



## AI ガバナンスとリスク管理

令和 6 年 7 月 29 日

弁護士 山田 晃久  
[yamada\\_a@clo.gr.jp](mailto:yamada_a@clo.gr.jp)

弁護士 土肥 俊樹  
[doi\\_t@clo.gr.jp](mailto:doi_t@clo.gr.jp)

弁護士 小山 詩音  
[koyama\\_s@clo.gr.jp](mailto:koyama_s@clo.gr.jp)

### 第 1 生成 AI の登場と動向

現在、生成 AI は、文書作成に代表される ChatGPT をはじめとして、画像や動画の作成、音声合成など様々な用途にサービス展開され、様々なビジネスにおける利活用が期待されています。一方、悪用や誤用、情報の流出、権利侵害や差別の助長など、さまざまなリスクが指摘されており、その取扱いには注意を要します。生成 AI の利活用については、その便益とリスクを踏まえて各国で法規制に関する議論が重ねられており、日本においても、令和 6 年 4 月 19 日、AI ガバナンスに関する考え方を整理したガイドラインとして「AI 事業者ガイドライン（第 1.0 版）」（以下、「AI 事業者ガイドライン」といいます。）が策定されました<sup>1</sup>。以下では、AI 事業者ガイドラインについてご説明いたします。

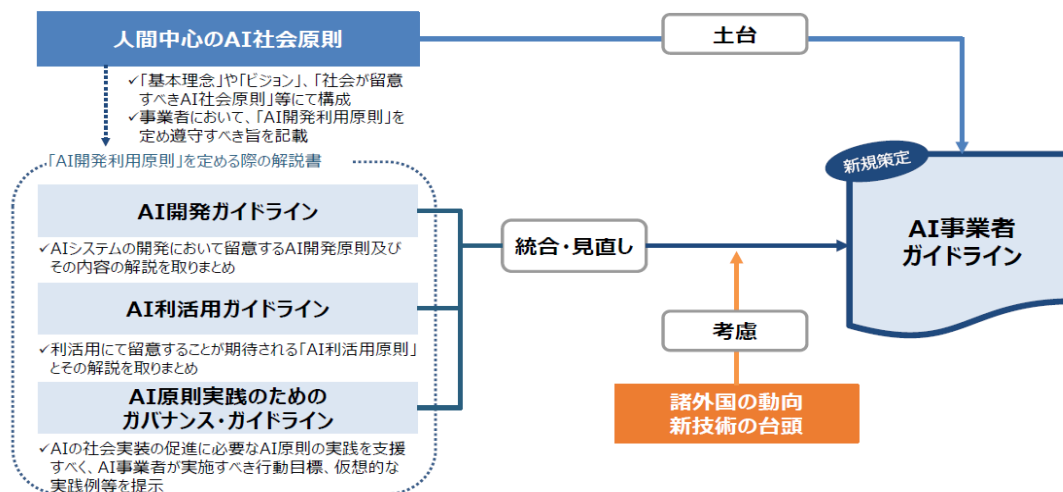
### 第 2 AI ガバナンスについて

#### 1 AI 事業者ガイドラインの策定

AI に関する議論は、従前より日本国内でも重ねられており、平成 29 年に制定された AI 開発ガイドラインをはじめ多数のガイドライン等が策定及び公表されてきました。そのような流れをうけ、下記の図のとおり、人間中心の AI 社会原則を土台としつつ、「AI 開発ガイドライン」「AI 利活用ガイドライン」「AI 原則実施のためのガバナンス・ガイドライン」という 3 つのガイドラインを統合・見直

<sup>1</sup> 経済産業省ウェブページ (<https://www.meti.go.jp/press/2024/04/20240419004/20240419004.html>)

しし、諸外国の動向や新技術の台頭を考慮して、事業者が AI の社会実装及びガバナンスをとともに実践するためのガイドラインとして令和 6 年 4 月 19 日に「AI 事業者ガイドライン」が策定されました。



(出典：総務省・経産省「AI 事業者ガイドライン (第 1.0 版)」(令和 6 年 4 月 19 日) 3 頁)

## 2 AI 事業者ガイドラインの位置づけ

AI 事業者ガイドラインは AI がもたらす社会的リスクの低減を図るとともに、AI のイノベーション及び活用を促していくために、関係者による自主的な取り組みを促すための非拘束的なソフトローという位置づけで策定されました<sup>2</sup>。したがって、AI 事業者ガイドラインはあくまで行動指針を示すものであり、これに記載された対応を取らないとしても法令違反となるものではありません。

