AI事業者ガイドライン（第1.0版）の徹底解説と同ガイドラインに準拠したポリシー・社内規程・利用規約をどう作るか？

（連絡先）
TEL: 03-5288-1021（代表）
Email: m-watanabe@miyake.gr.jp
k-koshida@miyake.gr.jp
k-iwata@miyake.gr.jp
n-idenuma@miyake.gr.jp

弁護士法人 三宅法律事務所
弁護士　渡邉　雅之
同　越田　晃基
同　岩田　憲二郎
同　出沼　成真

1. AI事業者ガイドラインの概要

AI事業者ガイドライン（第1.0版）

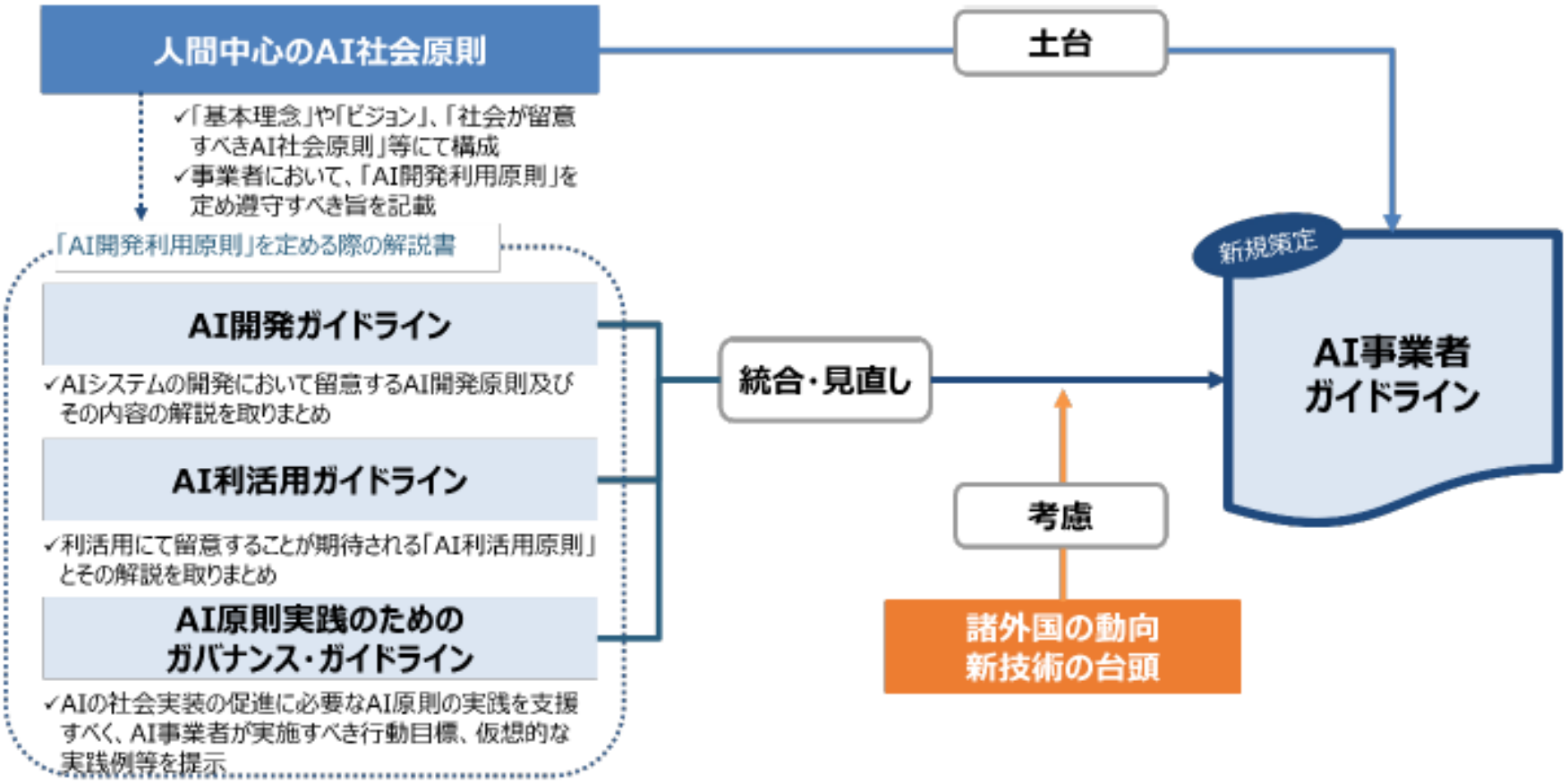
制定の経緯

- 2019年３月、「人間中心のAI社会原則」
  ⇒「AI開発ガイドライン」「AI利活用ガイドライン」（総務省）、「AI原則実践のためのガバナンス・ガイドライン」
- 2022年11月、OpenAI社のChatGPTのサービスの開始
  ⇒生成AIサービス急速に広がる
- 2023年４月「G7デジタル・技術閣僚宣言」
- 2023年５月「広島AIプロセス」（G7広島サミット）
- 2023年５月「AI戦略会議」（政府司令塔）設置
  ⇒「AIに関する暫定的な論点整理」

総務省・経済産業省がAIに関する懸念やリスクに適切に対応するための方針として、AI事業者向けの統一的でわかりやすいガイドラインの検討に着手
⇒「AIネットワーク社会推進会議」「AI事業者ガイドライン検討会」

- 2024年４月「AI事業者ガイドライン（第1.0版）」（既存のガイドラインを統合・見直し）

ガイドラインの位置付け



出所:「AI事業者ガイドライン(第1.0版)」

ガイドラインの基本的な考え方

考え方

1 事業者の自主的な取組の支援

対策の程度をリスクの大きさ及び蓋然性に対応させる「リスクベースアプローチ」にもとづいて、企業における対策の方向性を記載

2 国際的な議論との協調

国内外の関連する諸原則の動向や内容との整合性を確保

3 読み手にとっての分かりやすさ

「AI開発者」・「AI提供者」・「AI利用者」ごとに、AIに関わる考慮すべきリスクや対応方針を確認可能

＋

プロセス

マルチステークホルダー

教育・研究機関、一般消費者を含む市民社会、民間企業等で構成されるマルチステークホルダーで検討を重ねることで、実効性・正当性を重視したものとして策定

Living Document

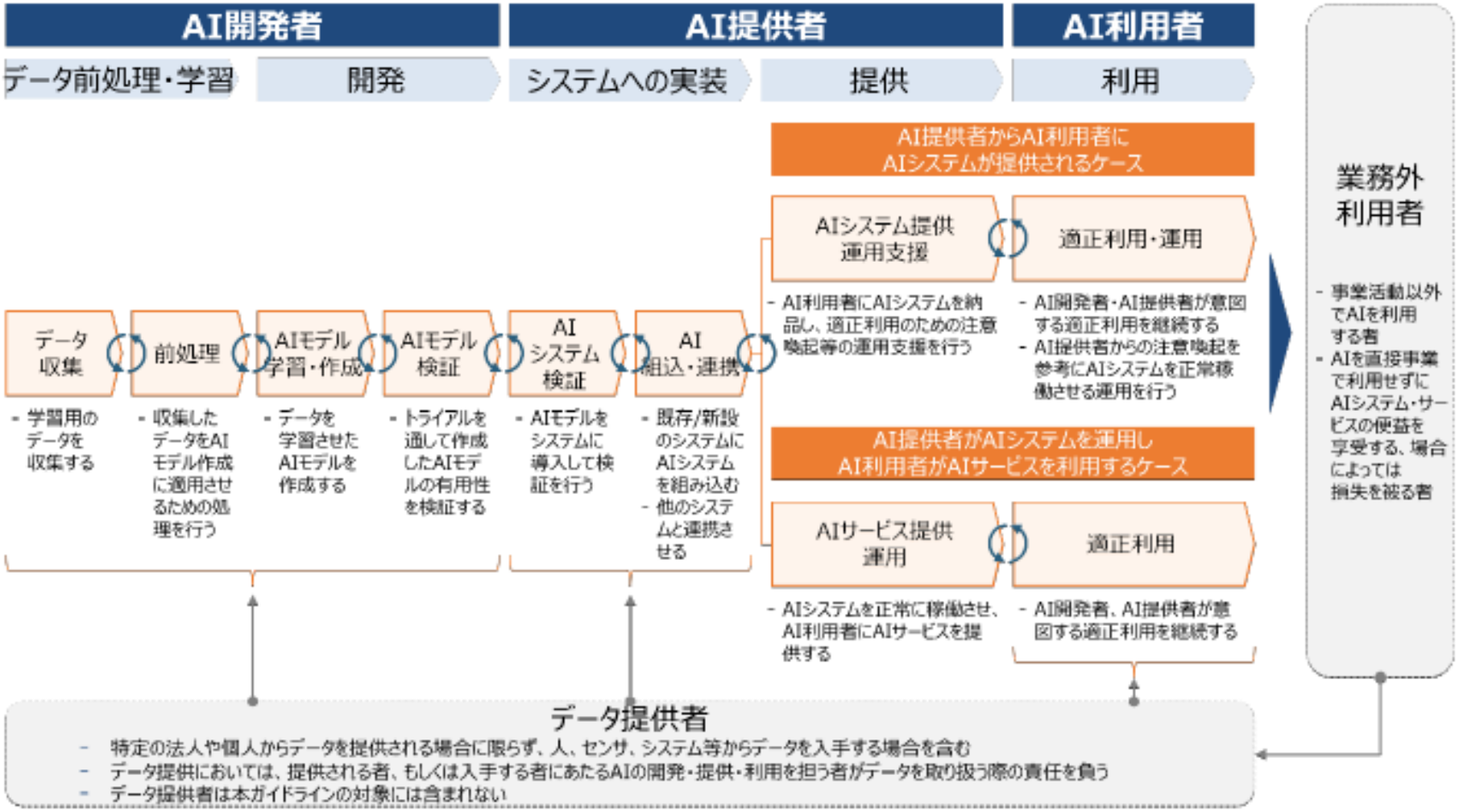
AIガバナンスの継続的な改善に向け、アジャイル・ガバナンスの思想を参考にしながら適宜、更新

出所：「AI事業者ガイドライン（第1.0版）」

AIの事業活動を担う主体

AI開発者	**AIシステムを開発する事業者（AIを研究開発する事業者を含む）** • AIモデル・アルゴリズムの開発、データ収集（購入を含む）、前処理、AIモデル学習及び検証を通して、AIモデル、AIモデルのシステム基盤、入出力機能等を含むAIシステムを構築する役割
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** • AIシステム検証、AIシステムの他システムとの連携の実装、AIシステム・サービスの提供、正常稼働のためのAIシステムにおけるAI利用者側の運用サポートまたはAIサービスの運用自体を担う。 • AIサービスの提供に伴い、様々なステークホルダーとのコミュニケーションが求められる。
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** • AI提供者が意図している適正な利用を行い、環境変化等の情報をAI提供者と共有し、正常稼働を継続することまたは必要に応じて提供されたAIシステムを運用する役割を担う。 • AIの活用において業務外利用者に何らかの影響が考えられる場合、当該者に対するAIによる意図しない不利益の回避、AIによる便益最大化の実現に努める役割を担う。

AIの開発から利用までのバリューチェーン



出所:「AI事業者ガイドライン(第1.0版)」

AIシステムの利用の例

ケース名	活用AI	概要	AI開発者	AI提供者	AI利用者	業務外利用者
採用AI	テキスト解析	A 社グループのグローバル各社における人材採用部門が、**エントリーシートの書類選考を判断する際の参考情報として使用されるAI サービス**である。 A 社AI 開発部門は、AI 利用者であるA 社人材採用部門（海外グループ企業を含む）より過去のエントリーシートデータ及び合否判定（内定の判定）結果を受領し、機械学習（分類モデル）で合否判定を支援するAI モデルを作成している。	A社 （開発部門）	A社 （システム部門・人材開発部門）	A社グループ （人材採用部門）	採用申込者
無人コンビニ	画像解析	全国のコンビニエンスストアチェーンを経営するJ 社が提供する**画像認識AI を活用した無人コンビニ（店内の客が商品を取るだけでAI が代金を計算し、店外に出る際に電子マネー等で一括決済ができるコンビニ）**である。 当AI サービスにはX 社で開発された無人コンビニ向けのAI システムを搭載している。	X社	J社 （AIシステム開発部門・コンビニ事業部）	コンビニエンス店舗	コンビニ利用客
スマート家電の最適化AI	センサデータ解析	**AI モデルが環境情報、ユーザーの行動等を解析し、スマート家電を最適化する。**A社のAI サービスは、ユーザー搭載したセンサ情報（ユーザーの位置・状態、温度、湿度、照度及びCO2 濃度）、オープンデータ（気象情報）及びユーザーからのフィードバック（ストレス、快適度の意見等）を取得してAI モデルが分析を行い、スマート家電機器（スマート冷蔵庫（食材管理、レシピ提案等）、空調、床暖房、空気清浄機、ロボット掃除機、換気システム等）を自動制御する。 AI 提供者はA 社（アプライアンス事業部）だが、代理店の場合もあり、消費者への説明等業務内容に応じた対応が求められる。	A社 （AI開発部）	A社 （アプライアンス事業部）	—	消費者

