NAGASHIMA OHNO & TSUNEMATSU
長島・大野・常松法律事務所
NO&T Technology Law Update
テクノロジー法ニュースレター

2024年5月　No.48

日本のAIガバナンスの基本となる「AI事業者ガイドライン（第1.0版）」の概要

弁護士　殿村　桂司
弁護士　丸田　颯人

はじめに（本ガイドラインの位置付け・構成）

1.　本ガイドラインの位置付け（AIガバナンスの設計・運用のための指針）

2024年4月19日、総務省及び経済産業省から「AI事業者ガイドライン（第1.0版）」（以下「本ガイドライン」）が公開されました（本稿の執筆者の殿村と丸田は、本ガイドラインのワーキンググループ委員として本ガイドラインの策定に関与して参りました。）。

これまで、我が国においては、2017年7月の「国際的な議論のためのAI開発ガイドライン案」をはじめとして3つのAIの利活用に関するガイドラインが策定・公表されてきましたが、生成AIの普及など2017年以降現在に至るまでAI技術が急速に発展したことを踏まえ、これらの従来のガイドラインを統合・見直して新規策定されたのが本ガイドラインです。

本ガイドラインは、我が国におけるAIガバナンスの指針を示すものです。AIガバナンスとは、本ガイドラインにおいては、「AIの利活用によって生じるリスクをステークホルダーにとって受容可能な水準で管理しつつ、そこからもたらされる正のインパクト（便益）を最大化することを目的とする、ステークホルダーによる技術的、組織的、及び社会的システムの設計並びに運用」と定義されています。AIの利活用によって生じるリスクを低減又は制御するための制度としては、例えば法制度（法律）によって担保することも考えられ、実際に欧州においては、高額な罰金を背景に事業者に一定の義務を課すAI法（AI Act）を制定するというアプローチが取られています。これに対して日本は、AIに関する技術の変化やリスクの多様性等に対して、リスクベースで迅速・柔軟に対応可能なガイドライン（ソフトロー）に基づいて対応するアプローチを選択しました。すなわち、本ガイドラインは、法律のように事業者に対して画一的な義務（ルール）を課すものではなく、各事業者が、自発的・継続的に自社によるAIの利活用によって生じるリスクを評価し、その低減を図るための技術的、組織的、及び社会的システム（AIガバナンス）を設計及び運用する際の指針を示すものです。

本ガイドラインは、直接的な法的拘束力を伴わないソフトローとしての性質を有するにとどまります。AIガバナンスの設計・運用を含む取組みは、「各主体が開発・提供・利用するAIシステム・サービスの特性、用途、目的及び社会的文脈を踏まえ、各主体の資源制約を考慮しながら自主的に進めること」が期待されているものであり、各社によって異なり得るものです。しかし、AIの利活用に関する取組みが社会から不適切もしくは不十分と評価される場合は、事業活動における機会損失が生じ、事業価値の維持が困難となる事態を招くおそれがあると本ガイドラインで指摘されているように、AIの利活用に伴うレピュテーションリスクも含めて考えれば、本ガイドラインに示されている取組みを自社に必要な範囲で積極的に取り入れることが重要です。

2. 個別法との関係

なお、AI の利活用によって生じるリスクの中には、例えば、第三者の著作物を AI の学習に利用することが著作権侵害に該当しないか、個人データをプロンプトに入力することが個人情報保護法違反に該当しないか、AI による分析結果を提供することが個別の業法（医師法、弁護士法等）に違反しないか等、既存の個別法に抵触するリスクも含まれます。したがって、AI ガバナンスを検討する際には、既存の個別法との関係にも留意する必要がありますが、本ガイドラインは、個別法の解釈を示すものではありません。既存の個別法との関係については、引き続き検討する必要があります。

3. AI ホワイトペーパー2024・責任ある AI 推進基本法（仮称）との関係

2024 年 4 月 11 日に自由民主党デジタル社会推進本部「AI の進化と実装に関するプロジェクトチーム」（以下「本 PT」）から公表された「AI ホワイトペーパー2024 ステージⅡにおける新戦略－世界一 AI フレンドリーな国へ－」（以下「AI ホワイトペーパー2024」）は、世界一 AI フレンドリーな国を実現するための国家戦略を提言するものであり、本ガイドラインとは性質が異なるものですが、AI ホワイトペーパー2024 においても、「AI 事業者ガイドライン等に基づき事業者等が自発的・継続的にリスクを評価し、低減を図ることを日本の AI ガバナンスの基本とすること」が提言されており、本ガイドラインの重要性が再確認されています。さらに、「幅広い業種において、その周知・浸透、各分野に応じた具体的な実装・実行等の取組を推進すること」も提言されており、今後は、各分野に応じた個別のガイドラインや取組みの議論が加速することが予想されます[1]。その意味でも、現時点において本ガイドラインの内容を把握しておくことは重要といえます。