## 3 AI 事業者ガイドラインの対象

### (1) 対象となる事業者

AI 事業者ガイドラインでは、下記の図のとおり様々な事業活動において AI の開発・提供・利用を担う全ての者を対象とし、各対象者が AI ライフサイクルにおいて担う具体的な役割を考慮して、「AI 開発者」「AI 提供者」「AI 利用者」という 3 つの事業活動主体に分けて整理しています。この枠外に、業務外利用者や、データ提供者が存在し、この 2 者は AI 事業者ガイドラインの対象外となっています<sup>3</sup>。

<sup>2</sup> 総務省・経産省「AI 事業者ガイドライン (第 1.0 版)」(令和 6 年 4 月 19 日) 2 頁

<sup>3</sup> 総務省・経産省「AI 事業者ガイドライン (第 1.0 版)」(令和 6 年 4 月 19 日) 4 頁

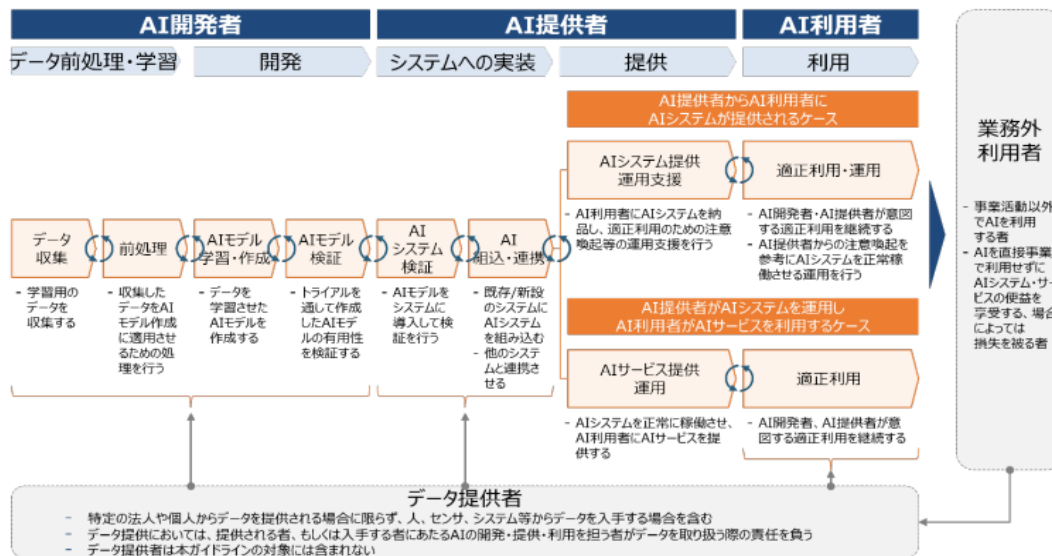


図3. 一般的な AI 活用の流れにおける主体の対応

(出典：総務省・経産省「AI 事業者ガイドライン（第1.0版）」（令和6年4月19日） 5頁）

## (2) 対象となる AI システム・AI サービス

AI 事業者ガイドラインでは、想定されうるすべての AI システム・AI サービスを広範に対象としており、あらゆる AI システムに関する取組事項のほか、高度な AI システムに関する取組事項についても触れられています。

## 4 AI 事業者ガイドラインの構成

AI 事業者ガイドラインは本編と別添に分かれます。

本編の構成は、第1部で用語の定義を中心に記載し、第2部では、基本理念や原則、各主体に共通する指針及び共通の指針を実践するために必要となるガバナンスの構築について説明しています。そして、第3部から第5部にかけて、3つの事業活動主体それぞれの留意点が記載されています。なお、第2部は各主体が取り組むべき事項を総論的に記載しているため、AIを活用する全ての事業者は、その内容を確認し、理解する必要があります。

