要を解説すると共に、生成 AI を活用する場面における個人情報の保護に関する法律（以下「個人情報保護法」又は「法」といいます）による現行の規制及び改正に向けた議論状況を解説します。

2. AI 新法の概要

AI 新法 19 条に基づき設置された人工知能戦略本部は、日本が「世界で最も AI を開発・活用しやすい国」になることを基本構想とします。以下では、AI 新法の目的・基本理念及び事業活動に AI を活用する場合に適用され得る規定を解説します。

(1) 目的（1 条）及び基本理念（3 条）

AI 新法は、国民生活の向上及び国民経済の健全な発展を目的とし（1 条）、国際競争力の向上（3 条 2 項）、基礎研究から活用に至るまでの計画的な推進（同 3 項）、適正な研究開発・活用のための透明性の確保その他必要な施策の実装（同 4 項）、国際協力における主導的な役割（同 5 項）を基本理念とします[1]。

(2) 活用事業者の責務（7 条）

AI 新法は、国・地方公共団体に対して、基本理念に則った総合的かつ計画的な施策の策定とその実施を求め（4 条及び 5 条）、研究開発機関に対して、研究開発及びその成果の普及や人材育成、国・地方公共団体の施策への協力を求めます（6 条 1 項）。

その上で、民間事業者[2]に対する責務を 7 条が規定するところ、積極的な人工知能関連技術の活用により事業活動の効率化及び高度化並びに新産業の創出に努めると共に、国及び地方公共団体が実施する施策に協力しなければならないとされています（傍点は筆者によります。以下同じ）。

事業活動の効率化・高度化、新産業の創出は努力規定である反面、国及び地方公共団体には「協力しなければならない」とされており、それゆえ、国及び地方公共団体が講じる施策に協力することが民間事業者の義務となります[3]。

(3) 指導、助言、情報提供等（16 条）

国は、以下の点に関する調査研究を実施し、その結果に基づいて、研究開発機関、活用事業者その他の者に対する指導、助言、情報の提供等の必要な措置を講ずることが規定されています。

- 国内外の人工知能関連技術の研究開発及び活用の動向に関する情報の収集
- 不正な目的又は不適切な方法による人工知能関連技術の研究開発又は活用に伴って国民の権利利益の侵害が生じた事案の分析及びそれに基づく対策の検討
- その他の人工知能関連技術の研究開発及び活用の推進に資する調査及び研究

調査結果については公表することも想定されており、公表に際しては事業者名も含まれ得るとされています。このような公表については、その公表が及ぼし得る効果・影響（人工知能関連技術の研究開発・活用の推進や国民の権利利益侵害の発生・拡大への影響、企業秘密等を不当

[1] 内閣府「AI 法 全面施行 －次なるフェーズへ－」（2025 年 10 月 3 日）

[2] AI 新法 7 条の名宛人は「活用事業者」であるところ、活用事業者は、AI に関連する技術を開発又は提供しようとするものに加え、事業活動において活用しようとする者を含むため、AI 関連技術を利用する民間事業者であれば 7 条が適用されることになります。

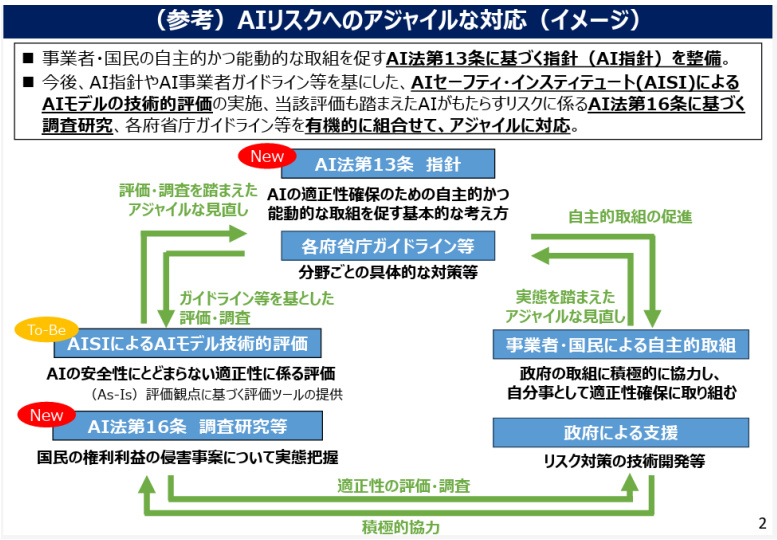
[3] 立案担当者によると、「人工知能関連技術を社会に実装し、国民生活の向上と国民経済の発展につなげていくためには、研究開発と実社会との間をつなぐ活用事業者の役割が非常に重要であることを踏まえ、他の関係各主体の責務に比して重い責務を明示的に求めることとした」とされています（内閣府 科学技術・イノベーション推進事務局 AI 制度審議会「人工知能関連技術の研究開発及び活用の推進に関する法律（令和 7 年法律第 53 号）の概要」NBL1294 号 , 8 頁（2025））。

