AIに関わる事業者に求められる責任と実務体制―AI法の成立が意味すること

アンダーソン・毛利・友常法律事務所外国法共同事業　パートナー弁護士　**中崎 尚**

中崎尚（なかざき たかし）●東京大学法学部卒業、2001年弁護士登録。2008年コロンビア大学ロースクールLL.M.卒業。米国Arnold & Porter法律事務所勤務後に復帰。「生成AI法務・ガバナンス」ほか著作・講演多数。政府の有識者委員を歴任。個人情報保護委員会の委託調査を担当。国立健康危機管理研究機構（JIHS）監事。AI・個人情報・セキュリティ・IT・著作権ほか幅広く取り扱う。

■ AI法制定の背景と施行状況

2025年6月4日、「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法）」が公布された。第3章（人工知能基本計画）及び第4章（人工知能戦略本部）を除く条文は、同日より施行されている。

今回、日本が制定したAI法は、EUのAI Actや韓国のAI基本法といった規制を中心とする法制度とは異なり、AIの「研究開発と活用の推進」を重視する点に特徴がある。背景には、国際的な競争環境の中で、日本のAI分野の立ち遅れを懸念する産業界からのイノベーションの加速を求める声が強まっていたことがある。一方で、ディープフェイクなどAI技術の悪用が現実の脅威として認識される中、国民からはAIに対する規制を求める声も高まっていた。

このような状況を踏まえ、日本政府はAI法の概要説明資料（図1）において、「イノベーションを促進しつつ、リスクに対応するためには、既存の刑法や個別の業法に加え、新たな法律が必要である」と明示している。そのうえで、「世界のモデルとなる制度」の構築を目指すとし、欧州など規制中心の法制度とは一線を画した姿勢を打ち出した。

2025年9月1日、AI法第3章・第4章が施行されると同時に、総理大臣を本部長、全閣僚を構成員とする「人工知能戦略本部」が内閣に設置された。現在、第3条に掲げられた「人工知能基本計画（AI基本計画）」の策定が進められている。

（図1）AI法の概要

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）の概要

法律の必要性	日本のAI開発・活用は遅れている。	多くの国民がAIに対して不安。
	イノベーションを促進しつつ、リスクに対応するため、既存の刑法や個別の業法等に加え、新たな法律が必要。	
法律の概要	**目的**	**国民生活**の向上、**国民経済**の発展
	基本理念	経済社会及び**安全保障上重要** ➡ 研究開発力の保持、**国際競争力**の向上 基礎研究から活用まで総合的・計画的に推進 **適正な研究開発・活用**のため**透明性**の確保等　**国際協力において主導的役割**
	AI戦略本部	**本部長：内閣総理大臣 構成員：全閣僚**　関係行政機関等に対して必要な協力を求める
	AI基本計画	研究開発・活用の推進のために**政府が実施すべき施策の基本的な方針**等
	基本的施策	**研究開発**の推進、**施設等の整備・共用**の促進　**人材確保、教育振興** **国際的な規範策定**への参画　**適正性**のための**国際規範に即した指針**の整備 **情報収集**、権利利益を侵害する**事案の分析・対策検討、調査** **事業者等への指導・助言・情報提供**
	責務	国、地方公共団体、研究開発機関、事業者、国民の責務、関係者間の連携強化 **事業者は国等の施策に協力しなければならない**
	附則	**見直し規定**（必要な場合は所要の措置）
世界のモデルとなる法制度を構築	国際指針に則り、イノベーション促進とリスク対応を両立。最もAIを開発・活用しやすい国へ。	

出典：内閣府　AI戦略会議（第14回）資料

（図2）今後のAI政策の進め方

今後のAI政策の進め方

人工知能（AI）戦略本部の設置

法律附則※1の規定に基づき、公布の日から三月以内に設置予定。

有識者会議の設置

政令又はAI戦略本部決定等により設置予定。

AI基本計画の策定

有識者の意見も踏まえつつ本部で案を作成し、パブリックコメントを経て、AI戦略本部決定/閣議決定予定。

AI指針の整備

既存のガイドライン類との関係を分かりやすく整理しつつ、内閣府で検討予定。

情報収集、調査研究

①主要な業種の活用実態調査、②主要なAI開発者の安全性向上対策の情報収集、③最新の技術や活用事例の調査、④国民の権利利益を侵害する案件・事象の調査を内閣府で実施予定。

国際協調

関係府省庁の協力の下、広島AIプロセス、GPAI※2、AISI※3等の活動の更なる推進

※1 AI法附則（施行期日）第一条 この法律は、公布の日から施行する。ただし、第三章及び第四章並びに附則第三条及び第四条の規定は、公布の日から起算して三月を超えない範囲内において政令で定める日から施行する。（「第四章（法第19条～第28条）」は、AI戦略本部関連の規定。）