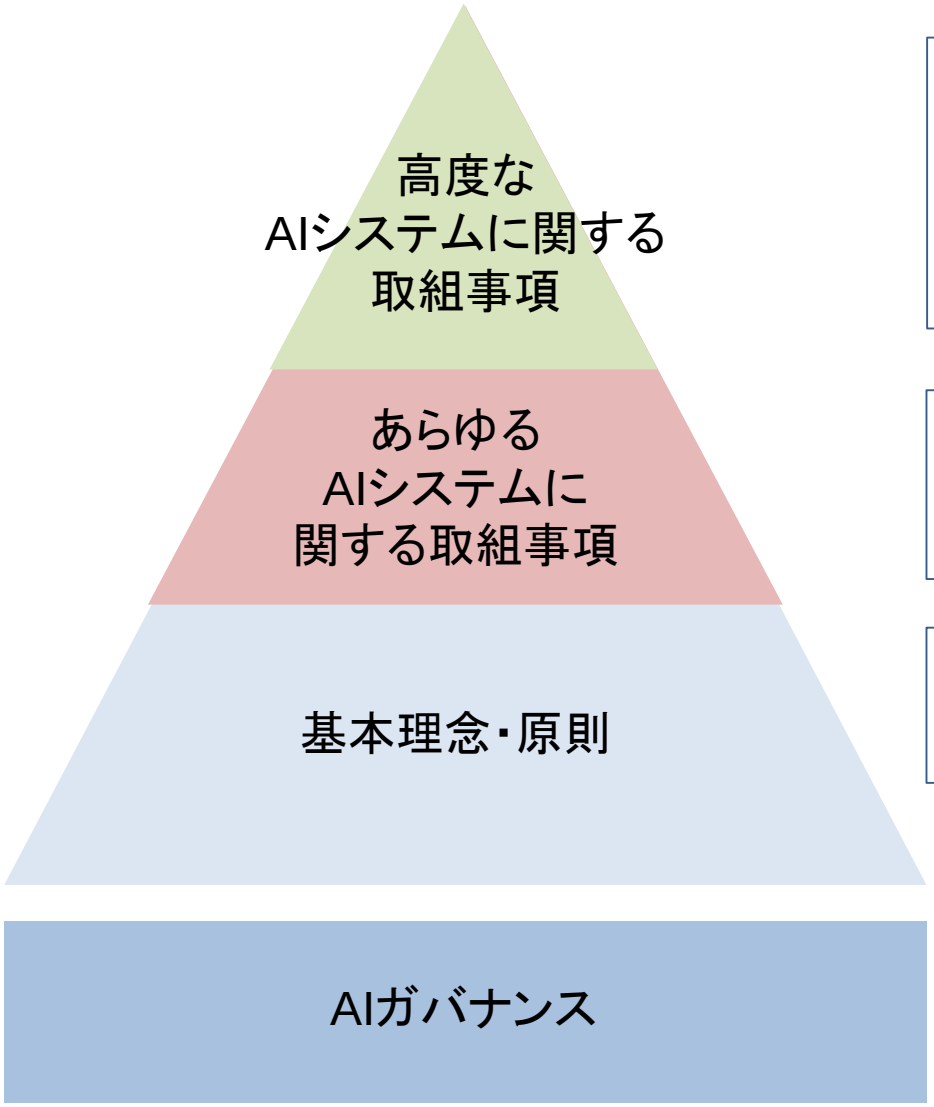
ガイドラインの構成

出所：「AI事業者ガイドライン（第1.0版）」

ガイドラインの用語の定義

用語	定義
AI	現時点で確立された定義はなく（統合イノベーション戦略推進会議決定「人間中心のAI社会原則」（2019年3月29日））、広義の人工知能の外延を厳密に定義することは困難である。本ガイドラインにおけるAIは「AIシステム（以下に定義）」自体又は機械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とする。
AIシステム	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とする（機械、ロボット、クラウドシステム等）。
高度なAIシステム	最先端の基盤モデル及び生成AIシステムを含む、最も高度なAIシステムを指す。
AIモデル（MLモデル）	AIシステムに含まれ、学習データを用いた機械学習によって得られるモデルで、入力データに応じた予測結果を生成する。
AIサービス	AIシステムを用いた役務を指す。AI利用者への価値提供の全般を指しており、AIサービスの提供・運営は、AIシステムの構成技術に限らず、人間によるモニタリング、ステークホルダーとの適切なコミュニケーション等の非技術的アプローチも連携した形で実施される。
生成AI	文章、画像、プログラム等を生成できるAIモデルにもとづくAIの総称を指す。
AIガバナンス	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。

AI事業者ガイドラインと既存のガイドラインとの関係



広島AIプロセスの成果（包括的政策枠組み）を反映
- 全てのAI関係者向けおよび高度なAIシステムを開発する組織向けの広島プロセス国際指針
- 高度なAIシステムを開発する組織向けの広島プロセス国際行動規範

【第2部：D「高度なAIシステムに関する事業者に共通の指針」、第3部】

原則を元に、各主体が取り組むべき指針や事項を整理
AI開発ガイドライン、AI利活用ガイドライン（総務省）も取り込み

【第2部：C「共通の指針」、第3部～第5部】

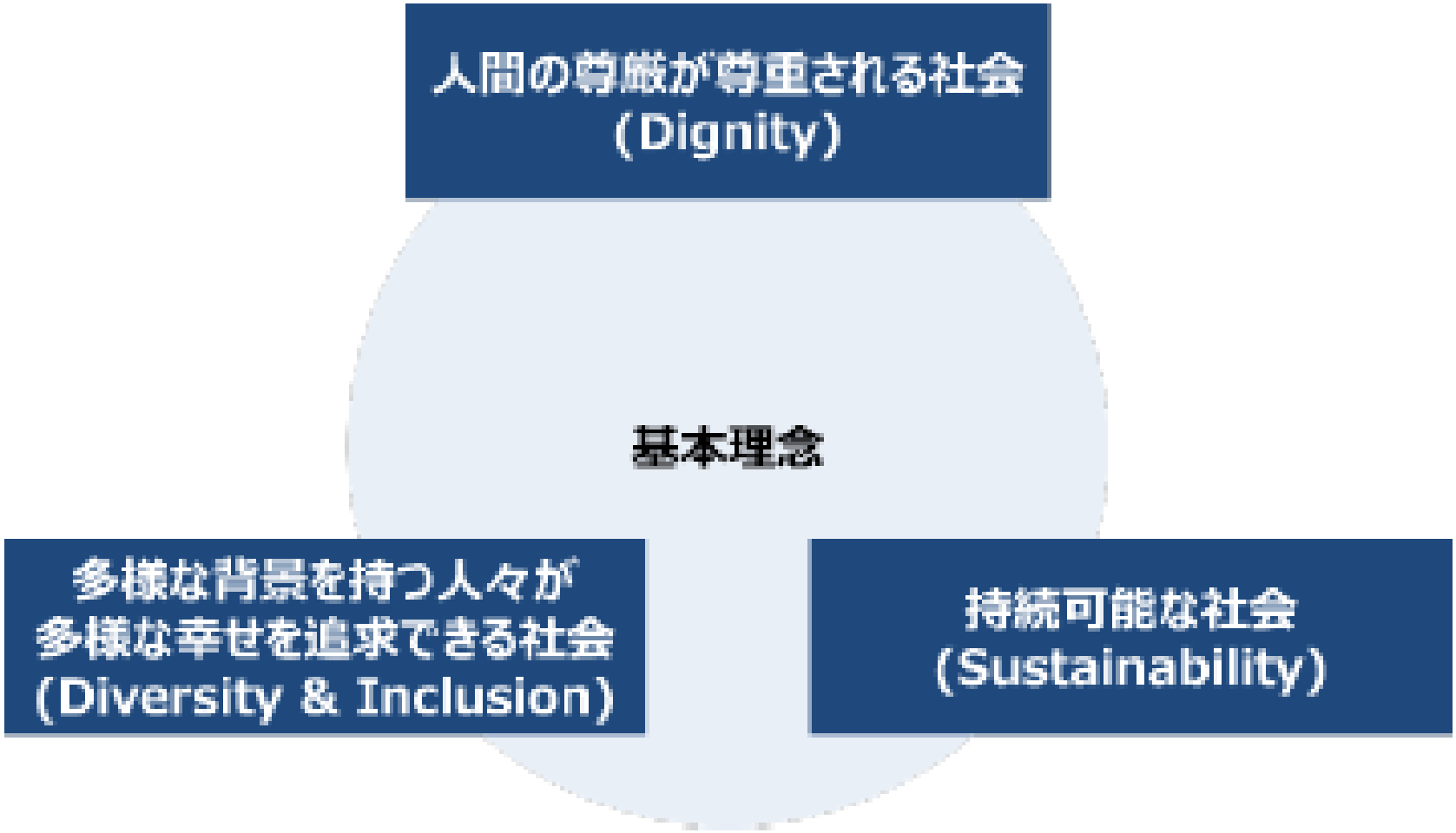
「人間中心のAI社会原則」の基本理念を土台とし、OECDのAI原則等を踏まえ、基本理念・原則を構成

【第2部：A「基本理念」、B「原則」】

AI原則実践のためのガバナンス・ガイドライン（経済産業省）を元に整理

【第2部：E「ガバナンスの構築」】

ガイドラインの基本理念

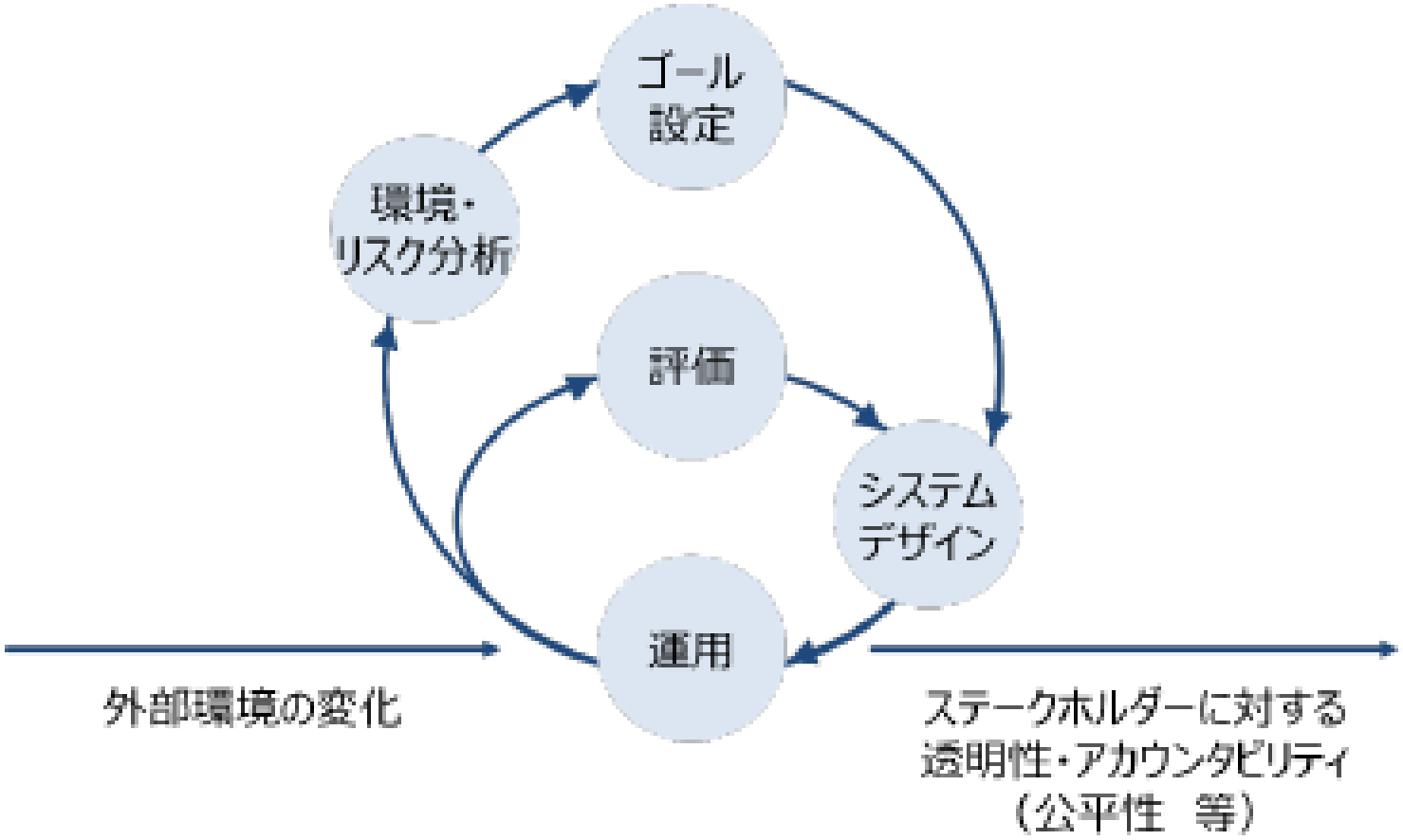


出所:「AI事業者ガイドライン(第1.0版)」

ガイドラインの原則および共通の指針

各主体が取り組む事項	①人間中心	✓ AIが人々の能力を拡張し、多様な人々の多様な幸せ（well-being）の追求が可能となるように行動する ✓ AIが生成した**偽情報・誤情報・偏向情報**が社会を不安定化・混乱させるリスクが高まっていることを認識した上で、必要な対策を講じる ✓ 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
	②安全性	✓ 適切なリスク分析を実施し、**リスクへの対策**を講じる ✓ 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することを避ける ✓ 学習等に用いる**データの透明性の確保、法的枠組みの遵守**、AIモデルの更新等を合理的な範囲で適切に実施
	③公平性	✓ 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 ✓ AIの出力結果が公平性を欠くことがないよう、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した上で、無意識や潜在的な**バイアスに留意**し、AIの開発・提供・利用を行う。
	④プライバシー保護	✓ 個人情報保護法等の**関連法令の遵守、各主体のプライバシーポリシーの策定・公表**等により、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が尊重され、保護されるよう、その重要性に応じた対応を取る
	⑤セキュリティ確保	✓ AIシステム・サービスの**機密性・完全性・可用性を維持**し、常時、AIの安全安心な活用を確保するため、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 ✓ AIシステム・サービスに対する外部からの攻撃は日々新たな手法が生まれており、これらの**リスクに対応するための留意事項を確認**する
	⑥透明性	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**（AIを利用しているという事実及び活用している範囲、データ収集及びアノテーションの手法、 AIシステム・サービスの能力、限界及び提供先における適正/不適正な利用方法　等）
	⑦アカウンタビリティ	✓ トレーサビリティの確保や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情報の提供と説明を行う ✓ 各主体の**AIガバナンスに関するポリシー、プライバシーポリシー等の方針を策定し、公表**する ✓ 関係する情報を文書化して一定期間保管し、必要なときに、必要なところで、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が期待される事項	⑧教育・リテラシー	AIに関わる者が、その関わりにおいて**十分なレベルのAIリテラシー**を確保するために必要な措置を講じる 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**
	⑨公正競争確保	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
	⑩イノベーション	国際化・多様化、**産学官連携**およびオープンイノベーションを推進 自らのAIシステム・サービスと他のAIシステムサービスとの相互接続性・相互運用性を確保 標準仕様がある場合には、それに準拠