に害する可能性、模倣犯や愉快犯の増長の可能性等）を総合的に勘案して決定されることとなります[4]。

活用事業者の義務（7 条）に反した場合等に指導・助言の対象になり得ることに加え、上記のような公表の対象となり得ることも踏まえ、自らの事業活動に AI を活用しようとする事業者は、適切な AI 活用を徹底することは当然のこと、今後公表されるであろう指針やガイドラインの内容を踏まえたアップデートを心掛けることが重要です。

(4) 指針の整備等（13 条）

国は、国際的な規範の趣旨に即した指針の整備等の施策を講じるところ（13 条）、指針及び各府省庁のガイドライン等との位置付けについては以下のように説明されています。



引用：内閣府「人工知能戦略専門調査会（第 2 回）資料 2-1『AI 法に基づく指針骨子（たたき台）概要』」（2025）

かかる規定を踏まえ、人工知能戦略本部は「人工知能関連技術の研究開発及び活用の適正性確保に関する指針（案）」を公表し、2025 年 12 月 5 日から同 11 日までの間にパブリックコメントを募集しました。同指針は、適法性確保のための基本方針として①リスクベースアプローチ、②ステークホルダーの関与、③AI ガバナンスの一気通貫での構築、④アジャイル対応の 4 点を挙げた上で、活用事業者が特に取り組むべき事項を以下の通り定めます。

- AI ガバナンスによる俯瞰的な適正性の確保
- ステークホルダーとの信頼関係の構築に向けた透明性の確保
- 十分な安全性の確保
- 事業継続性確保による安全な環境の維持
- AI のイノベーションの基礎となるデータの重要性を踏まえたステークホルダーへの配慮

このような指針を基に今後、ガイドラインや各種取組の検討が進むことが予想されることもあり、今後の動向を注視することが望ましいと考えます。

[4] 前掲注 3・NBL1294 号 10 頁, 脚注 14

3. 個人情報保護法の改正について

個人情報保護法においては、施行後 3 年ごとに法の施行状況について検討を加え必要に応じて所要の措置を講ずること（いわゆる「3 年ごと見直し」）が定められ、法を所管する個人情報保護委員会（以下「委員会」といいます）は、2023 年 11 月以降、現在に至るまで法の見直しに向けた検討を続けています。

以下では、AI の研究開発・活用の場面に焦点を当て、現行の法制度を紹介すると共に、「3 年ごと見直し」における議論状況及び改正が実現した場合の影響について解説します。

(1) 現行の個人情報保護法

個人情報保護法は、個人情報の目的外利用（法 18 条 1 項）や要配慮個人情報の取得（法 20 条 2 項）、個人データの第三者提供（法 27 条 1 項）について本人同意の取得を原則とします。これらの規制が、AI の研究開発・活用の場面でどこまで適用されるのかに関しては様々な議論があり、実務においても混乱が見られるところですので、現行法下における議論状況の概要を解説します。

ア　利用目的規制

（ア）AI を開発する場面における規制

AI の学習済みモデルを構成する学習済みパラメータ（重み係数）は、個人情報を含む学習用データセットを用いて生成したものであっても、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においては個人情報に該当しないというのが委員会の見解です[5]。また、ここで言及されている「特定の個人との対応関係が排斥されている」という点を満たす統計情報も同様に個人情報でないとされており[6]、ゆえに、個人情報を統計データに加工すること自体を利用目的として特定する必要はないとされています[7]。

