総務省、経済産業省「AI事業者ガイドライン」（第1.0版）の公表

弁護士 志部 淳之介

1　はじめに

令和6年4月19日、総務省、経済産業省の連名で、「AI事業者ガイドライン」が、公表された（[1]、以下、「ガイドライン」という）。ガイドラインは、我が国におけるAIの開発・提供・利用について、主に事業者を対象とした基本指針を示すものである。内容は、従前、政府が公表していた「人間中心のAI社会原則」を出発点として、「国際的な議論のためのAI開発のガイドライン案」、「AI利活用ガイドライン」、「AI原則実践のためのガバナンス・ガイドライン」と統合・見直しを行ったものである。

本文と資料編に分かれており、本文では、AIを活用する際のリスク及びその対応方針の基本的な考え方が示されている。

ガイドラインは、5部構成である。第1部が用語の定義、第2部が基本理念、第3～5部がAIを活用した事業活動をする主体ごとの留意点を示す。

2　法的拘束力

ガイドラインなので法的拘束力はないが、一般民事事件における違法性判断には影響すると考えられる。例えば、ある会社の開発したAIが他人に損害を与え、被害者が不法行為に基づく損害賠償請求をした場合には、同ガイドライン違反の有無が、製造物責任法の責任判断や、民法709条の不法行為の違法性判断に影響を与えると考えられる。ガイドラインが示す基本指針の中でも、特にAIによる意思決定・感情操作への留意や、プライバシー権の保護、著作権との緊張関係、セキュリティの確保、利害関係者へのデータ収集や学習範囲に関する情報提供等についての指針は、実務的にも重要と考えられる。

3　定義

ガイドラインは主体別に取り組むべき事項を示している。主体は下記の三者である。

①AI開発者　AIシステムを開発する事業者を指す。

②AI提供者　AIシステムをアプリケーション、製品、既存のシステム、ビジネスプロセス等に組み込んだサービスとして、AI利用者、場合によっては業務外利用者に提供する事業者を指す。

③AI利用者　事業活動において、AIシステム又はAIサービスを利用する事業者を指す。

4　指針

各主体に課せられた共通の課題は、以下の10項目である。項目ごとに留意すべき点が示されている。

①人間中心

各主体は、憲法が保障する又は国際的に認められた人権を侵すことがないようにすべきである。

②安全性

各主体は、AIシステム・サービスの開発・提供・利用を通じ、ステークホルダーの生命・身体・財産に危害を及ぼすことがないようにすべきである。

③公平性

各主体は、AIシステム・サービスの開発・提供・利用において、特定の個人ないし集団への人種、性別、国籍、年齢、政治的信念、宗教等の多様な背景を理由とした不当で有害な偏見及び差別をなくすよう努めることが重要である。

④プライバシーポリシー保護

各主体は、AIシステム・サービスの開発・提供・利用において、その重要性に応じ、プライバシーを尊重し、保護することが重要である。

⑤セキュリティ確保

各主体は、AIシステム・サービスの開発・提供・利用において、不正操作によってAIの振る舞いに意図せぬ変更又は停止が生じることのないように、セキュリティを確保することが重要である。

⑥透明性

各主体は、AIシステム・サービスの開発・提供・利用において、AIシステム・サービスを活用する際の社会的文脈を踏まえ、AIシステム・サービスの検証可能性を確保しながら、必要かつ技術的に可能な範囲で、ステークホルダーに対し合理的な範囲で情報を提供することが重要である。

⑦アカウンタビリティ

各主体は、AIシステム・サービスの開発・提供・利用において、トレーサビリティの確保、「共通の指針」の対応状況等について、ステークホルダーに対して、各主体の役割及び開発・提供・利用するAIシステム・サービスのもたらすリスクの程度を踏まえ、合理的な範囲でアカウンタビリティを果た

