AI開発・活用に関する法規制の全体像

AIデータ活用シンポジウム 2026

生成AIで揺らぐ知財とセキュリティ

～ 揺らぐ知的財産と変貌する脅威 ～

自己紹介

榊原　颯子 Sakakibara Soko

TMI総合法律事務所　弁護士

- 16年九州大学法学部卒業、18年中央大学法科大学院修了、20年弁護士登録
- データ利活用における個人情報保護法・各国データ保護法対応、情報セキュリティインシデント対応を中心としたデータ・プライバシー領域、M＆A、ベンチャー企業支援などのコーポレート・ガバナンス領域、システム/アプリ開発を中心としたIT法務・紛争を主に取扱う。
- 近時の著書に『Cookieポリシー作成のポイント』（共著、中央経済社、2024年）、『データ利活用のビジネスと法務』（共著、中央経済社、2024年）、『個人情報管理ハンドブック〔第5版〕』（共著、商事法務、2023年）など。

AIに関わるリスクと法問題

✓AI事業者ガイドラインで整理されているAIによるリスク

大分類	中分類	リスク例
技術的リスク (＝主にAIシステム特有のもの)	学習及び入力段階のリスク	データ汚染攻撃等のAIシステムへの攻撃
	出力段階のリスク	バイアスのある出力、一貫性のない出力等
		ハルシネーション等による誤った出力
	事後対応段階のリスク	ブラックボックス化、判断に関する説明の不足
社会的リスク (＝既存のリスクがAIにおいても発生又はAIによって増幅するもの)	倫理・法に関するリスク	個人情報の不適切な取扱い等
		生命等に関わる事故の発生
		差別的出力
		過度な依存
		悪用
	経済活動に関するリスク	知的財産権等の侵害
		金銭的損失
		機密情報の流出
		労働者の失業
		データや利益の集中
		資格等の侵害
	情報空間に関するリスク	偽・誤情報等の流通・拡散
		民主主義への悪影響
		フィルターバブル及びエコーチェンバー現象
		多様性・包摂性の喪失
		バイアス等の再生成
	環境に関するリスク	エネルギー使用量及び環境の負荷

出典：「AI事業者ガイドライン（第1.2版）別添（付属資料）概要」7頁

AIに関わるリスクと法問題

AI
ガバナンス

AI
倫理

- 知的財産権の侵害
- 個人情報・プライバシー権の侵害
- 肖像権/パブリシティ権/名誉権の侵害
- 違法・有害情報の拡散に関する責任
- 事故発生時の民事責任
- 情報漏えい・サイバーセキュリティへの対処と責任

AI事業者ガイドライン

AIのバリューチェーン全体で取り組むべき「共通の指針」は、以下のように整理される。

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利用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 ✓ AIシステム・サービスの特性及び用途を踏まえ、学習等に用いるデータの正確性等を検討するとともに、**データの透明性の支援、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する
3) 公平性	✓ 特定の個人ないし集団へのその人種、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**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適切な情報を提供**する（AIを利用しているという事実、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、提供先における適切/不適切な利用方法、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

（出典）「AI事業者ガイドライン（第1.2版）概要」15~16頁を元に作成

AI倫理の観点で問題となった事案

➢ **【公平性・差別の問題】：人事採用AIの事例**

エンジニアを採用するためのAIシステムを開発。過去10年間分の履歴書パターンを学習、5万個のキーワードを抽出・分析して、採用にふさわしいか否かをランク付け。過去のエンジニア職の応募がほぼ男性であったため、「女性」に関する単語が応募者の履歴書に記載されているとランクが下がる評価付に。

➢ **【プライバシーの問題】：顔画像の収集の事例**

米国企業がSNS等のインターネット上から顔画像を本人の同意を取得せずに収集し、顔画像認識AIを開発。収集した枚数は100億枚以上。米国ではプライバシー侵害であるとして訴訟提起、カナダ当局からの調査によりカナダでは事業撤退に至った。