なお、AI ホワイトペーパー2024 では、本稿の執筆者の殿村と丸田もメンバーとなっている本 PT のワーキンググループ有志により提案された「責任ある AI 推進基本法（仮称）」の考え方等を踏まえ、「政府は、極めて大きなリスクがある AI モデルに対し、必要最小限の法的枠組みを整備すること」も提言されています。上述のとおり、日本は本ガイドラインに基づくソフトローアプローチを採用していますが、国民の安心・安全を揺るがすリスクがある一定の規模・目的の AI 基盤モデルの開発者に対して、安全性や透明性に関する必要最小限の法的義務（ハードロー）を課すことが検討されています。

4. 本ガイドラインの構成

本ガイドラインは本編と別添に分かれており、本編は AI の利活用により「どのような社会を目指すのか」(why、基本理念)とそのために「どのような取組みを行うか」（what、共通の指針）を示し、別添では「どのようなアプローチで取り組むか」(how)を具体的に示しています。本編と別添を併せると分量が多いので、まずは本稿でポイントを押さえてから本ガイドラインを読み進めていただければ幸いです。

本ガイドラインの適用対象

本ガイドラインの適用対象は、「AI 開発者」、「AI 提供者」及び「AI 利用者」とされており、それぞれの定義は以下のとおりです。

AI 開発者	AI システム[2]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、製品、既存のシステム、ビジネスプロセス等に組み込んだ

[1] 例えば、ヘルスケア領域は、利用者の健康や生命に関わり、特に機微性の高い要配慮個人情報を取り扱うため、一般的なガイドラインとは別に、業界固有の社会的責任やリスクを十分に考慮した取組みが欠かせないことから、日本デジタルヘルス・アライアンス（JaDHA）は、本ガイドラインの最終版の公表に先立つ 2024 年 1 月 18 日に、「ヘルスケア事業者のための生成 AI 活用ガイド」（https://jadha.jp/news/news20240118.html）を公表しています。

[2] 本ガイドラインにおける「AI」とは「AI システム自体･･･又は機会学習をするソフトウェア若しくはプログラムを含む抽象的な概念」をいい、「AI システム」とは「活用の過程を通じて様々なレベルの自律性をもって動作し学習する機能を有するソフトウェアを要素として含むシステム」をいいます。

	サービスとして AI 利用者又は場合によっては業務外利用者に提供する事業者
AI 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

このように、事業活動において AI を利活用する者が広く本ガイドラインの適用対象者となる点に留意が必要です。他方、プライベートで ChatGPT を使うような「業務外利用者」や、データを提供するだけの「データ提供者」は本ガイドラインの適用対象外とされています。

後述するように、AI 開発者、AI 提供者、AI 利用者のいずれに該当するかによって、重要となる事項は変わってきます。また、AI 開発者としての立場と AI 提供者としての立場を兼ねる場合や、AI 開発者としての立場と AI 利用者としての立場を兼ねる場合等も考えられるので、自社がどのような形で AI の利活用にかかわるのかを見極める必要があります。

基本理念・原則・共通の指針と主体毎の重要事項

1. 基本理念・原則・共通の指針

本ガイドラインでは日本及び多国間の枠組みで目指すべき方向性として、「人間の尊厳が尊重される社会（Dignity）」、「多様な背景を持つ人々が多様な幸せを追求できる社会（Diversity＆Inclusion）」及び「持続可能な社会（Sustainability）」の３つの「基本理念」が掲げられています。

この基本理念を実現するための取組みにおいて念頭に置くべき事項として、後述の 10 個の「共通の方針」を文章化した「原則」が定められており、この原則では、各主体が取り組むべき７つの事項と社会と連携した取組みが期待される３つの事項に共通の指針を分けて記載してあります。AI の利活用をする企業にとっては特に前者の 7 項目が重要となります。これらの共通の指針の概要を記したのが以下の表１です。