すことが重要である。

⑧教育・リテラシー

各主体は、主体内の AIに関わる者が、AIの正しい理解及び社会的に正しい利用ができる知識・リテラシー・倫理感を持つために、必要な教育を行うことが期待される。また、各主体は、AIの複雑性、誤情報といった特性及び意図的な悪用の可能性もあることを勘案して、ステークホルダーに対しても教育を行うことが期待される。

⑨公正競争確保

各主体は、AIを活用した新たなビジネス・サービスが創出され、持続的な経済成長の維持及び社会課題の解決策の提示がなされるよう、AI をめぐる公正な競争環境の維持に努めることが期待される。

⑩イノベーション

各主体は、社会全体のイノベーションの促進に貢献するよう努めることが期待される。

以上をまとめた表がガイドライン21頁に掲載されている。

5　法的な観点からみた重要な留意点

本ガイドラインは、AIに関わる各主体が取り組むべき事項について、網羅的に整理したものである。いずれの事項も遵守すべきではあるが、法的なガバナンスという視点でみた場合には、特に以下の点が重要である。

(1) プライバシー保護と個人に関するデータの保護

第一に、プライバシーと個人に関するデータの保護である。すべての主体が関係する事項である。一定の個人情報から、AIを利用したプロファイリングを行い、当該個人の要配慮個人情報を生成した場合に、これが個人情報保護法上の要配慮情報の「取得」に当たり同意が必要かについては争いがある。ガイドラインは、個人情報の不適切入力及びプライバシー侵害について注意を呼び掛けていることから、今後は上記論点に影響を及ぼす可能性がある。

(2) 説明責任と透明性の確保

第二に、説明責任、透明性確保の問題である。ガイドラインは、すべてのAI主体に対して、AIを利用しているという事実や活用範囲、データ収集の手法、学習及び評価の方法、基盤としているAIモデルに関する情報等を提供すべきと明記している（ガイドライン17頁）。

仮に、AIの不具合により何らかの法的なリスクが顕在化した場合に、事前にAIに関する基本事項やリスクについて説明責任を果たしていたかどうかは、違法性判断に重要な影響を与えると考えられる。例えば、事業者がAIを利用したサービスを一般利用者に提供した場合に、安全に利用するための使い方について明確な方針・ガイダンスを設定、明示しておくことも重要である（ガイダンス27頁では、AI開発者に関する事項として明記）。第三者が誤った利用方法・本来的に想定しない利用方法を選択したことにより損害が発生した場合に、サービス提供者が責任を負うリスクを軽減できる可能性がある。

(3) 利用者の意思決定・感情操作

第三に、AIによる利用者の意思決定・感情操作等は避けるべきである。ガイドラインは、すべてのAI主体に対して、人間の意思決定、認知等、感情を不当に操作することを目的としたAIシステム・サービスの開発・提供・利用を行うべきでないと明記している（ガイドライン13頁）。近年、人間の無意識の習性に働きかけ、意思決定を誘導する、いわゆるダークパターンと呼ばれる手法が注目されている。AI技術は、大量・高速のデータ処理と精密なプロファイリングにより、従来のダークパターンをより高い精度で実現するリスクを秘めている。ガイドラインに照らしても、AIの利用方法としては不適切であり、避けるべきである。

6　おわりに

ガイドラインは、我が国のAIに関わる事業者に対して、基本指針を示すものである。一部の「取り組むべき事項」にはかなり具体的な留意点が明記されている。

ガイドラインは、禁止事項を明記するものではなくサンクションを伴う法的義務を課すものではないが、今後、民事訴訟等の法解釈に影響を与えるものと考えられる。AIに関わる事業者は、製品・サービスの設計段階からガイドラインに抵触しないよう確認し、法的問題が顕在化した場合のリスクを検討しておくことが必要である。

1　総務省、経産省「AI事業者ガイドライン 第1.0版」
https://www.meti.go.jp/press/2024/04/20240419004/20240419004-1.pdf