※2 GPAI（The Global Partnership on Artificial Intelligence）は、人間中心の考え方に立ち、「責任あるAI」の開発・利用をプロジェクトベースの取組で推進するため、2020年6月に発足した、政府・国際機関・産業界・有識者等のマルチステークホルダーによる国際連携イニシアティブ。

※3 AISI（AI Safety Institute）は、AIの安全性に関する評価手法等を検討・推進するため、2024年2月に独立行政法人情報処理振興機構（IPA）に設置された機関。

出典：内閣府　AI戦略会議（第14回）資料

■ AI法の適用範囲

AI法における中核的な概念である「人工知能関連技術」は、「人工的な方法により人間の認知、推論及び判断に係る知的な能力を代替する機能を実現するために必要な技術並びに入力された情報を当該技術を利用して処理し、その結果を出力する機能を実現するための情報処理システムに関する技術」と定義されている（第2条）。

ここで「予測」ではなく「推論」という言葉が選ばれているのは、自動運転のように将来の状態を予測するだけでなく、より複雑な推論を行う技術も対象に含める意図がある。また、「知的な能力」とすることで、人間の認知にかかわる他の感覚や生理的反応といった機能は対象外とされていると考えられる。

さらに、後段の「情報の処理と出力に関する技術」には、人工知能本体に限らず、その周辺にある関連技術も含まれる。例えば、学習データを効率的に処理する半導体技術、データのクリーニングや正規化技術、AIが生成したことを明示するための「電子透かし」の埋め込み技術、不適切な出力を防ぐフィルタリング技術なども、「人工知能関連技術」として位置づけられる。

AI法では、この技術を扱う関係者に対しても責務を規定しており、国（第4条）、地方公共団体（第5条）に加えて、「大学や研究法人などの研究開発機関」（第6条）、「事業活動において活用しようとする事業者」（第7条）、「国民」（第8条）が列挙されている。

■ AI法の下で「活用事業者」が負う義務

AI法は、活用事業者に対し、まず①人工知能関連技術の積極的な活用による事業活動の効率化・高度化及び新産業の創出に努めること、②第4条及び第5条に基づき、国及び地方公共団体が実施する施策に協力する義務を課している（第7条）。

特に②については、AIの研究開発を実社会に橋渡しし、国民生活の質向上や経済の発展につなげていく上で、活用事業者が担う役割の重要性を踏まえたものだ。他の関係主体に比して、より重い責務が明確に位置づけられている。

加えて、第16条では、国が以下の調査・研究等を実施する権限を有することが定められている。

- 国内外のAI関連技術の研究開発及び活用の動向に関する情報収集
- 不正な目的または不適切な方法によるAI技術の利用によって、国民の権利利益が侵害された事案の分析と、対策の検討
- その他、AI技術の研究開発及び活用の推進に資する調査・研究・開発

これらの結果に基づき、国は活用事業者等に対し、指導・助言・情報提供など、必要な措置を講ずるものとされている。

活用事業者にとって対応が求められる典型的な場面としては、まず①の情報収集に関連し、開示内容が不十分と判断された場合に、国から追加の情報提供を求められるケースがある。こうした情報は、国民への広報資料として公表される可能性もある。

もう一つの典型例としては②に関する場面で、不正な目的や不適切な方法でAI技術を開発・活用していたと判断された場合、国からの指導や助言がなされる可能性が

ある。報道によれば、重大な事案では民間事業者名の公表も検討されており、非協力的という評価がレピュテーションに与える影響は小さくない。罰則規定が存在しなくても、協力が実質的な強制となる可能性がある点には留意すべきだ。

実務上特に影響が大きいと考えられるのが、「透明性の確保」である。第3条第4項は、不正または不適切な方法でAI技術が活用された場合、その適正な実施を確保するために、開発・活用の過程における透明性確保等の必要な施策が講じられるべきと規定している。これにより、活用事業者はAIの研究開発・活用に際し、そのプロセスの透明性と安全性を確保する努力が求められる。

■ AIに関わる事業者に求められる責任

AIの活用事業者を含むAI関連事業者は、これまでは著作権をはじめとする知的財産権法、個人情報保護法などの情報保護法、そして規制業種においては業法を中心とした法令の遵守を重視して対応してきた。

一方で、AIに関わるリスクの中には、合法・違法の二元論では判断しきれないものや、価値観の対立から生じるものも多く含まれる。その判断は一様ではなく、リスクの深刻度も、日常レベルのものから社会的に看過できないものまで幅広い。したがって、違法性リスクのようにリスクを「ゼロ」に抑えるのは現実的でなく、社会的ステークホルダーが受容可能な水準にリスクを管理しつつ、AI活用による効率化やその他のベネフィットを最大化することが求められている。