表１　共通の指針の概要

共通の指針	概要
各主体が取り組む事項	
人間中心	✓ **（人間の尊厳及び個人の自律）**AI が活用される際の社会的文脈を踏まえ、人間の尊厳及び個人の自律を尊重する ✓ **（AI による意思決定・感情の操作等への留意）**人間の意思決定等を不当に操作すること等を目的とした AI システム・サービスの開発・提供・利用は行わない ✓ **（偽情報等への対策）**AI が生成した偽情報・誤情報・偏向情報のリスクを踏まえ、必要な対策を講じる ✓ **（多様性・包摂性の確保）**より多くの人々が AI の恩恵を享受できるよう社会的弱者による AI の活用を容易にするよう注意を払う ✓ **（利用者支援）**合理的な範囲で情報を提供し、選択の機会の判断のための情報を適時かつ適切に提供する ✓ **（持続可能性の確保）**ライフサイクル全体で、地球環境への影響も検討する
安全性	✓ **（人間の生命・身体・財産、精神及び環境への配慮）**必要に応じて客観的なモニタリング及び対処も含めて人間がコントロールできる制御可能性を確保する ✓ **（適正利用）**主体のコントロールが及ぶ範囲で本来の目的を逸脱した提供・利用により危害が発生しないように AI システム・サービスの開発・提供・利用を行う ✓ **（適正学習）**学習等に用いるデータの正確性・必要な場合には最新性（データが適切であること）等を確保する
公平性	✓ **（AI モデルの各構成技術に含まれるバイアスへの配慮）**バイアスの要因となるポイントを特定する

	✓ **（人間の判断の介在）**AI に単独で判断させるだけでなく適切なタイミングで人間の判断を介在させる利用を検討する
プライバシー保護	✓ **（AI システム･サービス全般におけるプライバシーの保護）**社会的文脈及び人々の合理的な期待を踏まえ、ステークホルダーのプライバシーの重要性に応じた対応を取る
セキュリティ確保	✓ **（AI システム・サービスに影響するセキュリティ対策）**AI システム・サービスの機密性・完全性・可用性を維持し、その時点での技術水準に照らして合理的な対策を講じる ✓ **（最新動向への留意）**日々生み出される新たな攻撃手法に対応するための留意事項を確認する
透明性	✓ **（検証可能性の確保）**データ量又はデータ内容に照らし合理的な範囲で、AI システム・サービスの開発過程、利用時の入出力等のログを記録・保存する ✓ **（関連するステークホルダーへの情報提供）**それぞれが有する知識及び能力に応じ、情報の提供及び説明を行う ✓ **（合理的かつ誠実な対応）**プライバシー及び営業秘密を尊重して、社会的合理性が認められる範囲で実施する ✓ **（関連するステークホルダーへの説明可能性・解釈可能性の向上）**関連するステークホルダーの納得感及び安心感の獲得等を目的として、説明を受ける主体がどのような説明が必要かを共有し、必要な対応を講じる
アカウンタビリティ	✓ **（トレーサビリティの向上）**開発・提供・利用中に行われた意思決定等について、技術的に可能かつ合理的な範囲で追跡・遡求が可能な状態を確保する ✓ **（「共通の指針」の対応状況の説明）**「共通の指針」の対応状況について、情報の提供及び説明を定期的に行う ✓ **（責任者の明示）**各主体においてアカウンタビリティを果たす責任者を設定する ✓ **（関係者間の責任の分配）**関係者間の責任について、主体間の契約等により、責任の所在を明確化する ✓ **（ステークホルダーへの具体的な対応）**必要に応じ AI ガバナンスに関するポリシー等の方針を策定し、公表する ✓ **（文書化）**上記に関する情報を文書化して一定期間保管し、適時かつ適切なところで、入手可能かつ利用に適した形で参照可能な状態とする
社会と連携した取組みが期待される事項	
教育・リテラシー	✓ 主体内の AI に関わる者が、AI の正しい理解・利用ができる知識等を持つために、必要な教育を行う
公正競争確保	✓ AI をめぐる公正な競争環境の維持に努める
イノベーション	✓ 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