これらの点を踏まえると、特定の個人との対応関係が排斥された学習済みパラメータを開発するために個人情報を利用する場合は利用目的規制の対象外となります。

もっとも、同見解に対しては以下の指摘がなされています[8]。

① 学習済みパラメータ作成と統計データへの加工とでは、最終的にその結果が個々人に適用されるか否かに関して相違があり得る

② 機械学習モデルの学習用データセットとして用いることは仮名加工情報制度の代表的な利用例として想定されていたことからすると、すでに保有している個人情報を

[5] 委員会「「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」（2025 年 7 月 1 日更新）1-8

[6] 前掲脚注 5・1-17

[7] 前掲脚注 5・2-5

[8] 中井杏「実務問答個人情報保護法（第 3 回）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 52 頁（2023 年）〔曽我部教授からのコメント〕

学習用データとして利用するという行為は統計データへの加工とは異なると理解されていた可能性がある

③ 学習済みパラメータ作成のための利用につき目的の特定が不要だとした場合、個人情報の「取扱い」に該当しないということになるのか

これらの指摘にも説得力があり、実務対応として参考になると考えます。

我々としては、特定の個人との対応関係が排斥された学習済みパラメータを開発するために個人情報を利用する場合には利用目的規制が及ばないと考えていることは上述の通りですが、当該パラメータに基づき実施されるプロファイリングの内容や利用される個人情報の内容によっては、さらに慎重に検討すべき場面が有り得るかもしれません。

例えば、「差別的取扱いを補助するための AI システムを開発するために、機械学習用データセットとして個人情報である仮名加工情報を利用する場合」は不適正利用（法19条）の問題に該当するとされています [9]。仮名加工情報として活用することが許されない利用方法が、統計情報や学習済みパラメータであれば利用が許容されるというのは些かアンバランスな結論であるという感覚は誰しもが有すると思われ、同様の利用目的による統計情報や学習済みパラメータとしての活用については慎重な検討を要するといえます。

また、個人情報保護法の規制が及ばないとしても、AI 開発のために利用される個人情報の内容が本人にとって不意打ちになる場合はあり得ます（例えば、健康情報や医療情報を用いた開発などの場合、このような自らの情報が AI 開発に利用されることは本人にとって想定外となるかもしれません。）。

このように、個人情報保護法の規制が及ばないから何をしても良いというものではなく、仮名加工情報に関する議論や本人の予測可能性といった観点からの検証を経た上で適切な利活用を進めるべきことには多言を要しません。

（イ）AI を利用する場面における規制

個人情報を含むプロンプトを AI に入力することが利用目的規制に抵触するリスクがあります。

個人情報取扱事業者は、個人情報の利用目的を「できる限り特定しなければならない」とされているところ、いわゆる「プロファイリング」といった、本人に関する行動・関心等の情報を分析する処理を行う場合には、分析結果をどのような目的で利用するかのみならず、どのような取扱いが行われているかを本人が予測・想定できる程度に利用目的を特定しなければならないとされます [10]。従前は、個人情報を利用することで生じる「結果」を特定すれば良いと考えられていたところ、このような要請により、本人の予

[9] 委員会事務局「仮名加工情報・匿名加工情報　信頼ある個人情報の利活用に向けて－制度編－」（2022 年 5 月更新）36 頁～38 頁

[10] 前掲脚注 5・2-1

測可能性を確保し難い場面においては個人情報を利用する「手段」の特定も必要とされました。

そのため、AI の活用に際して個人情報を利用し、かかる利用においてプロファイリング等本人が予測することが困難な態様を伴う場合は、どのような態様を取るのかを含めて利用目的を特定する必要があります（委員会によると「ウェブサイトの閲覧履歴や購買履歴等の情報を分析して、本人の趣味・嗜好に応じた広告を配信する」といった特定が必要となります[11]。）。