アジャイル・ガバナンスの基本的な考え方



出所：「AI事業者ガイドライン（第1.0版）」

AI開発者に関する事項

データ前処理 学習時	**①適切なデータ学習**	✓ プライバシー・バイ・デザイン等を通じて、学習時のデータについて、適正に収集するとともに、第三者の個人情報、知的財産権に留意が必要なもの16等が含まれている場合には、法令に従って適切に扱う ✓ データのアクセスを管理するデータ管理・制限機能の導入検討を行う等、**適切な保護措置**を実施
	②データに含まれるバイアス等への配慮	✓ 学習データ、AIモデルの学習過程によってバイアスが含まれうることに留意し、**データの質を管理するための相当の措置**を講じる ✓ 学習データ、AIモデルの学習過程からバイアスを完全に排除できないことを踏まえ、**AIモデルが代表的なデータセットで学習**され、**AIシステムに不公正なバイアスがないか点検**されることを確保する
AI開発時	**①人間の生命・身体・財産、精神及び環境に配慮した開発**	✓ 予期しない環境での利用にも耐えうる性能の要求 ✓ **リスクを最小限に抑える**方法の要求
	②適正利用に資する開発	✓ **安全に利用可能なAIの使い方について明確な方針・ガイダンスを設定** ✓ 事前学習済のAIモデルに対する事後学習を行う場合に、**学習済AIモデルを適切に選択**
	③AIモデルのアルゴリズム等に含まれるバイアスへの配慮	✓ AIモデルを構成する**各技術要素によってバイアスが含まれうる**ことまで検討 ✓ AIモデルが代表的なデータセットで学習され、AIシステムに不公正なバイアスがないか点検されることを確保する
	④セキュリティ対策のための仕組みの導入	✓ 採用する技術の特性に照らし**適切にセキュリティ対策を講ずる**（セキュリティ・バイ・デザイン）
	⑤検証可能性の確保	✓ AIの予測性能及び出力の品質が、活用開始後に大きく変動する可能性又は想定する精度に達しないこともある特性を踏まえ、**事後検証のための作業記録を保存**しつつ、その品質の維持・向上を行う
開発後	**①最新動向への留意**	✓ AIシステムに対する攻撃手法は日々新たなものが生まれており、これらのリスクに対応するため、**開発の各工程で留意すべき点を確認**する
	②関連するステークホルダーへの情報提供	✓ AIシステムの技術的特性、安全性確保の仕組み、利用の結果生じる可能性のある予見可能なリスク及びその緩和策等の安全性、AIシステムの動作状況に関する情報並びに不具合の原因及び対応状況等に関する**情報を提供**
	③AI提供者への「共通の指針」への対応状況の説明	✓ AI提供者に対して、AIには活用開始後に予測性能又は出力の品質が大きく変動する可能性、想定する精度に達しないこともある旨、その結果**生じうるリスク等の情報提供及び説明**を行う
	④開発関連情報の文書化	✓ AIシステムの開発過程、意思決定に影響を与えるデータ収集及びラベリング、使用されたアルゴリズム等について、可能な限り第三者が検証できるような形で**文書化**
	⑤イノベーションの機会創造への貢献	✓ AIの**品質・信頼性、開発の方法論等の研究開発**を行う ✓ **持続的な経済成長の維持及び社会課題の解決策**が提示されるよう貢献する ✓ DFFT等の国際議論の動向の参照、AI開発者コミュニティ又は学会への参加の取組等、国際化・多様化及び産学官連携を推進する ✓ **社会全体へのAIに関する情報提供**を行う

AI提供者に関する事項

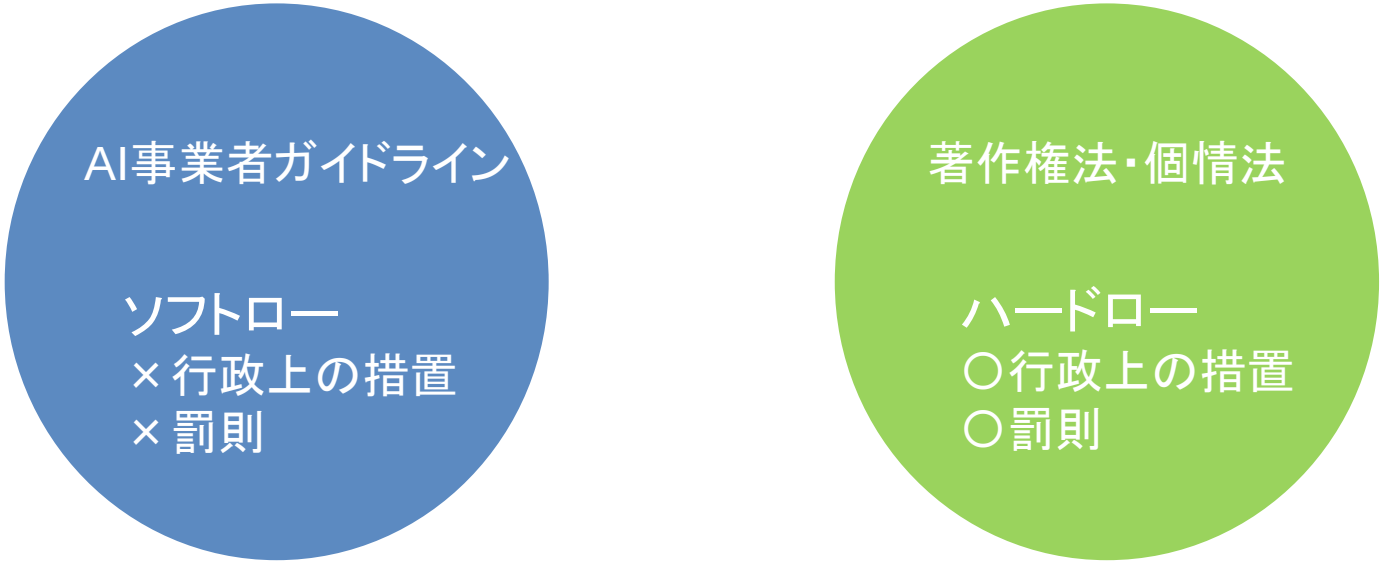
AIシステム実装時	**①人間の生命・身体・財産、精神及び環境に配慮したリスク対策**	✓ 様々な状況下でAIシステムがパフォーマンスレベルを維持できるようにし、**リスクを最小限に抑える方法**を検討
	②適正利用に資する提供	✓ AI開発者が設定した範囲でAIを活用する ✓ 提供時点でAIシステム・サービスの正確性・必要な場合には学習データの最新性等を担保すると同時に、**AI開発者が設定したAIの想定利用環境とAIシステム・サービスの利用者の利用環境に違い等がないかを検討**する
	③AIシステム・サービスの構成及びデータに含まれるバイアスへの配慮	✓ 提供時点でデータの公平性の担保及び参照する情報、連携する外部サービス等の**バイアスを検討**する ✓ AIモデルの入出力及び**判断根拠を定期的に評価**し、バイアスの発生をモニタリングする ✓ AIモデルの出力結果を受け取るAIシステム・サービス、ユーザーインタフェースにおいて、ビジネスプロセス及びAI利用者又は業務外利用者の判断を恣意的に制限するようなバイアスが含まれてしまう可能性を検討する
	④プライバシー保護のための仕組み及び対策の導入	✓ AIシステムの実装の過程を通じて、採用する技術の特性に照らし適切に個人情報へのアクセスを管理・制限する仕組みの導入等の**プライバシー保護のための対策**を講ずる（プライバシー・バイ・デザイン）
	⑤セキュリティ対策のための仕組みの導入	✓ 採用する技術の特性に照らし**適切にセキュリティ対策を講ずる（セキュリティ・バイ・デザイン）**
	⑥システムアーキテクチャ等の文書化	✓ AIシステム・サービスのシステムアーキテクチャ、データの処理プロセス等について**文書化**する
AIシステム・サービス提供後	**①適正利用に資する提供**	✓ **適切な目的**でAIシステム・サービスが利用されているかを定期的に検証する
	②プライバシー侵害への対策	✓ AIシステム・サービスにおけるプライバシー侵害に関して**適宜情報収集し、侵害を認識した場合等は適切に対処するとともに、再発の防止**を検討する
	③脆弱性への対応	✓ 最新のリスク及びそれに対応するために提供の各工程で気を付けるべき点の動向を確認し、**脆弱性に対応することを検討する**
	④関連するステークホルダーへの情報提供	✓ AIシステム・サービスの技術的特性、予見可能な動作状況に関する情報、不具合の原因及び対応状況、リスク及びその緩和策等の安全性に関する情報、出力又はプログラムの変化の可能性、動作状況に関する情報、不具合の原因及び対応状況、インシデント事例、学習するデータの収集ポリシー、学習方法、実施体制等を説明できるようにする ✓ **AIを利用しているという事実、活用している範囲、適切/不適切な使用方法等、更新を行った場合の更新内容及びその理由の情報**を説明できるようにする
	⑤AI利用者への共通の指針の対応状況の説明	✓ AI利用者に**適正利用を促し**、正確性・必要な場合には最新性等が担保されたデータの利用についての注意喚起、**個人情報を入力する際の留意点についての情報を提供**する ✓ AIシステム・サービスへの個人情報の不適切入力について注意喚起する
	⑥サービス規約等の文書化	✓ AI利用者に向けたサービス規約を作成するとともに**プライバシーポリシーを明示**する

AI利用者に関する事項

AIシステム・サービス利用時	**①安全を考慮した適正利用**	✓ AI提供者が定めた利用上の留意点を遵守して、**AI提供者が設計において想定した範囲内でAIシステム・サービスを利用**する ✓ AIの出力について精度及びリスクの程度を理解し、**様々なリスク要因を確認した上で利用する**
	②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	✓ 公平性が担保されたデータの入力を行い、プロンプトに含まれるバイアスに留意して、責任をもって**AI出力結果の事業利用判断を行う**
	③個人情報の不適切入力及びプライバシー侵害への対策	✓ AIシステム・サービスへ個人情報を不適切に入力することがないよう注意を払う ✓ AIシステム・サービスにおける**プライバシー侵害に関して適宜情報収集**し、防止を検討する
	④セキュリティ対策の実施	✓ AIシステムの実装の過程を通じて、採用する技術の特性に照らし適切に個人情報へのアクセスを管理・制限する仕組みの導入等の**プライバシー保護のための対策**を講ずる（プライバシー・バイ・デザイン）
	⑤関連するステークホルダーへの情報提供	✓ 公平性が担保されたデータの入力を行い、プロンプトに含まれるバイアスに留意してAIシステム・サービスから**出力結果を取得し、出力結果を事業判断に活用した際は、その結果を関連するステークホルダーに合理的な範囲で情報を提供**する
	⑥関連するステークホルダーへの説明	✓ 関連するステークホルダーの性質に応じて合理的な範囲で、適正な利用方法を含む情報提供を**平易かつアクセスしやすい形で行う** ✓ AIの特性及び用途、データの提供元となる関連するステークホルダーとの接点、プライバシーポリシー等を踏まえ、データ提供の手段、形式等について、あらかじめ当該ステークホルダーに情報提供する ✓ **関連するステークホルダーからの問合せに対応する窓口を合理的な範囲で設置**し、AI提供者とも連携の上説明及び要望の受付を行う
	⑦提供された文書の活用と規約の遵守	✓ AI提供者から提供されたAIシステム・サービスについての**文書を適切に保管・活用**する ✓ AI提供者が定めた**サービス規約を遵守**する

AI事業者ガイドラインをどのようにポリシー・社内規程・利用規約などに反映するか？

- AI事業者ガイドラインは、AIを開発・提供・利用をする事業者がAIを利活用するための指針として参考になるもの。
- もっとも、AI事業者ガイドラインは「ソフトロー」であり、著作権法や個人情報保護法のような「ハードロー」と違い、所管官庁による行政上の措置を伴うものではなく、また、罰則なども設けられていない。
- また、AI事業者ガイドラインの内容をすべてポリシー・社内規程・利用規約などに反映しようとすると「too much」になってしまう可能性がある。
- 自ら開発・提供・利用するAIについて理解し、適用可能な事項を良い意味で、「つまみ食い」していくことが重要ではないか？



２．AIと著作権に関する
チェックリスト＆ガイダンス

AIと著作権に関するチェックリスト＆ガイダンス（文化庁：令和6年7月31日）

AIと著作権に関するチェックリスト＆ガイダンス

- 近時取りまとめられた以下の文書を踏まえつつ、著作権と生成AIとの関係で生じるリスクを低減させる上で、また、自らの権利を保全・行使する上で望ましいと考えられる取組みを、生成AIに関係する当事者（ステークホルダー）の立場ごとに分かりやすい形で紹介するもの。
- 生成AIに関するポイントのうち、著作権に関するものに限って取り扱う。

① 文化庁文化審議会著作権分科会法制度小委員会「**AIと著作権に関する考え方について**」（「**考え方**」）
（本体）https://www.bunka.go.jp/seisaku/bunkashingikai/chosakuken/pdf/94037901_01.pdf
（概要版）https://www.bunka.go.jp/seisaku/bunkashingikai/chosakuken/pdf/94057901_01.pdf

② 内閣府知的財産戦略推進事務局「**AI時代の知的財産権検討会中間とりまとめ**」（「**中間とりまとめ**」）
https://www.kantei.go.jp/jp/singi/titeki2/chitekizaisan2024/0528_ai.pdf

③ 総務省・経済産業省「**AI事業者ガイドライン（第1.0版）**」（「**事業者ガイドライン**」）
（本編）https://www.soumu.go.jp/main_content/000943079.pdf
（別添）https://www.soumu.go.jp/main_content/000943081.pdf

1．1　AI開発者のリスク低減策：【データ前処理・学習時】 適切なデータの学習①

①行おうとする学習データの収集が「非享受目的」の要件を満たすか確認（法30条の4本文）	AI学習データの収集等のために行われる著作物の複製等には、原則として著作権法30条の4が適用され、権利者の許諾を要しないが、例えば以下のような場合は、AI学習データとして収集する等の場合であっても、「享受」目的が併存している場合に当たるとして、同条が適用されない場合がある。このような場合は、権利者の許諾を得て利用することが必要。 ①AI学習データに含まれる著作物の創作的表現（その全部or一部）を出力させることを目的とした追加的な学習（意図的な過学習等）を行う場合 ②検索拡張生成（RAG）等（データベースに含まれる既存の著作物の創作的表現（その全部or一部）を出力させることを目的としたものに限られる。）を実装する際に、生成AIへの入力用に、既存の著作物を含むデータベースを作成する場合（出力が、既存の著作物の「軽微利用」の範囲にとどまる場合は、著作権法第47条の5の適用も考えられる。） ③特定のクリエイターの作品である少量の著作物のみを学習データとした追加学習（LoRA（Low-Rank Adaptation）等の手法によるものであって、学習データの創作的表現（その全部or一部）を出力させることを目的としたもの）を行う場合
②行おうとする学習データの収集が「著作権者の利益を不当に害することとなる場合」の要件に該当しないか確認（法30条の4但書）	「AI学習用のデータセットとして、有償で提供されているデータベース著作物」を、AI学習のために無許諾で複製等する場合は、「著作権者の利益を不当に害することとなる場合は、この限りでない」とする著作権法30条の4ただし書に該当し、同条が適用されない場合がある。（このような著作物を利用する場合について、④も参照）
③AI学習データの収集を制限する技術的措置*を尊重 *ID/PWによるアクセス制限や”robots.txt”による制限等	• AI学習データの収集は、クローラと呼ばれるプログラムにより行われることが一般的であるが、ID/パスワードによるアクセス制限や、ウェブサイト内のファイル「robots.txt」等により、クローラによるAI学習データの収集を制限する技術的措置がとられていることがある。このような場合、こうした措置がとられていることや、過去の販売実績等から、AI学習用のデータセットとしてデータベース著作物が有償で提供される予定があると推認できる場合がある。 • このような場合に、上記のような技術的措置を回避してAI学習データを収集して行う当該データベース著作物の複製等には、②と同様に著作権法30条の4ただし書に該当し、著作権法30条の4が適用されない場合がある。（このような著作物を利用する場合について、④も参照）