2.　主体毎の重要事項

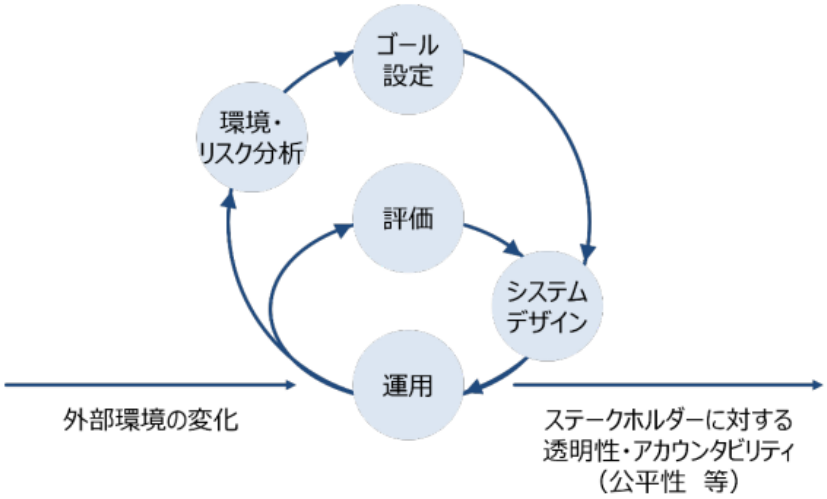
本ガイドラインは、共通の指針で示された取組みに加えて、AI システムのライフサイクルに沿って AI 開発者、AI 提供者、AI 利用者という各主体に重要となる事項を示しており（本編第 3 部から第 5 部）、その具体的な手法が細かく別添 3 から 5 において示されています。なお、これらの重要な事項についてはチェックリスト形式で別添 7C において主体毎に整理されていますのでご参照ください。

AI ガバナンスの構築

本ガイドラインでは AI ガバナンスの構築についても具体的な手法が示されています（本編第 2 部 E 及び別添 2）。上述のとおり、AI ガバナンスとは、「AI の利活用によって生じるリスクをステークホルダーにとって受容可能な水準で管理しつつ、そこからもたらされる正のインパクト（便益）を最大化することを目的とする、ステークホルダーによる技術的、組織的、及び社会的システムの設計並びに運用」と定義されています。AI に関する技術の変化やリスクの多様性等に対応するためには、このような複合的な体制（ガバナンス）を構築することが有用であると考えられていますが、その具体的な内容は、各主体が開発・提供・利用する AI システム・サービスの特性、用途、目的及び社会的文脈を踏まえ、各主体の資源制約を考慮しながら検討することが期待されており、各社による検討が必要となります。

AI ガバナンスにおいては、①「環境・リスク分析」、②「ゴール設定」、③「システムデザイン」、④「運用」、⑤「評価」（及び⑥「環境・リスク分析の再分析」）といったサイクルを、マルチステークホルダーで継続的かつ高速に回転させていく、「アジャイル・ガバナンス」の実践が重要とされており、これを図示したのが以下の図 1 です。

図 1　アジャイル・ガバナンスの基本的なモデル [3]



上記①～⑥の構築ステップを簡潔にまとめると、①まずは自社の現状及び AI の社会的受容状況を分析し、②経営陣のコミットメントを示すために AI ガバナンス・ゴールを設定する。③設定した AI ガバナンス・ゴールと現状の乖離を評価し、乖離に対応するための組織全体の方針やプロセスを経営陣が決定し、④システムの運用状況を説明可能な状態を確保する。その上で、⑤組織のガバナンス状況を継続的にモニタリング・評価し、⑥その評価結果を踏まえて再度①の分析を実施するという流れになります。

さらに、別添では上記①～⑥の構築ステップ毎に行動目標が設定されており、これらを表にしたものが下記の表 2 です。これらの行動目標にはそれぞれ「実践のポイント」及び「実践例」が示されており、具体的にどのような取組みをすればよいのか分かるようになっています。例えば、「2-1 AI ガバナンス・ゴール」の設定に関しては、「共通の指針」への対応事項等を示す自社の取組方針（「AI ポリシー」、「データ活用ポリシー」等）を設定することが考えられます。

[3] 本ガイドライン本編 p25 図 6

表２　AI ガバナンスの構築ステップと行動目標 [4]

分類	行動目標
1.環境・リスク分析	1-1 便益/リスクの理解 1-2 AI の社会的な受容の理解 1-3 自社の AI 習熟度の理解
2.ゴール設定	2-1 AI ガバナンス・ゴールの設定
3.システムデザイン	3-1 ゴール及び乖離の評価及び乖離対応の必須化 3-2 AI マネジメントの人材のリテラシー向上 3-3 各主体間・部門間の協力による AI マネジメント強化 3-4 予防・早期対応による利用者のインシデント関連の負担軽減
4.運用	4-1 AI マネジメントシステム運用状況の説明可能な状態の確保 4-2 個々の AI システム運用状況の説明可能な状態の確保 4-3 AI ガバナンスの実践状況の積極的な開示の検討
5.評価	5-1 AI マネジメントシステムの機能の検証 5-2 社外ステークホルダーの意見の検討
6.環境・リスクの再分析	6-1 行動目標 1-1～1-3 の適時の再実施