このような特定・通知等を経ることなく個人情報を AI に入力すると利用目的規制に反する可能性があるため、取得時において特定等していた利用目的を検証すると共に、必要に応じて利用目的をアップデートすることが重要となります。

イ　要配慮個人情報の取得規制

（ア）AI を開発する場面における規制

要配慮個人情報の取得規制への対応が AI の開発段階において必要となり得る場面として、AI モデルの開発・学習に用いるために情報をクローリングにより収集する際、収集した情報に要配慮個人情報が含まれているようなケースがあります。

要配慮情報を取得する際には、原則として、あらかじめ本人の同意を得る必要がありますが、クローリングに際して本人同意を取得することは容易ではありません。そこで、本人の同意なしに要配慮個人情報を取得することができる例外として、以下の規定に依拠することを検討することがあります。

- 当該要配慮個人情報が、本人、国の機関、地方公共団体やこれらに相当する外国の機関等によって、公開されている場合（法 20 条 2 項 7 号）[12]

もっとも、インターネット上に存在する要配慮個人情報の全てが本人によって公開されているとは限りません（例えば、家族や友人が公開するような場面も有り得ます。）。また、国の機関等によって公開されている情報のみをクローリングの対象とすることは有り得るものの、十分な AI 学習という観点から難があることも事実です。

そのため、要配慮個人情報の取得規制は AI 開発にとって大きなハードルとなり得るところ、2023 年 6 月 2 日に出された委員会の注意喚起によって、要配慮個人情報を取得してしまった場合の対応策が示されることで一定の対応方針が示されました[13]。もっとも、かかる注意喚起によって対応方針が全てが明確になったというわけではなく、現在、法改正による対応が検討されています（（2）参照）。

---

[11] 前掲脚注 5・2-1

[12] なお、一度、これらの者により公開された情報であれば、原則としてその先の規制は受けないと解されます。（委員会「『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）（案）』に関する意見募集結果（2016 年 11 月 30 日」No453）

[13] 委員会「OpenAI に対する注意喚起の概要」（2023 年 6 月 2 日）1（1）③

（イ）AI を利用する場面における規制

AI の利用段階においては、AI からの出力結果に要配慮個人情報が含まれることで、AI を利用した者が要配慮個人情報を「取得」することとなり本人同意規制（法 20 条 2 項）が適用されることがあり得ます。

この点については、生成AIが出力する結果は事実ではなく確率論に基づく推論であり、したがって、要配慮個人情報を推知させる情報にすぎないとして要配慮個人情報ではないとする整理が有り得ます。

また、出力結果が要配慮個人情報に該当するとしても、当該情報を取得しないように対応することも有り得ます。委員会は、インターネット上に公開されている個人情報を、単に画面上で閲覧する場合には個人情報の「取得」には当たらず、これを超えて、当該個人情報を転記の上、検索可能な状態にしている場合、当該個人情報が含まれるファイルをダウンロードしてデータベース化する場合には、個人情報を「取得」したと解し得るとの見解を示しています[14]。同見解から考えると、AI からの出力結果に要配慮個人情報が含まれていたとしても、これを閲覧したのみでは「取得」することには当たらず、これを超えて、要配慮個人情報を転記の上、検索可能な状態にした場合や、当該個人情報が含まれるファイルをダウンロードしてデータベース化する場合には、要配慮個人情報を「取得」したと解され、本人同意規制が適用されると整理することが可能であると考えます。

AI からの出力結果が「事実」なのか「推論」なのか、事実である要配慮個人情報が出力結果に含まれた場合にどのように対応すべきか、といった点は極めて悩ましいトピックです。当該出力結果を「取得」しないようにするという対応は多くの場面で模索されていますが、要配慮個人情報該当性の判断が悩ましいことは AI の文脈に限らずよく起こることであり、どのような情報を「取得」しないようにすることで足りるのかは必ずしも明確ではありません。これらの点は、社内ガイドライン等の整備を通じて模索が続けられているところではありますが、委員会による見解の表明等、さらなる議論が望まれます。