1．1　AI開発者のリスク低減策：【データ前処理・学習時】 適切なデータの学習②

④学習データ収集のための著作物の複製が権利制限規定の要件を満たさない場合は、許諾を得て（ライセンス契約の締結）利用	• 「非享受目的」の要件を満たさない場合は、学習データの収集に著作権法30条の4は適用されない（①参照）。また、AI学習用に有償で提供されている（又は有償での提供予定がある）データセットについては、同条ただし書に該当するため同条が適用されない場合がある（②・③参照）。 • このような場合に著作物を学習データとして収集したい場合は、他の権利制限規定の適用がある場合を除き、権利者の許諾が必要となる。当該著作物を含むデータセットの利用については、ライセンス契約を締結する等の方法で、権利者の許諾を得て利用するようにする。
⑤海賊版サイトと知りながら学習データの収集源としない	• 海賊版等の、権利を侵害してアップロードされているデータを学習データとして収集することは、海賊版による権利侵害の助長に繋がるおそれもあり、厳に慎むべき。あるウェブサイトが海賊版等の権利侵害複製物を掲載していることを知りながら、当該ウェブサイトから学習データの収集を行った場合、この学習データを用いて開発された生成AIにより生じる著作権侵害について、AI開発者も著作権侵害の責任を問われる可能性がある。
⑥学習データである著作物をそのまま出力させるような学習方法をとらない	• AI学習データの収集等のために行われる著作物の複製等に際して著作権侵害があった場合でも、ただちにAI学習により作成された学習済みモデル自体の廃棄請求等が認められるわけではない。 • しかし、当該学習済みモデルが、学習データである著作物と類似性のある生成物を高確率で生成する状態にある等の場合には、当該学習済みモデルが「学習データである著作物の複製物」と評価され、学習済みモデルの廃棄請求が認められる場合もあり得る。そのため、学習を行う際には、学習済みモデルが学習データである著作物をそのまま出力させるようなものにならないよう、適切な方法で学習を行うことが必要。

1．2　AI開発者のリスク低減策：【AI開発時】

①知的財産権侵害リスク回避のための技術の採用	
学習データである著作物と類似したものの生成を防止する技術的措置の採用を検討	• AI開発時に、学習データである著作物と類似したものの生成を防止する技術的措置を採用しておくことは、AI学習データの収集等のために行われる著作物の複製等を行った際のAI開発者の目的の判断に際して、「非享受目的」だったとの判断にプラスに働くと考えられる。 • また、開発された生成AIの利用による著作権侵害を防止する観点からは、著作権侵害の要件としては「類似性」及び「依拠性」が必要であることから、学習データである著作物と類似したものの生成を防止することで、生成AIの利用による著作権侵害の発生確率を低減させることが可能。 • なお、開発された生成AIの利用により生じる著作権侵害については、一定の場合に（AI利用者に加えて）AI開発者も侵害の責任を問われる場合があるが、AI開発時に既存の著作物の類似物を生成することを防止する措置を取っておくことで、AI開発者が侵害の責任を問われる可能性を低減させることにも資すると考えられる。
②トレーサビリティの向上	
学習データの出所や学習の過程等が確認可能な状態を確保	• 訴訟においては、著作権法上の権利制限規定の要件を満たすことは、原則として、その適用を主張する側（著作物を利用する側）で主張・立証することが必要。 • 著作権法30条の4等の要件を満たしていることを事後に適切に立証できるよう、学習データの出所（どのようなデータセットを利用したか、クローリングの際の収集ポリシー等）、学習の過程・方法に関する意思決定（どのような学習済みモデルを作成するために、どの学習データを用いて、どのような学習を行ったか）等について記録を保存・文書化しておく等、事後的に確認・検証が可能な状態を確保しておくことが望まれる。

1．3　AI開発者のリスク低減策：【AI開発後】

関連するステークホルダーへの情報提供	
①学習データの内容についてAI利用者等への情報提供に努める	• 著作権侵害の要件である、既存の著作物との「類似性」・「依拠性」のうち、依拠性については、AI利用者が「その著作物がAIの学習データに含まれていないこと」を示すことができれば、依拠性が認められる可能性を低減させる要素となることから、AI利用者にとっては、生成AIの利用に伴う著作権侵害のリスクを低減させるため、学習データに関する適切な情報提供がされていることが有益。 • そのため、AI開発者としても、こうしたAI利用者のニーズに応えるため、技術的な可否や営業秘密等との関係も考慮しつつ、学習データの出所（どのようなデータセットを利用したか、クローリングの際の収集ポリシー等）など、学習データに関してAI利用者等への情報提供に可能な限り努めることが望まれる。
②学習済みモデルにおける類似物の生成防止措置等、モデルにおける著作権侵害防止の取組みに関する情報提供に努める	• 著作権侵害の要件としては「類似性」及び「依拠性」が必要であることから、学習データである著作物と類似したものの生成を防止することで、生成AIの利用による著作権侵害の発生確率を低減させることが可能（1．2①）。 • このような類似物の生成防止措置が施されていること等の、当該生成AI（学習済みモデル）における著作権侵害の防止に向けた取組みに関する情報は、AI提供者にとって、AIサービスの利用規約等において、AI利用者による著作権侵害行為を抑制するための措置等を適切に定める上で重要な情報。また、生成・利用段階において著作権侵害となるおそれの程度等を踏まえて利用の是非を判断する上で、AI利用者にとっても重要な情報。 • そのため、こうした情報は、AI開発者からAI提供者やAI利用者等に対して提供されることが望まれる。
社会全体へのAIに関する情報提供	
③生成AIの仕組みや技術の概要等について、広く情報提供	• 生成AIに関する技術については、関係者からの懸念の解消に向けて、AI開発者等、その開発や提供を行う事業者等から分かりやすい形で社会に対する発信がされることが望まれます。生成AIやこれに関連する技術・仕組みについて、共通の理解が関係当事者間で醸成されることは、今後、生成AIを利用するかどうか、また、利用する場合どのように利用するべきか、といった判断を関係当事者が適切に行えるようになること、ひいては、生成AIの適切な利活用の土台として必要。 • AI開発者には、生成AIの仕組みや技術の概要、動作のメカニズム等について、分かりやすい形で社会に広く情報提供することが望まれる。

2．1　AI提供者のリスク低減策：【AIシステム実装後】

知的財産権の侵害リスク回避のための技術の採用	
①学習データである著作物と類似したものの生成を防止する技術的措置の採用を検討	• 生成AIの利用による著作権侵害を防止する観点からは、著作権侵害の要件としては「類似性」及び「依拠性」が必要であることから、AIシステム実装時に、学習データである著作物と類似したものの生成を防止する技術的措置を採用しておくことで、生成AIの利用による著作権侵害の発生確率を低減させることが可能。 • なお、提供される生成AIの利用により生じる著作権侵害については、一定の場合に（AI利用者に加えて）AI提供者も侵害の責任を問われる場合があるが、AIシステム実装時に既存の著作物の類似物を生成することを防止する措置を取っておくことで、AI提供者が侵害の責任を問われる可能性を低減させることにも資すると考えられる。
適正利用に資する提供	
②著作権侵害に対する適切な予防措置及び対応の検討	• AIシステム・サービスを提供する際、どのような学習済みモデル（どのような学習データを用いているか、学習の態様・方法等）を使用するか、類似物の生成を防止するどのような措置を採用するか（①参照）等によって、当該システム・サービスの使用に伴う著作権侵害のおそれの程度は変わり得る。 • そのため、著作権侵害を生じさせない適正な方法で生成AIが利用されることに向けて、学習済みモデルの選択や技術的措置の採用等を含めた著作権侵害に対する適切な予防措置を講じることが望まれる。 • 仮に生成AIの利用により著作権侵害が生じた場合に講じるべき対応（例えば、事案に関する情報共有、AIシステム・サービスの停止・復旧、原因解明、再発防止措置等）についても、あらかじめ想定し検討しておくことが望まれる。

2．2　AI提供者のリスク低減策：【AIシステム・サービス提供後】

関連するステークホルダーへの情報提供	
①提供するAIシステム・サービスについての適切な情報提供	• 以下のような情報は、提供されるAIシステム・サービスの利用の是非を判断する上で、AI利用者にとって重要な情報であり、AI提供者からAI利用者等に対して、平易でアクセスしやすい形で情報提供されることが望まれる。 **① 提供されるシステム・サービスにおいて生成AIを利用している事実** ：生成AIを使用する場合は「考え方」で示されているような著作権との関係を踏まえて使用する必要があることから、提供されるシステム・サービスにおいて生成AIを利用している事実は適切に情報提供されることが望まれる。 **② 想定される適切・不適切な使用方法、提供するAIシステム・サービスの技術的特性等** ：提供するAIシステム・サービスの技術的特性等を踏まえ、著作権侵害を生じさせないような適切な使用方法や、著作権侵害のおそれのある不適切な使用方法（著作権侵害防止のため施されている技術的な措置を回避した使用方法など）について、AI提供者からAI利用者等に対して適切に情報提供されることが望まれる。 **③ 学習済みモデルにおける学習データの収集ポリシーやその学習方法** ：学習データに関する適切な情報提供がされていることは、AI利用者にとって重要（1-3①）。AI提供者としても、こうしたAI利用者のニーズに応えるため、技術的な可否や営業秘密等との関係も考慮しつつ、学習データの出所（どのようなデータセットを利用したか、クローリングの際の収集ポリシー等）など、学習データに関する情報についてAI利用者等への情報提供に可能な限り努めることが望まれる。
サービス規約等の文書化	
②著作権侵害となるような利用を抑制する等の観点で適切な利用規約等の整備	• 生成AIの利用により生じる著作権侵害については、一定の場合に（AI利用者に加えて）AI提供者も侵害の責任を問われる場合があるが、既存の著作物の類似物を生成することを防止する措置を取っておくことで、AI提供者が侵害の責任を問われる可能性を低減させることに資すると考えられる（2-1①）。 • 生成AI（学習済みモデル）を第三者に利用させるに際して、当該第三者（利用者）による著作権侵害行為を抑制するための利用規約上の措置等（生成指示に際して既存の著作物又はその題号等を入力することを制限する規定を盛り込むこと等）が適切に取られていることで、AI提供者が侵害の責任を問われる可能性を低減させることが可能と考えられる。
社会全体へのAIに関する情報提供	
③生成AIの仕組みや技術の概要等について、広く情報提供	• 生成AIに関する技術については、関係者からの懸念の解消に向けて、AI提供者等、その開発や提供を行う事業者等から分かりやすい形で社会に対する発信がされることが望まれる。生成AIやこれに関連する技術・仕組みについて、共通の理解が関係当事者間で醸成されることは、生成AIを利用するかどうか、また、利用する場合どのように利用するべきか、といった判断を関係当事者が適切に行えるようになること、ひいては、生成AIの適切な利活用の土台として必要。 • AI提供者には、生成AIの仕組みや技術の概要、動作のメカニズム等について、分かりやすい形で社会に広く情報提供することが望まれる。

3．1　AI利用者（業務利用者）のリスク低減方策：【AIシステム・サービス利用時①】

安全性を考慮した適正利用	
①利用しようとする生成AIについての適切な情報確認	• 以下のような情報は、AIシステム・サービスの利用の是非を判断する上で重要な情報であり、AI利用者としては、これらの情報を適切に確認しておくことが望まれる。 **①生成AIの仕組み及び特性** ：生成AIを利用する場合、仕組み上、学習データに含まれる既存の著作物と類似した生成物が生成されることがあり、また、生成AIを利用しない場合と異なりAI利用者が既存の著作物を認識していなくても、生成・利用が著作権侵害となることがある。このような生成AIの仕組みや特性を理解した上で利用することが必要。 **② AIシステム・サービスで使用されている学習済みモデルに関する情報** ：学習済みモデルで用いられた学習データに関する適切な情報提供がされていることは、生成AIの利用に伴う著作権侵害のリスクの程度等に関係するため、AI利用者にとって重要（1-3①）。AI利用者としては、AIシステム・サービスの利用に先立って、あらかじめ、AI開発者やAI提供者が提供する学習済みモデルに関する情報を確認しておくことが望まれる。 **③ AIシステム・サービスの利用規約等** ：AIシステム・サービスにおいては、利用規約等の当該システム・サービスの利用上のルールにおいて、著作権侵害のおそれがある利用方法を禁止又は制限している場合がある（他人の著作物を入力することの禁止等）。あらかじめ、利用しようとするAIシステム・サービスの利用規約等を確認し、これに従って利用することが必要。 **④ AIシステム・サービスの利用に関する、従業員等に対する適切な著作権教育** ：不十分な著作権理解に基づく誤解（例えば、AI生成物の生成・利用に伴い、既存の著作物の著作権侵害が生じるかという問題と、AI生成物の著作物性の有無の問題とを混同する等）と、これに伴うAIシステム・サービスの不適正な利用を生じさせないよう、従業員等に対して著作権制度の理解を確認しておくことが必要。
②著作権侵害に対する適切な予防措置及び対応の検討	• AI利用者としては、利用するAIシステム・サービスに応じて、著作権侵害を生じさせない適正な方法で生成AIを利用できるよう、生成AIの利用に関する内部的ルールの策定等、著作権侵害に対する適切な予防措置を講じることが望まれる。 • 仮に生成AIの利用により著作権侵害が生じた場合に講じるべき対応（例えば、事案に関する情報共有、AIシステム・サービスの停止・復旧、権利者への対応、原因解明、再発防止措置等）についても、あらかじめ想定し検討しておくことが望まれる。
③AIシステム・サービスへの著作物の入力が「非享受目的」の要件（著作権法30条の4本文）を満たすか確認	• 生成AIに対して生成の指示をする際には、既存の著作物を指示として入力する場合が想定される（いわゆるImage to Imageにおける既存画像の入力等）。 • このような場合、がある。このような場合には、生成AIへの入力に伴う著作物の複製等について、権利者の許諾を得ることが必要。