その他

ここまで紹介した内容の他、本ガイドライン別添 8 では採用 AI を扱う事業者を例にとり、本ガイドラインに沿って、AI 開発者、AI 提供者、AI 利用者が重要事項の検討を行った場合の「主体横断的な仮想事例」が掲載されています。チェックリストの記載例も示されており、自社での AI 利活用にも応用いただける内容となっておりますのでご参照ください。

おわりに

AI は日々進歩しており、AI の利活用に関するリスクを事前に網羅的に検討することは非常に困難ですが、本ガイドラインは最新の諸外国の動向も踏まえて AI の利活用時に実施することが望ましい取組みを具体的に示した文書であり、これに従った取組みを実践することでリスクを効果的に低減することが期待できます。

AI ガバナンスの構築を含む本ガイドラインで求められている対応は、基本的に各社の裁量に委ねられていますが、最終的には経営判断であり、リスクが顕在化した場合の経営責任にもつながり得るものです。共通の指針で取り上げられている各主体が取り組む事項や AI ガバナンスの構築に関しては法的観点からの検討を要する項目も多く存在するため、プロジェクトの早い段階から法律の専門家を巻き込むメリットがあると考えられます。また、欧州を含む日本国外でグローバルに事業を展開する事業者は、欧州 AI 法（AI Act）を含む諸外国の規律も遵守する必要があり、検討すべき項目は多岐にわたります。AI ガバナンスの構築に向けた取組みに関してお困りのことがあればお気軽に弊所までお問い合わせください。

以上

[4] 本ガイドライン別添 p19 表 3

[執筆者]

殿村 桂司（弁護士・パートナー）
keiji_tonomura@noandt.com
TMT（Technology, Media and Telecoms）分野を中心に、M&A・戦略的提携、ライセンス・共同開発その他の知財関連取引、テクノロジー関連法務、ベンチャー投資・スタートアップ法務、デジタルメディア・エンタテインメント、ゲーム、テレコム、宇宙、個人情報・データプロテクション、ガバナンスなど企業法務全般に関するアドバイスを提供している。
ALB の Asia Super 50 TMT Lawyers 2024、Chambers Asia-Pacific 2024 の Ranked Lawyer (TMT)、Legal 500 Asia Pacific 2024 の Leading Individuals（TMT・Fintech）に選出。

丸田 颯人（弁護士・情報処理安全確保支援士）
hayato_maruta@noandt.com
2019 年 長島・大野・常松法律事務所入所、2021 年 情報処理安全確保支援士登録、2023 年 AI 事業者ガイドラインワーキンググループ委員。
情報漏えい事件やカルテル事件をはじめとする、国内外の危機管理・コンプライアンス分野を中心に多数の調査案件・当局対応案件の経験を有するとともに、企業風土検証等の企業のガバナンス体制構築について助言をしている。近時は AI 規制に関する有識者検討委員会委員に就任するなど、最先端のテクノロジーに対する規制についても専門的な知見を有している。

[編集者]

殿村 桂司（弁護士・パートナー）
keiji_tonomura@noandt.com
企業買収（M&A）取引・知財関連取引を中心に企業法務全般に関するアドバイスを提供している。TMT 業界の案件にも幅広い経験を有しているほか、シェアリング・エコノミー、Fintech、IoT、AI などテクノロジーの発展が生み出す新しい事業分野の案件も数多く取り扱っている。

長島･大野･常松 法律事務所 www.noandt.com

〒100-7036　東京都千代田区丸の内二丁目７番２号　ＪＰタワー
Tel: 03-6889-7000（代表）　Fax: 03-6889-8000（代表）　Email: info@noandt.com

長島・大野・常松法律事務所は、約 600 名の弁護士が所属する日本有数の総合法律事務所であり、東京、ニューヨーク、シンガポール、バンコク、ホーチミン、ハノイ、ジャカルタ*及び上海に拠点を構えています。企業法務におけるあらゆる分野のリーガルサービスをワンストップで提供し、国内案件及び国際案件の双方に豊富な経験と実績を有しています。
（*提携事務所）