ウ　第三者提供規制

（ア）AI を開発する場面における規制

開発段階において検討すべき第三者提供規制は大きく 2 つの場面があり、①学習済みパラメータの作成を第三者に委託するに伴い、個人データを含む学習用データを当該第三者（委託先）に提供する場合、②学習済みパラメータを第三者に提供する場合を挙げることができます。

[14] 委員会「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）」（2025 年 6 月一部改正）42 頁。前掲脚注 5・4-4

①については、委託先が委託された業務（すなわち、学習済みパラメータの作成）の範囲内でのみ個人データを取り扱う限りにおいては、法 27 条 5 項 1 号により本人同意は不要となります。

また、②についても、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学習済みパラメータは個人情報に該当しないという委員会の上記見解を基にすると、学習済みパラメータは個人データに該当しないため第三者提供規制は及ばないこととなります。

（イ）AI を利用する場面における規制

個人データを含むプロンプトを AI に入力する場面においても、第三者提供規制への抵触が問題となります。この点についても様々な議論がありますが、①個人データが「提供」されているか、②提供されているとした場合における提供先は「第三者」かという点から整理します。

委員会は、個人データをクラウドに保存する行為について、クラウドサービスを提供する事業者が個人データを取り扱わないことになっている場合には個人データの「提供」には該当しないとの見解（いわゆるクラウド例外）を示します[15]。このようなクラウド例外との関係で、委員会による生成 AI サービスの利用に関する注意喚起等（1）②における以下の記載を基に、生成 AI のプロンプトに個人データを入力することが「提供」に該当しないのではないかという議論が生じました。

> 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。

「提供」に該当しないとする考え方は、「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」か否かが「提供」の分水嶺であるとした上で、「個人データを機械学習に利用」するなどの「出力以外の目的」での利用がなされる場合は「提供」に該当するものの、「応答結果の出力」を目的とする取扱いのみがなされるのであれば「提供」に該当しないことを注意喚起が示したものであるとします。

このような考え方も十分に有り得るところですが、委員会による注意喚起の趣旨は必ずしも明確でなく、「応答結果の出力」を目的とする取扱いのみがなされる場合であれば「提供」がないとする理屈を構築し難い点を踏まえると、このような場合であっても「提供」があると見ることが現時点においては無難な対応と考えます。

[15] 前掲注 5・7-53

そうすると、個人データの提供先となる AI ベンダーが「第三者」に該当するか（上記②）が次の検討課題となります。

この点について、個人情報保護法上の委託（法 27 条 5 項 1 号）に該当する場合、当該委託先は「第三者」でなく、個人データの提供に際して本人同意が不要となります。このような「委託」における委託先が第三者でないとする根拠は委託元との一体性にあります [16]。そのため、かかる「一体性」を維持できない場合は「委託」に該当しないところ、委託元が達成しようとする利用目的と離れた委託先による利用目的に用いられる場合は「委託」に該当しません。

そのため、入力（提供）した個人データが機会学習に利用されるような場合は AI ベンダーを委託先と解することはできず、翻って、機会学習機能をオフにするなどし、委託元の利用目的を達成することのみに個人データが利用される場合、委託構成を採用することで本人同意なく個人データをプロンプトに入力することが可能になると考えます。

(2)「3 年ごと見直し」における議論状況

（1）で述べた現行法上の規制は、プライバシーの保護を含めた個人の権利利益を保護することを目的として、個人情報の目的外利用（法 18 条 1 項）や要配慮個人情報の取得（法 20 条 2 項）、個人データの第三者提供（法 27 条 1 項）について、原則としてあらかじめ本人同意を取得することを求めるものです。

もっとも、生成 AI 等の新たな技術の普及等により、大量の個人情報を取り扱うビジネス・サービス等が生まれており、本人同意が求められる現行法の在り方について、個人の権利利益の保護とデータ利活用とのバランスを考慮し、その整備を検討する必要があります。

いわゆる「3 年ごと見直し」においては、個人の権利利益の保護とデータ利活用のバランスとの観点に加え、個人の権利利益に直接の影響があるのかといった観点をも考慮した上で、以下に該当する場合については、本人同意を要しないものと整理できるのではないかとの議論がされています [17]。