3．1　AI利用者（業務利用者）のリスク低減方策：【AIシステム・サービス利用時②】

安全性を考慮した適正利用	
④生成物の生成と利用では著作権侵害の判断が異なり得ることに留意	• 生成AIによる生成自体は、個人が私的使用の目的で生成する場合（著作権法30条1項）や企業・団体等の内部において、権利者から許諾を得て利用することを前提に、検討の過程において生成する場合（同法30条の3）は、これらの権利制限規定の範囲内であれば、権利者の許諾なく適法に行うことができる。 • これに対して、AI生成物の利用（インターネットでの配信、複製物の譲渡等）については、権利制限規定の範囲外となる場合が多いと考えられる。 • そのため、AI生成物の生成自体は適法に行える場合でも、生成物を更に利用しようとする場合は、著作権侵害を生じさせないか確認（⑤も参照）することが必要。
⑤生成物の利用に先立って、既存の著作物と類似した生成物となっていないか確認	• 著作権侵害の要件としては、既存の著作物との「類似性」及び「依拠性」の双方が必要。そのため、既存の著作物との関係で「類似性」がないAI生成物については、その利用について、著作権法上、特段の許諾を得ることは不要。 • そのため、AI生成物については、その利用に先立って、まずは既存の著作物と類似していないかを確認（インターネット検索（文章検索・画像検索）の活用など）することが必要。
関連するステークホルダーへの説明	
⑥関係するステークホルダーに対して、AIの利用について適切に説明	• AI生成物をライセンス契約等の取引の対象とする場合、当該AI生成物が著作物であるかどうかが取引の重要な要素となる場合も想定される。 • あるAI生成物について、これが著作物であることを前提にライセンス契約等の取引の対象とする場合には、関係するステークホルダーに対して、AIを利用したAI生成物であることや、その著作物性等について、適切に説明することが求められる。 • 当該AI生成物が、既存の著作物の著作権を侵害するものでないこと（特に、既存の著作物と類似したものとなっていないこと等）についても、可能な確認措置（インターネット検索等）を行っていることを適切に説明できるようにしておくことが望まれる。
⑦生成に用いたプロンプト等、生成物の生成過程が確認可能な状態の確保に努める	• 著作権侵害の要件のうち「依拠性」については、生成AIを利用した場合であっても、AI利用者が既存の著作物を認識しており、生成AIを利用して当該既存の著作物と類似したものを生成させた場合には、依拠性が認められると考えられる。生成AIへの指示（プロンプト）として既存の著作物そのものを入力した場合や、既存の著作物の題号（タイトル）、キャラクター名などの特定の固有名詞を入力した場合は、AI利用者が既存の著作物を認識していたことを推認させる間接事実となり、依拠性が認められやすくなると考えられる。 • AI生成物の利用に際しては、まずは既存の著作物と類似していないか確認することが重要である（⑤参照）、これに加えて、依拠性がないことを説明できるよう、生成に用いたプロンプト等、生成物の生成過程を確認可能な状態にしておくよう努めることが望まれる。 • AI生成物が「著作物」に該当するか（著作物性）は、生成に当たってAI利用者が有していた「創作意図」とAI利用者の「創作的寄与」の程度によって判断されることから、生成物の著作物性について関連するステークホルダーに対して説明する観点でも、生成に用いたプロンプト等を確認可能にしておくことが望まれる。

３．１　AI利用者（業務利用者）のリスク低減方策：【AIシステム・サービス利用時③】

社会全体へのAIに関する情報提供	
⑧生成AIの仕組みや技術の概要等について、広く情報提供	• 生成AIに関する技術については、AI利用者からも、関係者からの懸念の解消に向けて、分かりやすい形で社会に対する発信がされることが望まれます。生成AIやこれに関連する技術・仕組みについて、共通の理解が関係当事者間で醸成されることは、現行の法解釈を踏まえた適切な当事者間のルール・ガイドラインの構築や、今後の議論の土台として必要。 • AI利用者には、生成AIの仕組みや技術の概要、動作のメカニズム等について、分かりやすい形で社会に広く情報提供することが望まれる。

4．1　業務外利用者（一般利用者）のリスク低減方策：【AIシステム・サービス利用時①】

安全性を考慮した適正利用	
①利用しようとする生成AIについての適切な情報確認	• 以下のような情報は、AIシステム・サービスの利用の是非を判断する上で重要な情報であり、業務外利用者としては、これらの情報を適切に確認しておくことが望まれる。 **①生成AIの仕組み及び特性** ：生成AIを利用する場合、仕組み上、学習データに含まれる既存の著作物と類似した生成物が生成されることがあり、また、生成AIを利用しない場合と異なりAI利用者が既存の著作物を認識していなくても、生成・利用が著作権侵害となることがある。このような生成AIの仕組みや特性を理解した上で利用することが必要。 **② AIシステム・サービスで使用されている学習済みモデルに関する情報** ：学習済みモデルで用いられた学習データに関する適切な情報提供がされていることは、生成AIの利用に伴う著作権侵害のリスクの程度等に関係するため、AI利用者にとって重要（1-3①）。AI利用者としては、AIシステム・サービスの利用に先立って、あらかじめ、AI開発者やAI提供者が提供する学習済みモデルに関する情報を確認しておくことが望まれる。 **③ AIシステム・サービスの利用規約等** ：AIシステム・サービスにおいては、利用規約等の当該システム・サービスの利用上のルールにおいて、著作権侵害のおそれがある利用方法を禁止又は制限している場合がある（他人の著作物を入力することの禁止等）。あらかじめ、利用しようとするAIシステム・サービスの利用規約等を確認し、これに従って利用することが必要。 **④ AIシステム・サービスの利用に関する、適切な著作権理解の習得** ：不十分な著作権理解に基づく誤解（例えば、AI生成物の生成・利用に伴い、既存の著作物の著作権侵害が生じるかという問題と、AI生成物の著作物性の有無の問題とを混同する等）と、これに伴うAIシステム・サービスの不適正な利用を生じさせないよう、あらかじめ著作権制度の適切な理解を習得しておくことが必要。
②著作権侵害に対する適切な予防措置及び対応の検討	• 業務外利用者には、利用するAIシステム・サービスに応じて、著作権侵害を生じさせない適正な方法で生成AIを利用できるよう、既存の著作物と類似したものを意図した生成は行わないといった、著作権侵害を生じさせない取組みが望まれる。 • 仮に生成AIの利用により著作権侵害が生じた場合に講じるべき対応（例えば、AIシステム・サービスの利用停止・再開、権利者への対応等）についても、あらかじめ想定し検討しておくことが望まれる。
③AIシステム・サービスへの著作物の入力が「非享受目的」の要件（著作権法30条の4本文）を満たすか確認	• 生成AIに対して生成の指示をする際には、既存の著作物を指示として入力する場合が想定される（いわゆるImage to Imageにおける既存画像の入力等）。 • このような場合、入力に伴って生じる著作物の複製等は、入力された著作物を情報解析して生成AIに対する生成の指示（プロンプト）とするためのものであり、原則として著作権法第30条の4が適用されると考えられるが、「入力した既存の著作物と類似する生成物を生成させる」といった目的で入力を行う場合は、「享受」目的が併存している場合に当たるとして、同条が適用されない場合がある。このような場合には、生成AIへの入力に伴う著作物の複製等について、権利者の許諾を得ることが必要。

4．1　業務外利用者（一般利用者）のリスク低減方策：【AIシステム・サービス利用時②】

安全性を考慮した適正利用	
④生成物の生成と利用では著作権侵害の判断が異なり得ることに留意	• 生成AIによる生成自体は、個人が私的使用の目的で生成する場合（著作権法30条1項）や企業・団体等の内部において、権利者から許諾を得て利用することを前提に、検討の過程において生成する場合（同法30条の3）は、これらの権利制限規定の範囲内であれば、権利者の許諾なく適法に行うことができる。 • これに対して、AI生成物の利用（インターネットでの配信、複製物の譲渡等）については、権利制限規定の範囲外となる場合が多いと考えられる。 • そのため、AI生成物の生成自体は適法に行える場合でも、生成物を更に利用しようとする場合は、著作権侵害を生じさせないか確認（⑤も参照）することが必要。
⑤生成物の利用に先立って、既存の著作物と類似した生成物となっていないか確認	• 著作権侵害の要件としては、既存の著作物との「類似性」及び「依拠性」の双方が必要。そのため、既存の著作物との関係で「類似性」がないAI生成物については、その利用について、著作権法上、特段の許諾を得ることは不要。 • そのため、AI生成物については、その利用に先立って、まずは既存の著作物と類似していないかを確認（インターネット検索（文章検索・画像検索）の活用など）することが必要。
⑥生成に用いたプロンプト等、生成物の生成過程が確認可能な状態の確保に努める	• 著作権侵害の要件のうち「依拠性」については、生成AIを利用した場合であっても、AI利用者（業務外利用者）が既存の著作物を認識しており、生成AIを利用して当該既存の著作物と類似したものを生成させた場合には、依拠性が認められると考えられる。生成AIへの指示（プロンプト）として既存の著作物そのものを入力した場合や、既存の著作物の題号（タイトル）、キャラクター名などの特定の固有名詞を入力した場合は、AI利用者（業務外利用者）が既存の著作物を認識していたことを推認させる間接事実となり、依拠性が認められやすくなると考えられる。 • AI生成物の利用に際しては、まずは既存の著作物と類似していないか確認することが重要であるが（⑤参照）、これに加えて、依拠性がないことを説明できるよう、生成に用いたプロンプト等、生成物の生成過程を確認可能な状態にしておくよう努めることが望まれる。
⑦「私的使用目的の複製」等の権利制限規定の範囲内での利用となるか確認	• 個人が生成AIを利用する場合、AI生成物を「個人的に又は家庭内その他これに準ずる限られた範囲内において使用すること（私的使用）」を目的とする場合であれば、仮に生成物に既存の著作物との類似性及び依拠性があったとしても、権利者の許諾は必要なく、生成物の生成や私的な鑑賞などが可能。 • 学校その他の教育機関において、教員・生徒が、授業の過程において利用することを目的とする場合であれば、同様に、その目的の範囲内でAI生成物を生成して授業に利用することには、原則として権利者の許諾は必要ない。 • このように、業務外利用者の場合は生成・利用段階で適用される権利制限規定が考えられることから、著作権侵害を生じさせない観点からは、既存の著作物との類似性を十分に確認すること（⑤参照）、依拠性がないことを説明できるようにしておくこと（⑥参照）等とともに、上記のような権利制限規定が適用される範囲内での利用となっているか確認することも、より安全に利用するための一手段として考えられる。

３．AIポリシー・AIガバナンスポリシーにどのようなことを盛り込むか？

AIポリシー・AIガバナンスポリシーにどのようなことを盛り込むか？

- そもそもAIポリシーとは何か？
  - ✓ 公表の予定されたAIに関する社内ルール
    - 自社の役職員がAIに関して従うべきルール
    - あくまで社内ルールにすぎないため、（それが契約内容として組み込まれている等の事情のない限り）直ちには公表者の具体的義務・責任を構成するものではないと考えられる。
    - AIポリシーの公表により、顧客やエンドユーザ等からの信頼確保に資する。
    - 自社の公表するAIポリシーに反する事業遂行は「炎上」リスクを孕むと考えられる（⇒信頼の裏返し。公表することのデメリット）。

  - ✓ AI事業者ガイドラインにおける「AIポリシー」の用法（同24頁）

> **AIガバナンス・ゴールとして、本ガイドラインに記載の「共通の指針」への対応事項からなる自社の取組方針（「AIポリシー」等、呼称は各主体により相違）及び「共通の指針」への対応事項を包含しつつそれ以外の要素を含む取組方針（データ活用ポリシー等）を設定すること等が考えられる。AIを活用することによって包摂性を向上させる等の便益を高めるための指針を提示してもよい。また、呼称も各主体に委ねられている。**

    - AIポリシーの定義はさほど重要ではないが、「共通の指針」への対応事項は、AIポリシーの策定に当たり重視すべき事項であると考えられる。

AIポリシー・AIガバナンスポリシーにどのようなことを盛り込むか？

- そもそもAIポリシーとは何か？
  - ✓ AIポリシーにおいて、「関連するステークホルダーへの情報提供」事項（「共通の指針」のうち「透明性」に関するもの）を謳うことも考えられる。

> **② 関連するステークホルダーへの情報提供**
> - **AIとの関係の仕方、AIの性質、目的等に照らして、それぞれが有する知識及び能力に応じ、例えば、以下について取りまとめた情報の提供及び説明を行う**
>   - **AIシステム・サービス全般**
>   - **AIを利用しているという事実及び活用している範囲**
>   - **データ収集及びアノテーションの手法**
>   - **学習及び評価の手法**
>   - **基盤としているAIモデルに関する情報**
>   - **AIシステム・サービスの能力、限界及び提供先における適正/不適正な利用方法**
>   - **AIシステム・サービスの提供先、AI利用者が所在する国・地域等において適用される関連法令等**

（※）「アノテーション」とは、テキストや音声、画像などのさまざまな形式のデータに、タグやメタタグと呼ばれる情報を付与する作業のことをいう。

AIポリシー・AIガバナンスポリシーにどのようなことを盛り込むか？

◘ そもそもAIポリシーとは何か？

- ✓ 特にAI利用者においては、AIに関する利用方針を盛り込むことが考えられる。特に、AI の出力が直接に業務外利用者又は第三者に対して影響を及ぼす態様により AI を活用する場合には、業務外利用者又は第三者が AI の活用について適切に認識することができるよう、AI に関する利用方針を作成・開示し、問い合わせがあった場合には説明を行うことが考えられる（別添148頁参照）。

●以下の事項を盛り込んだAI に関する利用方針の開示

- **AI を利用している旨（具体的な機能・技術を特定できるのであれば、その名称、内容等）**
- **AI 活用の範囲及び方法**
- **AI の出力の根拠**
- **AI 活用に伴うリスク**
- **相談窓口**

- ✓ AI に関する利用方針を公表することが求められるのは、利用する AI の出力が、業務外利用者又は第三者に直接の影響を及ぼす場合であると考えられる。
  - ➢ 人事採用においてAIの出力を参照する場合
  - ➢ サービス利用の可否についてAIの出力を参照する場合　など
- ✓ 人間の思考に供するための分析道具として AI を活用するにとどまる場合又は、AI が原案を作成しつつも、最終的に人間が判断することが実質的に担保されている場合には、AI に関する利用方針の公表が必ずしも求められるわけではない。

AIポリシー・AIガバナンスポリシーにどのようなことを盛り込むか？

- そもそもAIポリシーとは何か？
  - ✓ その他のAI事業者ガイドライン及び別添に言及のある情報提供項目
    - ➢ データ収集ポリシー
    - ➢ 「共通の指針」への対応事項に加え、プライバシーに関するデータ活用の指針等を取りまとめたプライバシーポリシー　等（専ら個人情報保護法対応のみを意図したポリシーではなく、より広い意味でのポリシーを念頭に置くものと思われる。）
    - ➢ AIガバナンスに関するポリシー
    - ➢ AI 活用により包摂性向上等の便益を高めるためのポリシー
    - ➢ AIマネジメントシステムの整備及び運用等に関する情報
    - ➢ AIシステムの利用に伴うリスク管理及び安全性確保のためのポリシー
    - ➢ AIシステム・サービスについての情報
    - ➢ AIに関する利用方針