別添は、本編の読解やそれに基づく検討・行動をサポートする解説書として位置づけられています。

なお、各主体に共通の指針及び各主体毎に重要となる事項については下記の表をご覧ください。

表 1. 「共通の指針」に加えて主体毎に重要となる事項

	第 2 部. C.共通の指針	「共通の指針」に加えて主体毎に重要となる事項		
		第 3 部. AI 開発者 (D)	第 4 部. AI 提供者 (P)	第 5 部. AI 利用者 (U)
1) 人間中心	① 人間の尊厳及び個人の自律 ② AI による意思決定・感情の操作等への留意 ③ 偽情報等への対策 ④ 多様性・包摂性の確保 ⑤ 利用者支援 ⑥ 持続可能性の確保	*	*	*
2) 安全性	① 人間の生命・身体・財産、精神及び環境への配慮 ② 適正利用 ③ 適正学習	i. 適切なデータの学習 ii. 人間の生命・身体・財産、精神及び環境に配慮した開発 iii. 適正利用に資する開発	I. 人間の生命・身体・財産、精神及び環境に配慮したリスク対策 II. 適正利用に資する提供	I. 安全を考慮した適正利用
3) 公平性	① AI モデルの各構成技術に含まれるバイアスへの配慮 ② 人間の判断の介在	I. データに含まれるバイアスへの配慮 II. AI モデルのアルゴリズム等に含まれるバイアスへの配慮	I. AI システム・サービスの構成及びデータに含まれるバイアスへの配慮	I. 入力データ又はプロンプトに含まれるバイアスへの配慮
4) プライバシー保護	① AI システム・サービス全般におけるプライバシーの保護	I. 適切なデータの学習 (D-2) I. 再掲)	I. プライバシー保護のための仕組み及び対策の導入 II. プライバシー侵害への対策	I. 個人情報の不適切入力及びプライバシー侵害への対策
5) セキュリティ確保	① AI システム・サービスに影響するセキュリティ対策 ② 最新動向への留意	I. セキュリティ対策のための仕組みの導入 II. 最新動向への留意	I. セキュリティ対策のための仕組みの導入 II. 脆弱性への対応	I. セキュリティ対策の実施
6) 透明性	① 検証可能性の確保 ② 関連するステークホルダーへの情報提供 ③ 合理的かつ誠実な対応 ④ 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	I. 検証可能性の確保 II. 関連するステークホルダーへの情報提供	I. システムアーキテクチャ等の文書化 II. 関連するステークホルダーへの情報提供	I. 関連するステークホルダーへの情報提供
7) アカウンタビリティ	① トレーサビリティの向上 ② 「共通の指針」の対応状況の説明 ③ 責任者の明示 ④ 関係者間の責任の分配 ⑤ ステークホルダーへの具体的な対応 ⑥ 文書化	I. AI 提供者への「共通の指針」の対応状況の説明 II. 開発関連情報の文書化	I. AI 利用者への「共通の指針」の対応状況の説明 II. サービス規約等の文書化	I. 関連するステークホルダーへの説明 II. 提供された文書の活用及び規約の遵守
8) 教育・リテラシー	① AI リテラシーの確保 ② 教育・リスキリング ③ ステークホルダーへのフォローアップ	*	*	*
9) 公正競争確保	*	*	*	*
10) イノベーション	① オープンイノベーション等の推進 ② 相互接続性・相互運用性への留意 ③ 適切な情報提供	I. イノベーションの機会創造への貢献	*	*

(出典：総務省・経産省「AI 事業者ガイドライン (第 1.0 版)」(令和 6 年 4 月 19 日) 21 頁)

## 5 AI ガバナンス

### (1) AI ガバナンスの定義

AI 事業者ガイドラインにおいて、AI ガバナンスは「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<sup>4</sup>。

## (2) AI ガバナンスの構築について

AI 事業者ガイドラインでは、AI ガバナンスの構築における行動を「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」「6. 環境リスクの再分析」に分類し、下記の図のとおり、これらの行動をサイクルとして行っていくことが想定され、その行動毎に行動目標が設定されています<sup>5</sup>。また、AI ガバナンスの構築においては上記の構築・運用のサイクルを高速で回転させるアジャイルガバナンスの実践が重要とされています。加えて、AI ガバナンスの検討にあたっては、AI システム・AI サービスにおけるバリューチェーン・リスクチェーンを念頭に置いた上で、複数主体間の連携確保や、バリューチェーン・リスクチェーンが複数国にまたがる場合の適切なデータ流通のためのリスク管理及びガバナンスの実施、そして、経営層へのコミットメント等にも留意することが重要となります。