① 統計作成等、特定の個人との対応関係が排斥された一般的・汎用的な分析結果の獲得と利用のみを目的とした取扱いを実施する場合

② 取得の状況からみて本人の意思に反しない取扱いを実施する場合

③ 生命等の保護又は公衆衛生の向上等のために個人情報を取り扱う場合であって本人の同意を得ないことに相当の理由があるとき

生成 AI の開発・利用の場面において重要となるのは①であるところ、統計情報等の作成（AI 開発も含む）のために複数の事業者が持つデータを共有し横断的に解析するニーズが高まっていること、特定の個人との対応関係が排斥された統計情報等の作成や利用はこれによって個人の

[16] 前掲脚注 14・82 頁

[17] 委員会「『個人情報保護法　いわゆつ 3 年ごと見直しに係る検討』の今後の検討の進め方について」(2025 年 1 月 22 日)5 頁~6 頁

権利利益を侵害する恐れが少ないものであることから、本人同意なき個人データ等[18]の第三者提供（特定された利用目的の達成に必要な範囲を超える第三者提供を含む）及び公開されている要配慮個人情報の取得を可能にしても良いのではないかとの議論がされています。もっとも、同議論が妥当するのは、このような統計情報等の作成にのみ利用されることが担保されている場合であることから、以下のような条件を課すことが想定されています[19]。

＜個人データ等の本人同意なき第三者提供＞

以下の点を条件に、本人同意を得ることなく第三者提供を可能にすることが検討されています。

- 個人データ等の提供元・提供先における一定の事項（提供元・提供先の氏名・名称、行おうとする統計作成等の内容等）の公表
- 統計作成等のみを目的とした提供である旨の提供元・提供先間の書面による合意
- 提供先における目的外利用及び第三者提供の禁止を義務付け

＜公開されている要配慮個人情報の本人同意なき取得＞

以下の点を条件に、本人同意を得ることなく要配慮個人情報を取得することを可能にすることが検討されています。

- 要配慮個人情報の取得者における一定の事項（取得者の氏名・名称、行おうとする統計作成等の内容又は本規律に基づく本人同意なき個人データ等の第三者提供を行う目的である旨等）の公表
- 取得者における目的外利用及び第三者提供（本規律に基づく本人同意なき個人データ等の第三者提供を行う目的である場合における当該第三者提供を除く）の禁止を義務付け

現行法では、個人データを含む学習用データを第三者に提供する場合は、委託に基づく場合を除き、本人同意が必要となっておりますが、これらの改正が実現すれば、学習済みパラメータの作成のみを目的としている限りは、委託に基づく場合に限らず、本人同意を得ることなく第三者提供をすることが可能となります。

また、現行法では、AI モデルの開発に用いるために情報をクローリングにより収集する際、同情報に要配慮個人情報が含まれている場合には本人同意を取得することが原則となるところ、これらの改正が実現すれば、AI の学習済みパラメータの作成を行うことを目的としてクローリングを行った際に要配慮個人情報を取得したとしても、本人同意を得る必要が無くなります。

以上の通り、これらの改正が実現すると、AI 開発に際して個人情報を利用できる場面が増え、生成 AI の開発が推進されることが期待されるところ、2025 年 12 月 4 日、統計情報等の作成にのみ利用される場合には、要配慮個人情報の取得及び個人データの第三者提供について本人同

[18] 要配慮個人情報も含むと解されています。

[19] 委員会「個人情報保護法の制度的課題に対する考え方について」（2025 年 3 月 5 日）1 頁~2 頁

意を不要とする内容が法改正に含まれている旨の報道がなされました[20]。今後、委員会から公表されるであろう改正案の内容に注視が必要です。

4. まとめ

生成 AI を用いたビジネスやサービスが飛躍的に増加する中、日本国内の企業・組織による AI モデル開発等の技術開発の動きも盛んに行われています。3（2）記載の個人情報保護法の改正が実現した場合には、生成 AI の開発や利用がより活発化していくことが期待されます。

[20] 「ＡＩに個人情報、同意不要　統計化が条件　保護法改正案」朝日新聞 2025 年 12 月 4 日