      …などなど（情報提供項目は上記の他にも散在的に言及されている。）。

  - ✓ 上記項目を形式的に網羅することは求められておらず、AIポリシーの呼称、体裁、構成及び内容は、各社の創意工夫に委ねられているものと考えられる。
    - ➢ **本来的に、「ひな形」の利用には馴染みにくい。**
  - ✓ とはいえ、何から手を付けて良いかが分からない結果、AIポリシーの策定検討が遅れてしまうことは望ましくない。
  - ✓ 例えば、AI利用者については、次のようなモデルをベースとして、各社創意工夫することはあり得るか。

AIポリシー・AIガバナンスポリシーモデル案（AI利用者）

1. AI基本指針
   - ✓ AI事業者ガイドライン第2部「C.共通の指針」をベースとして構成する。
   - ✓ 10ある「共通の指針」の全てを掲げることも考えられるが、適宜取捨選択を行うことを想定。

2. AIの利用方針
   - ① AIを利用している旨
   - ② AI活用の範囲及び方法に関する事項
   - ③ データの収集に関する事項
   - ④ AI活用に伴うリスク及びその低減策に関する事項
   - ⑤ プライバシー情報の利用に関する事項

3. 相談窓口

- ✓ 情報項目の取捨選択により、AIに関する専門知識がなくても読みやすいポリシーとなることを意識
- ✓ AIに関する専門知識のない方がAIに対して抱える漠然とした不安を軽減することを意識
- ✓ AIポリシーが過度に行為規範的になることにより、却って社内におけるAIの利活用が阻害されることのないよう留意
- ✓ 個人情報の分析等にAIが利用される場合には、個人情報保護法との関係にも留意

AIポリシー・AIガバナンスポリシーモデル案（AI利用者）

AIポリシー（仮称・利用者向け）

AIは、業務効率化、生産性・創造性の向上等の恩恵をもたらす強力なツールである一方で、各種のリスクも指摘されていることから、その利活用には、法的・倫理的な責任を伴うものであると認識しています。

そこで、当社は、AIのリスクを最低限に抑制しつつ、透明で責任のあるAIの利活用を通じ、ステークホルダーの皆さまに、より革新的な価値を提供するべく、次のとおりAIポリシーを公表します。

- ✓ いわゆる「前文」については、各社の理念や事業目的と融合させる体裁とする（少なくとも矛盾しないようにする）ことが望ましい。

AIポリシー・AIガバナンスポリシーモデル案（AI利用者）

第１　AI基本指針

１　人間中心のAI利活用

当社がAIの利活用に当たり最も重視している価値観は、人間の尊厳・個人の自律の尊重です。当社は、多様なステークホルダーが多様な幸せ（well-being）を追求することに繋がるよう、絶えずAIを利活用する社会的文脈を検証し続けます。

２　安全性の確保

当社は、セキュリティ対策に万全を期するとともに、AIの利活用状況を絶えず人間の目でモニタリングすることを通じて、ステークホルダーにAIの利活用による革新的な価値だけではなく、安心・安全をご提供いたします。

３　公平性の担保

AIには、時として誤った情報やバイアスのある情報を生み出すリスクが指摘されています。当社は、こうしたAIのリスクを正しく認識し、人間との協働による公平な判断に確実を期します。

４　AIの適正な利活用

当社は、当社のAIに関わる者が、AIを適正に利活用するために必要かつ十分な知識・リテラシー・倫理感を持つために、教育体制に万全を期します。

５　責任あるAIの利用

当社は、AIの利活用に関する責任者を設置するとともに、AIの利活用に関する相談窓口を設置し、広くステークホルダーの声に耳を傾けることを通じて、当社におけるAIの利活用の在り方を絶えず検証するとともに、ステークホルダーにアカウンタビリティを果たします。

- ✓ AI事業者ガイドライン第２部「C.共通の指針」をベースとして構成することで、概ねハズレのない体裁になるのではないかと思われる。
- ✓ 10ある「共通の指針」の全てを掲げることも考えられるが、適宜取捨選択を行うことを想定。

AIポリシー・AIガバナンスポリシーモデル案（AI利用者）

第1　AI基本指針

1　人間中心のAI利活用

当社がAIの利活用に当たり最
ステークホルダーが多様な幸
検証し続けます。

2　安全性の確保

当社は、セキュリティ対策に万
通じて、ステークホルダーにAI

3　公平性の担保

AIには、時として誤った情報や
リスクを正しく認識し、人間との

4　AIの適正な利活用

当社は、当社のAIに関わる者
ために、教育体制に万全を期し

5　責任あるAIの利用

当社は、AIの利活用に関する
ホルダーの声に耳を傾けるこ
ホルダーにアカウンタビリティを

①人間中心	✓ AIが人々の能力を拡張し、多様な人々の多様な幸せ（well-being）の追求が可能となるように行動する ✓ AIが生成した**偽情報・誤情報・偏向情報**が社会を不安定化・混乱させるリスクが高まっていることを認識した上で、必要な対策を講じる ✓ 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
②安全性	✓ 適切なリスク分析を実施し、**リスクへの対策**を講じる ✓ 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することを避ける ✓ 学習等に用いる**データの透明性の確保、法的枠組みの遵守**、AIモデルの更新等を合理的な範囲で適切に実施
③公平性	✓ 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 ✓ AIの出力結果が公平性を欠くことがないよう、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した上で、無意識や潜在的な**バイアスに留意**し、AIの開発・提供・利用を行う。
④プライバシー保護	✓ 個人情報保護法等の**関連法令の遵守、各主体のプライバシーポリシーの策定・公表**等により、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が尊重され、保護されるよう、その重要性に応じた対応を取る
⑤セキュリティ確保	✓ AIシステム・サービスの**機密性・完全性・可用性を維持**し、常時、AIの安全安心な活用を確保するため、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 ✓ AIシステム・サービスに対する外部からの攻撃は日々新たな手法が生まれており、これらの**リスクに対応するための留意事項を確認**する
⑥透明性	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**（AIを利用しているという事実及び活用している範囲、データ収集及びアノテーションの手法、 AIシステム・サービスの能力、限界及び提供先における適正/不適正な利用方法　等）
⑦アカウンタビリティ	✓ トレーサビリティの確保や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情報の提供と説明を行う ✓ 各主体の**AIガバナンスに関するポリシー、プライバシーポリシー等の方針を策定し、公表**する ✓ 関係する情報を文書化して一定期間保管し、必要なときに、必要なところで、入手可能かつ利用に適した形で参照可能な状態とする
⑧教育・リテラシー	AIに関わる者が、その関わりにおいて**十分なレベルのAIリテラシー**を確保するために必要な措置を講じる 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**
⑨公正競争確保	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
⑩イノベーション	国際化・多様化、**産学官連携**およびオープンイノベーションを推進 自らのAIシステム・サービスと他のAIシステムサービスとの相互接続性・相互運用性を確保 標準仕様がある場合には、それに準拠

- ✓ AI事業者ガイド
  ねハズレのない
- ✓ 10ある「共通の指針」の全てを掲げることも考えられるが、適宜取捨選択を行うことを想定。

AIポリシー・AIガバナンスポリシーモデル案（AI利用者）

第２　AIの利活用方針

１　AIを利活用する業務

当社は、次の業務に関して、AIを利活用しています。

・●●サービスの入会審査

　サービス申込書にご入力いただきましたお客様情報の内容を分析し、●●サービスへの入会審査、利用限度額の設定のために利用いたします。

・広告業務

　お客様の本ウェブサイトにおける閲覧履歴や購買履歴、位置情報等の情報を分析して、趣味・嗜好に応じた新商品・サービスに関する広告のために利用いたします。

・人事採用

　ご提出のあった履歴書等に記載された採用候補者の情報を分析して、当社の人事採用、採用後の配属の検討のために利用いたします。

２　データ収集の基本原則

当社は、AIを利活用するにあたり、適正妥当な方法によりデータを収集するものとし、いやしくも偽りその他不正の手段によるデータの収集は行いません。

- ✓ AI利用者による「AIに関する利用方針」の項目も参考にしつつ、社会的関心が高いと思われる項目を抜粋したもの
- ✓ データ収集の基本原則は、AI利用者において追加学習のためのデータ利活用を行う場面を念頭に置きつつ、ただし一般論に留めた記載とした
- ✓ どこまでの粒度で記載を行うかは、依然として各社判断に委ねられているものと考えられる

AIポリシー・AIガバナンスポリシーモデル案（AI利用者）

３　AIの利活用に伴うリスク及びその低減策

AIの出力する情報に誤情報やバイアスのかかった情報が含まれることにより、AIの利活用のみでは誤った判断がなされるリスクがあります。そのため、当社では、かかるリスクの低減のため、次の方策を講じています。

・●●サービスの入会審査：再審査制度の用意

●●サービスにお申込みいただいたにもかかわらず、ご希望に沿えない結果となった場合には、AIによる入会審査に加えて、当社担当者による入会の再審査を申請することができます。

・広告業務：広告へのフィードバック機能の実装

AIの分析結果に応じて掲載する広告がお客様の趣味・嗜好に沿わない場合、その広告についてフィードバックを送信することができます。当社は、お客様からのフィードバックを踏まえて、掲載する広告の内容を調整いたします。

・人事採用：AIに頼りすぎない人事採用システムの構築

当社の人事採用にはAIによる情報分析技術を利用していますが、人事採用、採用後の配属に関する最終決定は、当社の人事担当者が直接行うことで、AIに固有のリスクの低減を図っています。

- ✓ AIに漠然とした不安を抱いている層が最も知りたい情報は上記のような内容ではないかと思い作成したもの
- ✓ いずれも想定事例であり、各社のケースごとに個別的な検討を要する
- ✓ AIを利活用する業務が多岐にわたる場合、個別に問い合わせてもらうことも考えられる。
- ✓ こちらもどこまでの粒度で記載するかは各社の判断（ここまで記載しなければならないということでもない）ため、自社の考え方も踏まえて検討

AIポリシー・AIガバナンスポリシーモデル案（AI利用者）

４　プライバシーの保護について

①当社プライバシーポリシーの遵守

当社は、AIの利活用にあたり個人情報を利用するにあたっては、当社の別途定めるプライバシーポリシーを遵守いたします。当社のプライバシーポリシーは、下記URLからご確認ください。

＜URL貼付＞

【学習用データとしても利用する場合】

②当社の利用するAIの精度向上のための利用

当社は、AIの利活用にあたり収集した個人情報を、特定の個人との対応関係が排斥された学習用パラメータ（重み係数）として、当社の利用するAIの精度向上のために利用することがあります。なお、当社のAIの精度向上のために利用するデータから、特定の個人を識別することは一切ありません。

- ✓ AIと個人情報保護法は切っても切れない関係にあると思われるため、プライバシーポリシーとの連続性を示す体裁とした。
- ✓ 機械学習目的の記載は個人情報保護法上の要請に基づくもの（利用目的規制。ただし不要説もある。）
  - ➢ 本来はプライバシーポリシーに記載してもよい内容であるが、一覧性の観点から、AIポリシーに（も）記載することとした。

AIポリシー・AIガバナンスポリシーモデル案（AI利用者）

第3　相談窓口

当社によるAIの利活用に関するご相談は、下記の窓口までお問合せ下さい。
〒000-0000
東京都千代田区有楽町0-0-0
XX株式会社AI相談室
TEL:03-0000-0000（平日10時～17時）
Mail:xxxxxxxx@xxx.co.jp

✓ AI関連専用の相談窓口ではなく、一般の相談窓口を記載する運用も考えられる。

4. プライバシーポリシー（利用目的等）にどのようなことを盛り込むか？
～個人情報保護法の要請への＋αは？

プライバシーポリシー（利用目的等）にどのようなことを盛り込むか？
～個人情報保護法の要請への＋αは？

◘ AI事業者ガイドラインにおける言及

- ✓ 特に掘り下げた言及なし
  - ➢ 単に法令遵守・プライバシー保護の文脈において個人情報保護法への言及がいくつかみられるにとどまる。

◘ AI開発者たるOpenAI に対する注意喚起の概要（令和5年6月2日個人情報保護委員会）

当委員会は、令和5年6月1日付けで、OpenAI, L.L.C. 及び OpenAI OpCo, LLCに対し、個人情報の保護に関する法律（平成 15 年法律第 57 号。以下「法」という。）第 147 条の規定に基づき、下記概要のとおり、注意喚起を行った。なお、本注意喚起は、当委員会が現時点で明確に認識した懸念事項を踏まえたものであり、今後新たな懸念事項を認識した場合には、必要に応じて、追加的な対応を行う可能性がある。

記

1 要配慮個人情報の取得

あらかじめ本人の同意を得ないで、ChatGPT の利用者（以下「利用者」という。）及び利用者以外の者を本人とする**要配慮個人情報を取得しないこと**（法第 20 条第2項各号に該当する場合を除く。）。特に、以下の事項を遵守すること。

（1）機械学習のために情報を収集することに関して、以下の4点を実施すること。

① **収集する情報に要配慮個人情報が含まれないよう必要な取組を行うこと**。

② 情報の収集後できる限り即時に、収集した情報に含まれ得る要配慮個人情報をできる限り減少させるための措置を講ずること。

③上記①及び②の措置を講じてもなお収集した情報に要配慮個人情報が含まれていることが発覚した場合には、できる限り即時に、かつ、学習用データセットに加工する前に、当該要配慮個人情報を削除する又は特定の個人を識別できないようにするための措置を講ずること。

④ 本人又は個人情報保護委員会等が、特定のサイト又は第三者から要配慮個人情報を収集しないよう要請又は指示した場合には、拒否する正当な理由がない限り、当該要請又は指示に従うこと。

（2）**利用者が機械学習に利用されないことを選択してプロンプトに入力した要配慮個人情報について、正当な理由がない限り、取り扱わないこと**。

2 利用目的の通知等

利用者及び利用者以外の者を本人とする**個人情報の利用目的について、日本語を用いて、利用者及び利用者以外の個人の双方に対して通知し又は公表すること**

プライバシーポリシー（利用目的等）にどのようなことを盛り込むか？
～個人情報保護法の要請への＋αは？

- AI利用者が留意すべき個人情報保護法上の規制
  - ✓ 利用目的規制
    - 個人情報を取り扱うにあたっては利用目的を特定し、取得に際して本人に対して通知・公表・明示しなければならない（法17条、21条）。
    - 利用目的の変更は合理的関連性の範囲内のみ可（法17条）。
    - 利用目的外の個人情報の利用には本人同意を要する（法18条）。

  - ✓ 提供規制
    - 個人データの提供には原則として本人の同意を要する（法27条）。
    - 個人データの国内処理委託に本人同意は不要であるが、委託先の監督等を要する（法25条）。
    - 外国（EU・英国以外）にある第三者への個人データの提供にあたっては、それが委託目的であっても、一定の情報提供と本人の同意を要する（法28条）。
    - 外国第三者への個人データの提供であって、当該第三者が一定の個人情報保護体制を整備している場合には、国内処理委託同様、本人同意は不要であるが、委託先の監督等を要する（法25条）。