➢ **【透明性・説明責任の問題】：人事評価の事例**

AIを使用した人事評価ツールを導入し、スキルやパフォーマンス等を評価。労働組合が当該企業に対して団体交渉を通じてAIがどのように評価付をしているのか、具体的説明を求めたところ、AIはあくまで人事評価のツールに過ぎないとして情報開示を拒否。労働組合は、賃金決定の透明性を求めて、東京都労働委員会に救済を申し立てた。

日本におけるAI関連の法体系

日本においては、「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」他に、AI特有の法規制はなく、個別法において規制されている他、各種ガイドラインにおいてAIの活用に係る諸問題に対処している。

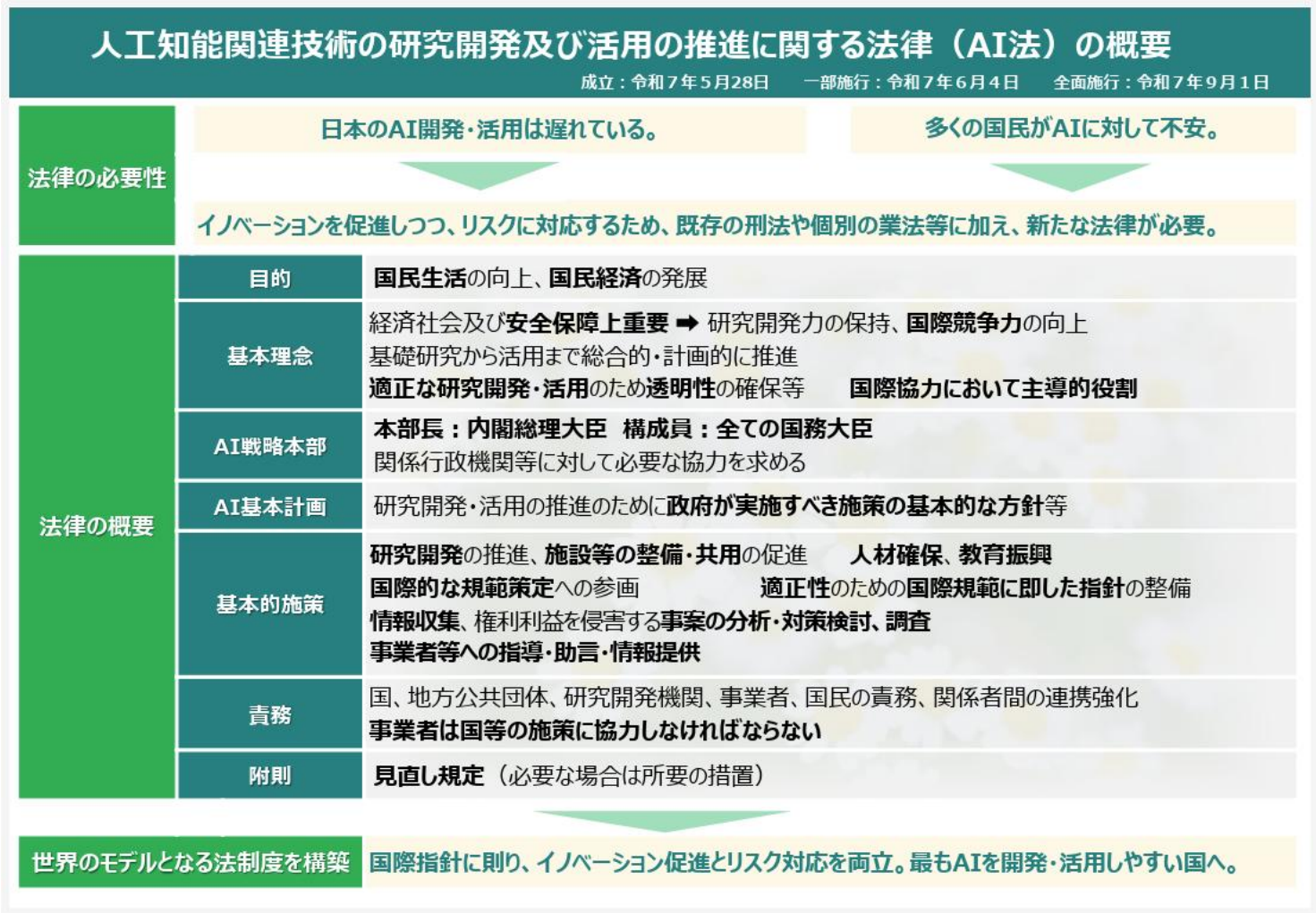
ハードロー

- **知的財産法**　著作権法/不正競争防止等
- **個人情報保護法**
- **民事責任**　民法/製造物責任法
- **労働関連法令**
- **業法規制**　金融・医療業規制/弁護士法等

ソフトロー

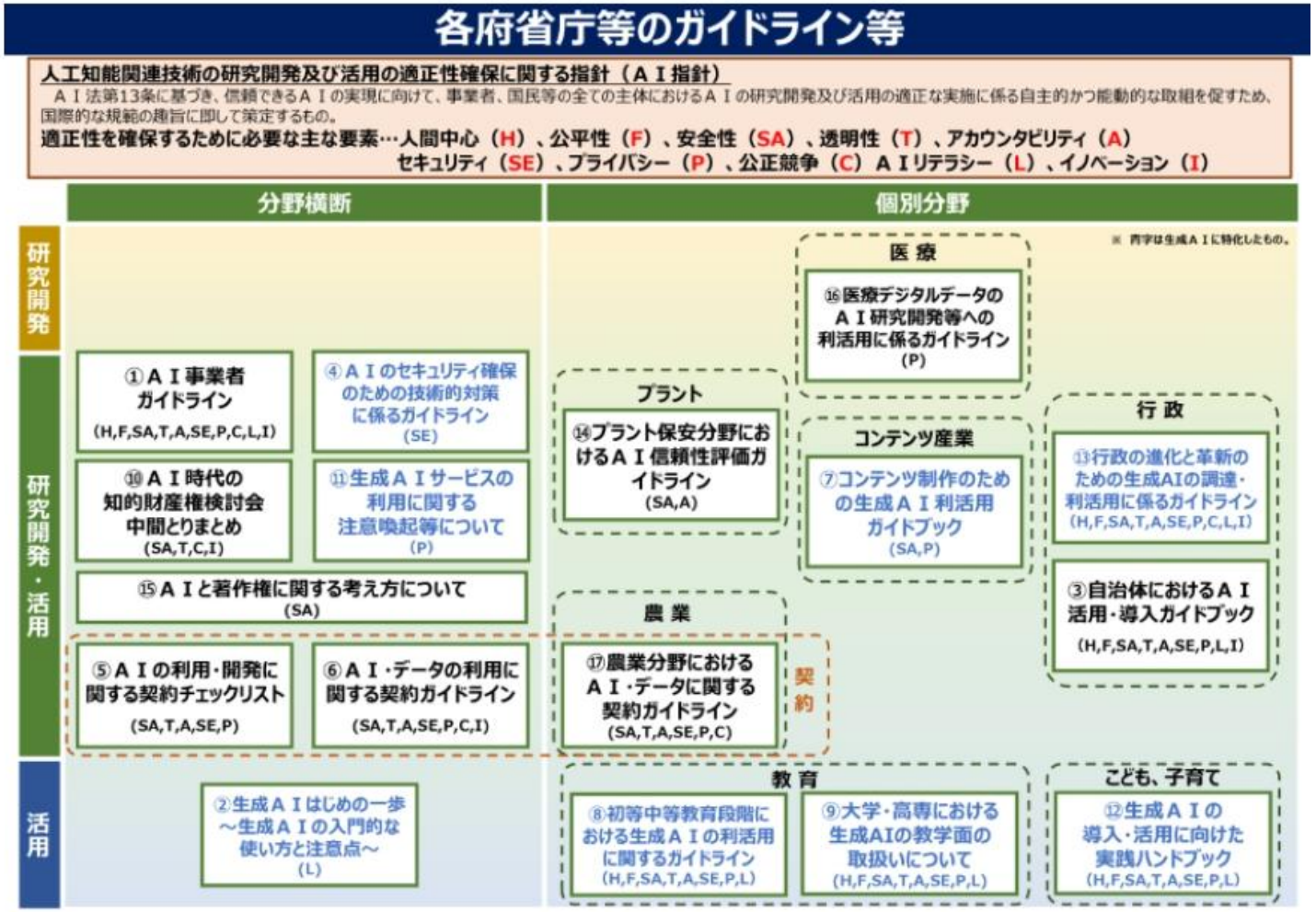
- **AI事業者ガイドライン**
- **AIのセキュリティ確保のための技術的対策に係るガイドライン**
- **生成AIの適切な利活用等に向けた知的財産の保護及び透明性に関するプリンシプル・コード**
- **AI・データの利用に関する契約ガイドライン**