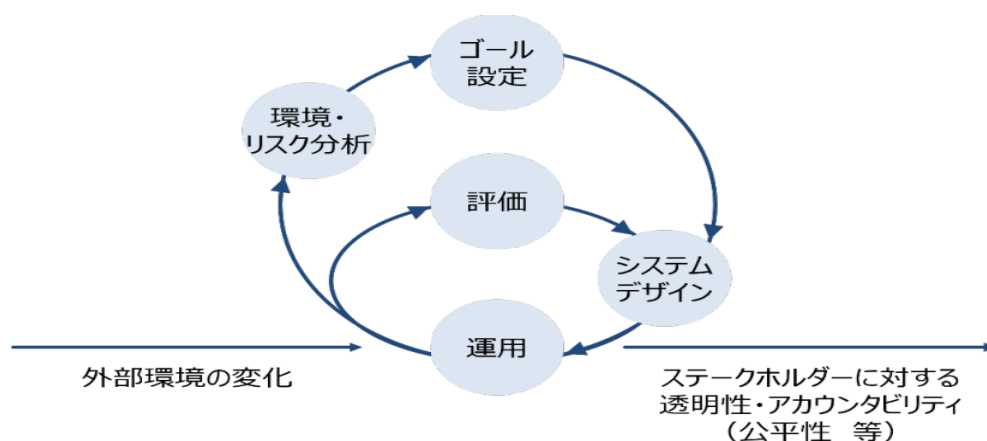


図6. アジャイル・ガバナンスの基本的なモデル

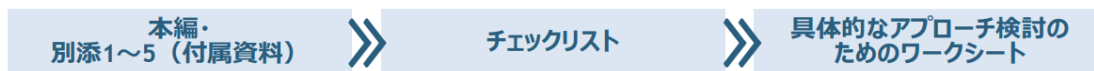
(出典：総務省・経産省「AI 事業者ガイドライン（第1.0版）」（令和6年4月19日） 25頁）

具体的なAI ガバナンス構築への取り組み方については、AI 事業者ガイドラインにおいて、下記図の流れで行うことが想定されています。自社のビジネスにおいてAIの開発やその利活用を行っている場合には、まずはAI事業者ガイドラインの内容を確認し、自社が「AI開発者」「AI提供者」「AI利用者」の位置付けにあるかを検討した上で、AIガバナンスの重要性や各主体において期待されていることを理解し、附属資料であるチェックリストを用いてその取り組みを確認す

<sup>4</sup> 総務省・経産省「AI 事業者ガイドライン（第1.0版）」（令和6年4月19日） 8頁

<sup>5</sup> 総務省・経産省「AI 事業者ガイドライン（第1.0版）別添（附属資料）」（令和6年4月19日） 19頁

る必要があります。そして、最後に附属資料であるワークシートを活用して具体的なアプローチの検討を進めることとなります。



本編・別添を読んでAIガバナンスの重要性や、各事業者に期待されることを理解する



「チェックリスト」を活用し、本編・別添についての各主体の取組(What)を確認する



「具体的なアプローチ検討のためのワークシート」を使用し、各事業者の具体的なアプローチ(How)を検討する

(出典：総務省・経産省「AI 事業者ガイドライン (第 1.0 版) 別添 (附属資料) 概要」(令和 6 年 4 月 19 日) 14 頁)

## 6 まとめ

以上のとおり、AI 事業者ガイドラインは非拘束的なソフトローという位置づけではあるものの、事業活動に AI を活用する際の基本的な考え方、事業者として取り組むべき事項及びそれらを実践するためのガバナンスの構築にかかる事項等を記載しているため、その内容について理解することが重要です。同ガイドラインについては、今後も適宜内容の更新が想定されているため<sup>6</sup>、その動向にも注視していくことが望まれます。

以上

<sup>6</sup> 総務省・経産省「AI 事業者ガイドライン (第 1.0 版)」(令和 6 年 4 月 19 日) 3 頁

当事務所では、主として名刺交換をさせていただいた方を対象とし、有用な法律情報等をお知らせすべく定期的にメールマガジンを発行させていただいております。また、バックナンバーは[こちら](#)に掲載しておりますので、あわせてご覧ください。

本稿は一般的な情報を提供するもので、リーガルアドバイスを目的とするものではありません。本稿記載の見解は執筆担当者の個人的見解であり、当事務所の見解ではありません。個別の案件については当該案件の個別の状況に応じ、弁護士の適切なアドバイスを求めていただく必要がございます。お問い合わせ等ございましたら、執筆担当者までご遠慮なくご連絡くださいますよう、お願いいたします。

【配信停止・お問い合わせについて】

今後、本メールマガジンの配信又は配信停止をご希望の方、メールアドレスの変更その他お問い合わせがございましたら、大変お手数ではございますが、下記メールアドレスまでご連絡ください。

([clo\\_mlstop@clo.gr.jp](mailto:clo_mlstop@clo.gr.jp))