プライバシーポリシー（利用目的等）にどのようなことを盛り込むか？
～個人情報保護法の要請への＋αは？

- AI利用者が留意すべき個人情報保護法上の規制
  - ✓ 利用目的規制
    - ➢ 個人情報を取り扱うにあたっては利用目的を特定し、取得に際して[redacted]示しなければならない（法17条、21条）。
    - [redacted]連性の範囲内のみ可（法17条）。
    - [redacted]用には本人同意を要する（法18条）。

プライバシーポリシーへの追記については、主に利用目的規制との関係が問題となる。

  - ✓ 提供規制
    - ➢ 個人データの提供には原則として本人の同意を要する（法27条）。
    - ➢ 個人データの国内処理委託に本人同意は不要であるが、委託先の監督等を要する（法25条）。
    - ➢ 外国（EU・英国以外）にある第三者への個人データの提供にあたっては、それが委託目的であっても、一定の情報提供と本人の同意を要する（法28条）。
    - ➢ 外国第三者への個人データの提供であって、当該第三者が一定の個人情報保護体制を整備している場合には、国内処理委託同様、本人同意は不要であるが、委託先の監督等を要する（法25条）。

プロンプト入力と利用目的規制

- 利用目的を達成するために必要な範囲内であれば、生成AIサービスに個人情報を含むプロンプト（質問・作業指示）を入力することは、利用目的規制との関係においては、問題ないと考えられる 。

> **○生成 AI サービスの利用に関する注意喚起等（令和5年6月2日個人情報保護委員会）（1）①**
> 『個人情報取扱事業者が**生成 AI サービスに個人情報を含むプロンプトを入力する場合**には、特定された当該個人情報の**利用目的を達成するために必要な範囲内であることを十分に確認すること**。』

- もっとも、プロンプト入力に伴い個人データが生成AIサービスを提供する事業者（「AI事業者」）に送信される場合には、「提供規制」との関係に留意を要する。

- 個人情報を仮名化して行うプロンプト入力
  - ✓ 安全管理措置の観点から望ましい対応であるとはいえる。
  - ✓ ただし、仮名化したとしても、容易照合性の観点から、「個人情報」該当性を否定することは容易ではない。
    - ➢ 仮名化したとしても利用目的規制を免れないことを前提とすべき。

プロファイリングと利用目的規制

本人から得た情報から、本人に関する行動・関心等の情報を分析する場合、個人情報取扱事業者は、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。（通則編ガイドライン3-1-1（※1）

【本人から得た情報から、行動・関心等の情報を分析する場合に具体的に利用目的を特定している事例】
事例1）「取得した閲覧履歴や購買履歴等の情報を分析して、趣味・嗜好に応じた新商品・サービスに関する広告のために利用いたします。」
事例2）「取得した行動履歴等の情報を分析し、信用スコアを算出した上で、当該スコアを第三者へ提供いたします。」

⇒AIシステム・サービスの利用に伴いプロファイリングやスコアリングを行う場合には、上記のガイドラインが当てはまる。

プライバシーポリシー（利用目的）への追記案

0. 前提

- ✓ プライバシーポリシーへの追記案は、あくまで利用目的規制を念頭に整理しているものであり、提供規制については別途検討する必要がある点に留意。

1. 個人情報をプロンプト入力する場合

「当社は、前各号に定める利用目的（既存の利用目的）の達成に必要な範囲で、個人情報を、AIシステム・サービスを用いて、分析・検討に利用いたします。」

- ✓ 既存の利用目的の達成に必要な範囲内である限りにおいて、利用目的の追記は、本来的には不要であると考えられる。もっとも、利用目的の特定性については、令和3年頃の「プロファイリング」や「スコアリング」に関する議論と同様、より本人目線で分かりやすくすることが望ましいと考えられる。
- ✓ 特にAIシステム・サービスの利用については、本人が事前に予測することは困難であると考えられることから、上記のとおり簡単に追記することが考えられる。

2. AIを用いてプロファイリング・スコアリングを行う場合

「当社は、取得した閲覧履歴や購買履歴等の情報〔情報項目〕を、AIシステム・サービスを用いて分析の上、趣味・嗜好に応じた新商品・サービスに関する広告のために利用いたします。」

- ✓ プロファイリング・スコアリング目的の追記は、法律上の要請であるから、これらの目的でAIを用いる場合には、利用目的に明記しなければならない。
- ✓ ただし、上記同様、AIを利用していることや、分析アルゴリズムの公表までが求められているわけではないため、AIを利用している旨の開示は任意である。

プライバシーポリシー（利用目的）への追記案

３．個人情報を機械学習目的に利用する場合

「当社は、取得した個人情報を、〔特定の個人を識別することのできない方法により、〕AIシステム・サービスの機械学習のために利用いたします。」

- ✓ 機械学習目的については、利用目的としての特定は不要であるという説もあるが、必要説も（の方が？）有力であり、保守的対応としては追記すべき。
- ✓ 本人同意なく追記するかことができるか否かについては、これもまた難しい議論を要するが、概ね、以下のようなイメージで良いと考える。
  - A）機械学習が既存の利用目的の達成に必要な範囲で行われる場合
    - ➢ 機械学習目的の追記は、単に本人が一般的かつ合理的に予測・想定できる程度に利用目的を特定し直すものにすぎないとして、利用目的の変更にすら該当しない場合もある。本人同意不要。
  - B）既存のプライバシーポリシーに「データ分析」ないしこれに類する利用目的が掲げられている場合
    - ➢ 機械学習目的とこれらの目的との間に合理的関連性が認められ、利用目的の変更（法17条２項）及び変更後の利用目的の通知又は公表（法21条３項）により対応可能となる場合が多い。
  - C）既存の利用目的と機械学習目的との間に合理的関連性を見出しがたい場合
    - ➢ 事後的にプライバシーポリシーに機械学習目的を記載しても、本人同意なき目的外利用に該当するリスク有あり。
    - ➢ 本人の同意を得ることが現実的でない場合には、利用目的の変更に当たり合理的関連性が要求されない仮名加工情報制度の利用が考えられる（法41条９項参照）。

【参考】AIシステム・サービスの利用と「クラウド例外」

- クラウドサービス提供事業者に対して個人データを送信する場合であっても、当該事業者が当該個人データを取り扱わないこととなっている場合には、個人データを「提供」したことにはならないため、そもそも提供規制に服することもない（いわゆる「クラウド例外」。Q&A7-53）。
- 個人情報保護員会による令和5年6月2日付「生成AIサービスの利用に関する注意喚起等」（1）②は、以下の注意喚起を公表している。

> 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。

- この注意喚起につき、AI事業者がプロンプト入力された個人データを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ことがなく、機械学習に利用しないことが担保されていれば、プロンプト入力に伴う個人データの送信は「提供」に該当せず、提供規制との関係で問題が生じないとしているように読める旨指摘する見解もある 。
- もっとも、上記個人情報保護員会の見解も「プロンプトに対する応答結果の出力」を含めて個人データの「取り扱い」に該当することを前提としているようにも読めることから、AI事業者が個人データを「取り扱わないこととなっている」とは直ちに評価し得るものではなく、今後の議論の進展が待たれる。
- したがって、個人情報保護委員会の公式見解のない現時点においては、**AI事業者が個人データを機械学習目的に利用しないことの確認をもって、プロンプト入力を通じた個人データの送信が「提供」に該当しないと整理することについては慎重な対応が必要**となると考えられる。

【参考】クラウドサービス提供事業者が個人情報保護法上の個人情報取扱事業者に該当する場合の留意点について
（注意喚起）（令和6年3月25日・個人情報保護委員会）

1 クラウドサービスを利用して個人データを取り扱う場合の留意点

今回の事例において、**クラウドサービス提供事業者が個人情報取扱事業者に該当すると判断された考慮要素は以下のとおり**ですので御留意ください(なお、以下における「クラウドサービス利用者」とは、冒頭に記載したとおり個人情報取扱事業者です。)。

○ 利用規約において、**クラウドサービス提供事業者が保守、運用上等必要であると判断した場合、データ等について、監視、分析、調査等必要な行為を行うことができること**及び**システム上のデータについて、一定の場合を除き、許可なく使用し、又は第三者に開示してはならないこと等が規定**され、**クラウドサービス提供事業者が、特定の場合にクラウドサービス利用者の個人データを使用等できる**こととなっていたこと。

○ クラウドサービス提供事業者が**保守用ID を保有し、クラウドサービス利用者の個人データにアクセス可能な状態**であり、**取扱いを防止するための技術的なアクセス制御等の措置が講じられていなかったこと。**

○ **クラウドサービス利用者と確認書を取り交わした上で、実際にクラウドサービス利用者の個人データを取り扱っていたこと。**

2 クラウドサービス利用者による、委託先（クラウドサービス提供事業者）の監督に関する留意点

個人情報取扱事業者が、**クラウドサービス提供事業者に個人データの取扱いを委託する場合**には、以下のような点について御留意ください。

- サービスの機能やサポート体制のみならず、サービスに付随するセキュリティ対策についても十分理解し、確認した上で、クラウドサービス提供事業者及びサービスを選択してください。
- 個人データの取扱いに関する、必要かつ適切な安全管理措置（個人データの取扱いに関する役割や責任の分担を含みます。）として合意した内容を、規約や契約等でできるだけ客観的に明確化してください（ガイドラインQ＆A5－8参照）。
- 利用しているサービスに関し、セキュリティ対策を含めた安全管理措置の状況について、例えば、**クラウドサービス提供事業者から定期的に報告を受ける等の方法**により、確認してください。

3 個人データの取扱いの委託先がクラウドサービスを利用している場合の留意点

- 例えば、従業者等の個人データを取り扱う個人情報取扱事業者が、個人データの取扱いを外部の事業者に委託している場合に、当該委託先事業者が、クラウドサービス提供事業者が提供するアプリケーションを利用して、委託された個人データを取り扱っているケースがあります。この場合、**委託元である個人情報取扱事業者は、委託先事業者に対する監督の一内容として、当該クラウドサービスの安全性などを委託先事業者に確認する**ことが考えられます。
- ガイドラインでも、「委託元が委託先について『必要かつ適切な監督』を行っていない場合で、委託先が再委託をした際に、再委託先が不適切な取扱いを行ったときは、元の委託元による法違反と判断され得るので、再委託をする場合は注意を要する」ものとされています（ガイドライン3－4－4）。
- 委託元である個人情報取扱事業者においては、前記1のとおり、委託先事業者のクラウドサービスの利用によって、**当該委託先事業者からクラウドサービス提供事業者に対する「再委託」となっている場合がある**ことを念頭において、法**第23 条が求める個人データの安全管理のために必要かつ適切な措置及び法第25 条が求める委託先に対する必要かつ適切な監督**を行うよう留意してください。

【参考】AIシステム・サービスの利用と「委託」

【委託構成】

- 「生成AIサービスの利用に関する注意喚起等」（1）②（前頁参照）は、一定範囲で、本人の同意なく生成AIサービスに個人データを含むプロンプトを入力することを許容しているように読める。
- 個人情報保護員会はその論理構成を明示していないが、「クラウド例外」を除き、あり得る構成としては「委託」構成がある。仮に「委託」構成に依拠する場合、国内の委託先AI事業者への個人データの提供にあたり、委託先AI事業者は「第三者」とはみなされず、本人の同意は不要であると整理することができる（法27条5項1号参照）。

【委託構成の難点】

- 外国（EEA加盟国及び英国を除く 。）の委託先AI事業者への個人データの提供については、直ちに「委託」構成に依拠することはできず、原則として、当該外国の委託先となるAI事業者がいわゆる基準適合体制整備者（法28条1項括弧書参照）でなければならない 。
- 「委託」構成に依拠する場合、委託先の監督義務が課されることとなる（法25条）。もっとも、とりわけ外国のAI事業者については、委託元の一つに過ぎない日本の事業者が、委託先として基準適合体制の整備及び監督に服することを求めることは現実的であるとはいえない。

【目下の暫定的整理】

- 外国のAI事業者がプライバシー保護体制を構築するにあたり、わざわざ日本の個人情報保護法に準拠した体制を整備している先はほとんど見られないものの、EUのGDPRに準拠して体制整備している先は散見される。
- 特に、GDPR準拠のDPA（データ処理契約）を締結する選択肢を用意しているAI事業者との関係においては、基本的には、日本法の下でも基準適合体制整備者としての要件を充足するのではないかと考えられる。
  - DPAが引き続きGDPRに準拠していることを年に1回程度確認することで、ひとまずは基準適合体制整備者に対する「委託」と整理することも不合理ではないと考える。

【参考】AI開発者・提供者が個人データを独自利用する場合

AI開発者orAI提供者が、AI利用者がプロンプトに入力した個人データを、機械学習目的をはじめとする応答結果の出力以外の目的に利用することが予定されている場合には、「クラウド例外」や「委託」構成に依拠することはできず、プロンプト入力に伴うAI事業者に対する個人データの提供は第三者提供（法27条1項柱書）又は外国第三者提供（法28条1項）となる。

- ✓ 国内事業者が提供先であれば、本人の同意を得る必要がある。
- ✓ 外国の事業者が提供先であれば、必要な情報提供に加えて、本人の同意を得る必要がある。

① 当該外国における個人情報保護制度の有無
② 当該外国の個人情報保護制度の指標となり得る情報
③ OECD8原則に対応する事業者の義務・本人の権利の不存在
④ その他本人の権利利益に重大な影響を及ぼし得る制度の存在

【参考】個人情報保護法 いわゆる3年ごと見直しに係る検討の中間整理
（個人情報保護委員会　令和6年6月27日）

『**生成 AI** などの、社会の基盤となり得る技術やサービスのように、社会にとって有益であり、公益性が高いと考えられる技術やサービスについて、**既存の例外規定では対応が困難と考えられるものがある。**これらの技術やサービスについては、社会的なニーズの高まりや、公益性の程度を踏まえて、例外規定を設けるための検討が必要である。この際、「いかなる技術・サービスに高い公益性が認められるか」について、極めて多様な価値判断を踏まえた上で高度な意思決定が必要になる。個人の権利利益の保護とデータ利活用の双方の観点から多様な価値判断が想定されるものであり、関係府省庁も含めた検討や意思決定が必要と考えられる。』

⇒個人情報保護委員会も個人情報保護法の例外規定では生成AIの利活用にハードルがあることを認めている。

個情委の有識者ヒアリングにおいては、有識者から「個人情報をAIが一般的な知識の一環として利活用すること」が個情法に例外規定として設けることが提言された 。ただし、例外規定を設ける場合には、一定の要件が必要であり、情報源とアーキテクチャが重要であり、インターネット上に公開されているデータの扱い方、たとえば、ニューラルネットワークにおいて、不適切なプロファイリングといった利用は禁止されるべきであるし、出力に関しても不適正な利用は問題となるとされている。➡どのような例外規定が設けられるかは現状不明