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



出典：「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」

AIに関する各府省庁等のガイドライン

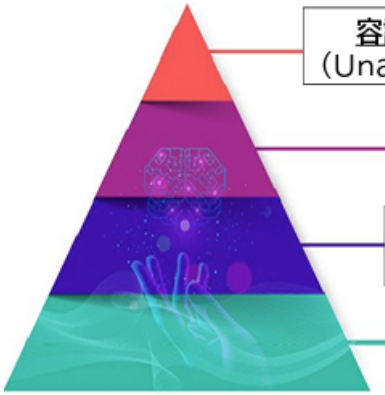


出典：「各府省庁等のガイドライン等の一覧（概要）」

EU AI Act

○ AI法では、**リスクベースアプローチを採用**し、4つのリスクレベルを設け、各々のリスクに応じた規制を規定。それに加え、汎用AIに関する規制あり。

リスクベースアプローチ



（欧州委員会HP等の資料から一部加工）

容認できないリスク (Unacceptable Risk)	➢ サブリミナル技術、ソーシャルスコアリング、職場又は教育機関での感情推測システム、公共空間における法執行目的でのリアルタイム遠隔生体認証システム　等 ➢ **原則禁止**
ハイリスク (High Risk)	➢ 機械、医療機器、生体認証、重要インフラ、教育、雇用、法執行、移民管理　等 ➢ **プロバイダー、輸入者、販売業者、導入者それぞれに対して、リスク管理、データガバナンス、技術文書の作成、人的監視措置、適合性評価手続、ログ保存など厳格な規制**
限定的なリスク (Limited Risk)	➢ 生成AI、自然人とやり取りするAI、感情認識システム　等 ➢ **AIにより生成されたコンテンツである旨のマーキングやAI使用の告知など限定的な透明性義務**
最小限のリスク (Minimal Risk)	➢ 上記以外 ➢ **自由に利用可能（自主的な行動規範の推奨あり）**

汎用AIモデル提供者に対する義務

汎用AIモデル一般	システミックリスクを有する汎用AIモデル
➢ 技術文書の作成及び更新 ➢ 汎用AIモデルをAIシステムに統合する提供者向けの情報・文書の作成、更新及び提供 ➢ 著作権法を遵守するためのポリシーの実行 ➢ 汎用AIモデルの学習に使用したコンテンツに関する十分に詳細な要約の作成及び公開 ➢ 域内代理人の指名	（左記に加えて） ➢ モデル評価の実施 ➢ EUレベルでのシステミックリスクの評価及び軽減 ➢ 深刻なインシデント及びそれに対する是正措置のAIオフィスへの報告 ➢ 適切なレベルのサイバーセキュリティ保護