このため、多くの事業者は上記の法令遵守だけでなく、AIビジネスに携わる事業者に対して倫理面やセキュリティ面を含む包括的なあり方を示した「AI事業者ガイドライン」をベースに、事業の特徴や事業者固有の事情を踏まえて、これらのリスクやベネフィットをコントロールしようとしてきた。

こうした背景から、多くの事業者は法令遵守だけでなく、倫理面やセキュリティ面を含む包括的な対応を目指してきた。AIビジネスに携わる者の基本姿勢として、「AI事業者ガイドライン」などを参照しつつ、自社の事業特性や固有の事情を踏まえたリスクとベネフィットのコントロールを試みている。

今回のAI法では罰則こそ設けられなかったものの、活用事業者に一定の義務が課された点において、これまで潜在化していたリスクの一部が法的に顕在化したとも評価できる。

特に第3条第4項に掲げられた「透明性の確保」に関しては、以下のような対応が求められる可能性がある。

① 検証可能性の確保

- ログの記録・保存：AIシステム／サービスの開発プロセス、利用時の入出力、学習プロセス、推論過程、判断根拠などについて、データ量・内容に照らして合理的な範囲でログを記録・保存する。
- 保存方法の検討：使用技術の特性や用途を踏まえ、事故原因の究明、再発防止策の検討、損害賠償責任の立証の必要性などに基づき、記録方法・頻度・保存期間を検討する。

② ステークホルダーへの情報提供

- 情報の網羅性と理解しやすさ：AIとの関係性やその性質・目的に応じて、相手の知識や理解度を踏まえながら、以下のような情報を整理・提供する。

・利用しているAIの種類や範囲
・データ収集やアノテーションの手法・学習・評価方法
・基盤AIモデルに関する情報
・能力・限界・想定利用方法・関連法令など
・対話と関与：多様なステークホルダーとの対話を通じて、社会的影響や安全性に関する意見を収集し、積極的な関与を促す。
・リスクとベネフィットの共有：AI導入による優位性とそれに伴うリスクを、実態に即して明示する。

③ 合理的かつ誠実な対応
・情報提供の適正性：プライバシーや営業秘密を尊重したうえで、使用技術の特性や用途を踏まえ、社会的合理性のある範囲で情報提供を行う。
・規程の順守：公開技術を使用する際には、それぞれの規定に準拠する。
・オープンソース化の検討：開発したAIをオープンソース化する場合には、社会的影響の評価も行う。

④ 説明可能性・解釈可能性の向上

納得感と安心感の提供：ステークホルダーが納得し、安心できるよう、AIの動作に対する説明責任を果たす。そのために、「何をどこまで説明すべきか」を説明する側が把握し、「どのような説明が求められているか」を受け手と共有したうえで、必要な対応を行う。

■ 実現に向けた実務体制

では、こうした対応はどのように実現されるべきか。まず、AIに関わる事業者といっても、開発者（デベロッパー）、提供者（プロバイダー）、利用者（ユーザー）では直面するリスクが異なる。それゆえ、講じるべき対策の内容も変わってくる。

さらに、事業者内部においても、
・経営層
・AIリスクやビジネス展開を統括する部門
・実務としてAIに携わる現場の担当部門
・その他の従業員

といった役割によって、果たすべき責任や対応も異なる。これらを十分に踏まえることが重要である。

社内体制の整備は、まず各部門におけるAIの利用状況を洗い出す「棚卸し」から始めるべきだ。その上で、現在の利用状況と、今後会社として目指すAI活用方針に即して、以下の項目を整理する必要がある。
・法令順守の観点にとどまらず、リスクとベネフィットをどう制御するかという視点
・禁止事項と推奨事項の明確化
・実際の現場状況を踏まえた具体的手順の明文化

このプロセスには、現場の理解と協力が不可欠となる。完成した社内ルールは単に文書化するだけでなく、eラーニングを含む社内教育を通じて定着を図ることが求められる。ただし、どれだけ丁寧にルールを作成したとしても、実践の中では齟齬や不足が生じることも多い。そのため、経営層のリーダーシップのもと、ルールの運用状況を継続的にモニタリングし、乖離を評価するPDCAサイクルの運用が不可欠となる。

こうした一連の取り組みの中で記録を蓄積し、AIガバナンスの目標設定や、AIマネジメントシステムの整備・運用に関する情報を、企業のコーポレートガバナンス・コードにおける非財務情報として位置づけ、外部への開示を検討することも期待されている。