５．AI社内規程（AI利用者向け）のポイント

1．前文・業務に利用可能なAI

AI利用ガイドライン（仮称・利用者向け社内規程用）

本規程は、当社従業員が、当社の業務でAIを利用する際に注意すべき事項を定めたものです。

AIは、業務効率化などに役立つ反面、入力するデータの内容や出力結果の利用方法によっては法令に違反したり、他者の権利を侵害したりする可能性があります。本規程をよく読んでいただいた上で、AIを利用してください。

第１　業務に利用可能なAI

本ガイドラインが対象とするAIは●●とします。それ以外のAIの利用を希望する場合には●●部門にお問い合わせください。

2. AIの利活用に関する留意点

1. 安全性の観点

（1）当社では、以下の用途・業務でのAIの利活用を禁止します。

【ア　・・・】

（2）AIの利活用にあたっては、AI提供者が定めた利用上の留意点及び利用規約を遵守し、AI提供者が想定していない用途では利用しないでください。

（3）AIには、正確性及び（必要に応じ）最新性が担保されたものを入力してください。特に、学習等に用いるデータについては、正確性及び（必要に応じ）最新性が担保されたものを利用してください。

（4）AIの出力結果には虚偽情報・誤情報が含まれる可能性があること、他人の権利を侵害する可能性があること等、AIの精度・リスクを理解し、出力結果を利用する場合には、その根拠や裏付けを確認するようにしてください。

2　公平性の担保

AIは、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偏見及び差別等の不適切なバイアスを含むものを出力することがあります。生成AIの利活用にあたっては、公平性が担保されたデータの入力を行うよう注意し、プロンプトに含まれるバイアスに留意して、AI出力結果の事業利用判断を行うようにしてください。

3　セキュリティ対策

AIの利活用にあたっては、生成AI提供者が定めたセキュリティ上の留意点を遵守してください。

4　透明性・アカウンタビリティの担保

（1）AIにプロンプト入力を行う場合、又は出力結果を特定の個人若しくは集団に対する評価の参考にする場合には、AIポリシー、プライバシーポリシーその他の方法により公表された用途又は関連するステークホルダーに通知された用途の範囲内での利用か事前に確認してください。公表又は通知された用途の範囲外である場合には、関連するステークホルダーに対し、事前に情報提供を行ってください。

（2）AIポリシーその他の方法により公表された用途又は関連するステークホルダーに通知された用途の範囲外で出力結果を事業判断に活用した場合、その結果を関連するステークホルダーに合理的な範囲内で情報提供してください。

（3）AIにより出力された文章・画像等を対外的にそのまま使用する場合には、AIにより作成されたものであることを明記してください。

（4）AIの利活用に関し、関連するステークホルダーからの問い合わせを受けた場合には、速やかに●●部門にご報告ください。

３．AI利活用に関する法令・契約の遵守①

１．著作権

- 自らの著作物と認められないAI生成物の、外部への配信・アップロード・販売等の著作物の享受を目的とした利用については、AI生成物が学習元の著作物との類似性・依拠性が認められると、著作権侵害に該当する場合があります。著作権侵害の類似性・依拠性の有無を判断することは困難な場合もあるので、AIのプロンプトに既存の著作物、作家名、作品名等を入力しないようにしてください。
- また、AI生成物を利用する場合には、そのAI生成物が既存の著作物に類似しないか調査してください。
- 入力に伴って生じる著作物の複製は、入力された著作物を情報解析して生成AIに対する生成の指示（プロンプト）とするためのものであり、「非享受」目的として、著作権法違反にならない場合が多いですが、「入力した既存の著作物と類似する生成物を生成させる」といった目的で入力を行う場合は、「享受」目的が併存している場合に当たり、著作権法違反になる可能性がありますので留意してください。
- なお、AI生成物の利用（インターネットでの配信、複製物の譲渡等）については、著作権法違反となる場合が多いと考えられますので、留意してください。
- 著作権法違反にならないか不安がある場合は、事前に【法務部】にご相談ください。

３．AI利活用に関する法令・契約の遵守②

２　商標権・意匠権

AI生成物を商標・意匠として利用する場合、他者の登録商標・意匠と同一又は類似の商標・意匠を利用する行為は、商標権侵害や意匠権侵害に該当する可能性があります。
AI生成物を商標・意匠として利用する場合は、そのAI生成物が既存の商標・意匠と同一か又は類似していないか調査してください。

３　肖像権・パブリシティ権

AIを利用して生成された著名人の肖像、音声等を利用する場合には、肖像権・パブリシティ権の侵害や名誉毀損等の人格権侵害に該当する可能性がありますので、AIにプロンプト入力を行う場合には、著名人の顔写真、氏名、音声を入力しないようにしてください。

４　個人情報

AIに個人情報をプロンプト入力する行為は、違法な個人データの第三者提供に該当する可能性がありますので、個人情報を入力しないでください。氏名、生年月日などの特定の個人が識別できる情報を削除しても、他の情報と照合して容易に特定の個人を識別出来る場合には個人情報に該当しますので、そのような情報の入力もしないでください。

５　名誉毀損等

出力結果に個人や法人に関する虚偽情報・誤情報が含まれる場合、そのような情報の利用は、名誉毀損・信用毀損に該当する可能性がありますので、行わないでください。

４．秘密保持義務・出力結果の商用利用

６　秘密保持義務・守秘義務

（１）他者の秘密情報

AIに他社との間で秘密保持契約などを締結して取得した秘密情報を入力する行為は、第三者であるAI提供者に秘密情報を開示することになるため、秘密保持契約に違反する可能性がありますので、他社の秘密情報は入力しないでください。

（２）当社の機密情報

AIに当社の機密情報は入力しないでください。当社の機密情報の入力を希望する場合には、事前に●●部門にお問合せください。

７　出力結果の商用利用

　生成AIの生成物等の出力結果を商用利用する場合、AI提供事業者の利用規約において商用利用が認められていることを事前に確認してください。

６．AI利用契約・利用規約のポイント

1．1　AIからのアプローチ：AIの目的外利用の禁止、その他検証

〇AI提供者
- AI 開発者が設定したAI の想定利用環境とAI システム・サービスの利用者の利用環境に違い等がないかを検討する（「2）安全性」）（113頁）
- 適切な目的でAI システム・サービスが利用されているかを定期的に検証する（113頁）

〇AI利用者
- AI 提供者が定めた利用上の留意点を遵守して、AI 提供者が設計において想定した範囲内でAI システム・サービスを利用する（「2）安全性」）（139頁）

- AIは汎用性が高いツールであるところ、AI開発者やAI提供者が予想していなかった機能を有していたり、利用法が発見されたりすることが想定される。AI事業者ガイドラインにおいても、利用者に対しては「AI 提供者が定めた利用上の留意点を遵守して、AI 提供者が設計において想定した範囲内でAI システム・サービスを利用する」と提言がなされている。
  ➡AIの利用目的を具体化するとともに、AI利用者としては、AI提供者の利用規約をよく読み、当該利用目的の範囲内で利用することが求められる。
- AI提供者においては、「適切な目的でAI システム・サービスが利用されているかを定期的に検証する」ことが求められており、AI利用者としては、定期的な検証に協力することも考えられる。

1．2　AIからのアプローチ：
利用者による人の生命、身体、財産を害するおそれがある場合の報告（努力）義務

○AI提供者 • AI 開発者も気づいていないようなリスクの存在を認識した場合に、速やかなAI 開発者への通知及び対応策の相談・検討（112頁）
○AI利用者 • AI 利用者は、AI の出力結果について疑義がある場合には、必要に応じて、AI 提供者（又はAI 提供者を通じてAI 開発者）に問い合わせを行うことが期待される。（141頁）

- AI開発者においては、開発時に予想しなかったリスクの存在をAI提供者・AI利用者が認識した場合には、速やかに通知・対策策を求める旨の規定を開発契約に入れることが考えられる（AI利用者が認識したものはAI提供者を通じて報告を受ける）。

- AI利用規約において、AI利用者（業務外利用者を含む）がAIの出力結果に疑義がある場合には、AI提供者（又はAI 提供者を通じてAI 開発者）に問い合わせを行う旨の規定を置く。

1．3　AIからのアプローチ：インシデントが発生した場合の通知義務

AI利用者
〇適正な範囲・方法での利用
　AI 提供者（又はAI 提供者を通じてAI 開発者）に対するインシデント情報のフィードバック（何らかインシデントが発生した場合、インシデントが起こる予兆があった場合を含む）（140頁）

- AI事業者ガイドラインにおいて、AI利用者は、「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」が求められており、「AIの出力結果について疑義がある場合には、必要に応じて、AI 提供者（又はAI 提供者を通じてAI 開発者）に問い合わせを行うことが期待され」ている。
- また、AI提供者は、AIの適正な範囲・方法での利用の観点から、「AI 提供者（又はAI 提供者を通じてAI 開発者）に対するインシデント情報のフィードバック（何らかインシデントが発生した場合、インシデントが起こる予兆があった場合を含む）」も期待されている。
- そこで、AI利用者は、AIを利用している際に上記のような事態が発生した場合、その旨の問い合わせ・情報のフィードバックをすることも考えられる。

1．4　AIからのアプローチ：アップデート条項

○AI提供者
- 個人のプライバシーを侵害する情報の消去の依頼、AI のアルゴリズムの更新等（118頁）
  - AI 利用者等関連するステークホルダー又は個人のプライバシーを侵害する情報を拡散した場合
  - AI 利用者等関連するステークホルダー又は個人のプライバシーを侵害する情報を取得した場合

○AI利用者
- 活用の過程を通じて、AI の機能を向上させ、リスクを抑制するために実施するAI システムのアップデート、AI の点検・修理等（140頁）

- AIは、その性質や利用の態様等によって、人の生命、身体、財産を害する可能性がある。AI提供者において、「AI 利用者等関連するステークホルダー又は個人のプライバシーを侵害する情報を拡散した場合」に、「個人のプライバシーを侵害する情報の消去の依頼、AI のアルゴリズムの更新等」が求められたり、AI利用者においても「活用の過程を通じて、AI の機能を向上させ、リスクを抑制するために実施するAIシステムのアップデート、AI の点検・修理等」が求められている。
- AIを導入するにあたり、AI提供者による点検やアップデートが必要と考えられることから、その旨定めた条項を導入することが考えられる。

１．５　AIからのアプローチ：ネットワーク遮断条項

〇AI提供者
- AI がアクチュエータ等を通じて人の生命・身体・財産に危害を及ぼした場合に講ずるべき措置について、あらかじめ整理しておくことが期待される。（111頁）
- （インシデント対策の整理及び発生時の措置の初期対応について）AI システムの停止（キルスイッチ）、AI システムのネットワークからの遮断（133頁）

- AI がアクチュエータ等を通じて人の生命・身体・財産に危害を及ぼす場合ことも考えられる。
- そのような場合の初期対応として、例えば「AI システムの停止（キルスイッチ）」や「AI システムのネットワークからの遮断」が考えられ、「AI提供者の利用規約」や「AI提供者とAI利用者との契約」において、AI利用者からそのような措置を求めることができるような条項を導入することが考えられる。

2．1　データからのアプローチ：（個人）データの目的外利用の禁止

〇AI提供者
- AI 開発者が設定した範囲でAI を活用する（「2）安全性」）（113頁）
- 安全確認等の事前及び動作時の人間関与、並びに事後における再発防止策の検討（112頁）
- AI モデルの入出力及び判断根拠を定期的に評価し、バイアスの発生をモニタリングする（114頁）
- AI システム・サービスにおけるプライバシー侵害に関して適宜情報収集し、侵害を認識した場合等は適切に対処するとともに、再発の防止を検討する（123頁）

- AIに個人情報を含む様々なデータを入力することが想定されるところ、AIは汎用性が高いツールである以上、利用者側で想定した目的以外の目的で利用されることが懸念される。
- そこで、AIに入力するAI提供者との間でデータの具体的な利用目的を特定した上で、それ以外の利用を禁止することが考えられる。
- AI提供者（開発者）側で独自利用（例えば、AI学習のための利用）ができるかどうか、要確認。
- この点に関し、AI提供者の立場からすれば、「AI システム・サービスにおけるプライバシー侵害に関して適宜情報収集し、侵害を認識した場合等は適切に対処するとともに、再発の防止を検討する」ことが求められていることから、（個人データの）利用目的の特定の際には、AI開発や検証も利用目的に加えておくなど、広く定めておくことが考えられる。
- AI利用者としては、入力したデータをどの範囲で利用できるかよく確認し、必要に応じてAI提供者と相談する必要がある。

２．２　情報の漏えい、プライバシー侵害が発生した場合の報告義務

〇AI利用者
- 個人のプライバシーを侵害した場合の措置について、AI 提供者から情報提供（AI 開発者からのものを含む）があった場合には、留意の上措置を検討する（143頁）

- AI利用者において、「個人のプライバシーを侵害した場合…、AI 提供者から情報提供（AI 開発者からのものを含む）があった場合には、留意の上措置を検討する」ことが求められている。そこで、AI提供者のほうで、情報の漏えいやプライバシー侵害等が発生した場合に、報告義務を定めることが考えられる。
- なお、「侵害」としては、「過失」による「（個人データ）の漏えい・滅失・毀損」のほか、本人の同意を得ない「意図的・故意」による「目的外利用」や「（個人データ）の第三者提供」なども該当すると考えられる。
- 「いわゆる3年ごと見直し」の中間整理においては、現行法では個情委への報告・本人通知の対象となっていない、「意図的・故意」による「個人データの第三者提供」についても個情委への報告・本人通知の対象とすることが検討されている。

2．3　不要な情報の入力禁止

○AI提供者 • データの代表性を満たすために個人情報を含む大量のデータを集めようとする場合に、個人情報のマスキング、削除等プライバシーに配慮して扱う（114頁）
○AI利用者 • データの代表性を満たすために個人情報を含む大量のデータを集めようとする場合に、個人情報のマスキング、削除等プライバシーに配慮して扱う（141頁） • 例えば、生成 AI サービスの利用にあたって、入力する個人データが生成 AI サービスの提供者においてAI の学習データとして利用されることが予定されている場合には、同意を得られていない個人データを含むプロンプトを入力しないよう留意する（144頁）

- 「生成 AI サービスの利用にあたって、入力する個人データが生成 AI サービスの提供者においてAI の学習データとして利用されることが予定されている場合には、同意を得られていない個人データを含むプロンプトを入力しないよう留意する」ことが求められている。
- また、AI利用者が個人情報（個人データ）を入力する場合、利用目的に照らし、本人からの同意を取得する等、AI提供者より適法な個人情報（個人データ）の提供を求められると考えられる。
- そこで、「AI提供者の利用規約」や「AI提供者とAI利用者との契約」で、AI利用者としては、AIに入力して良い情報とそうでない情報を区別するとともに、適法な手続を得た情報のみをAIに入力する旨を規定することが考えられる。