6

出典：「EU AI法の概要」

知的財産権法上の問題

- AIによる著作権侵害のリスク
- 知的財産権と優越的地位の濫用

AIによる著作権侵害のリスク

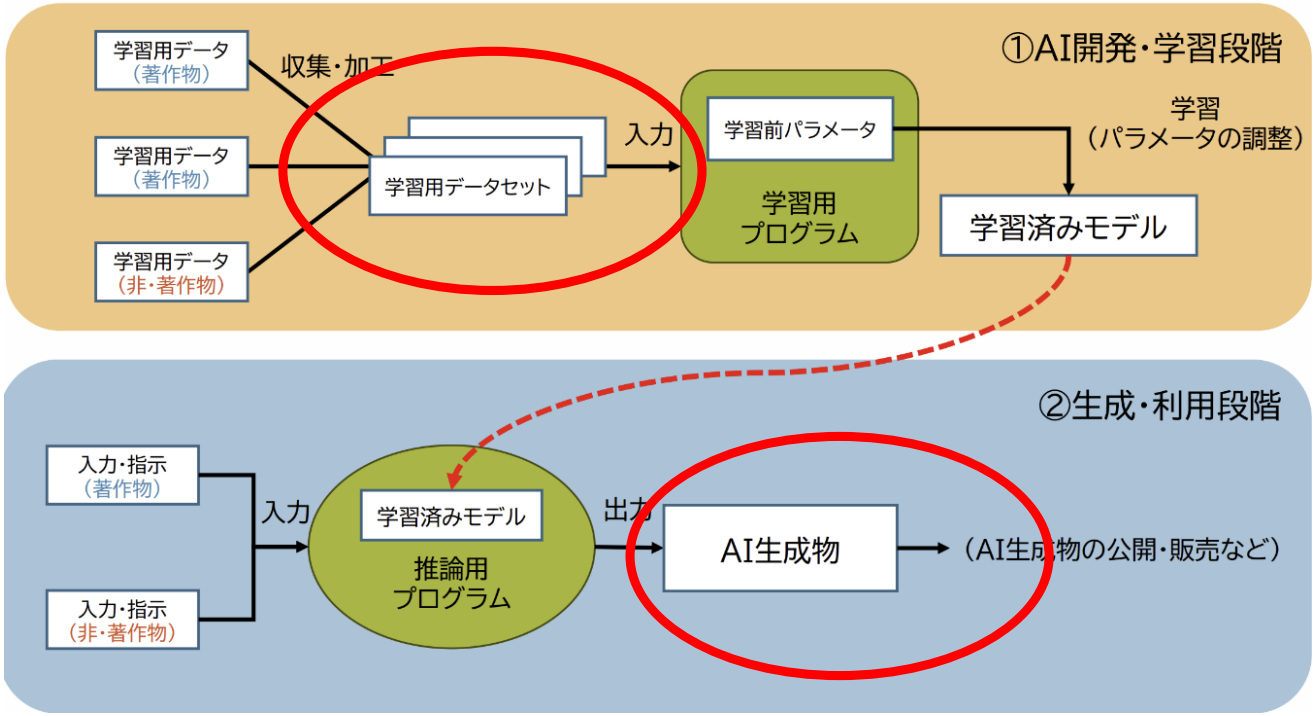
AI開発・学習段階（著作権法第30条の4※等）

※平成30年著作権法改正により新たに規定

- 著作物を学習用データとして収集・複製し、学習用データセットを作成
- データセットを学習に利用して、AI（学習済みモデル）を開発

生成・利用段階

- AIを利用して画像等を生成
- 生成した画像等をアップロードして公表、生成した画像等の複製物（イラスト集など）を販売



（出典）文化庁「AIと著作権に関する考え方について（概要）」3頁、「AIと著作権Ⅱ」セミナー資料9頁

AIによる著作権侵害のリスク

原告は、ウルトラマンシリーズの著作権者である円谷製作株式会社から中国でのライセンスを受けた代理店。被告事業者による生成画像機能のサービスで、ウルトラマンと酷似した生成AIによる作成画像が発見され、許可なく著作物をAIに学習させて実質的に類似する画像を生成しているとして、広州インターネット裁判所に提訴し、この被告事業者に侵害の差止や損害賠償責任が認められた事案。

中国で初めての生成AIサービスに特化した法令である生成型AIサービス管理暫定弁法の規定を理由に、被告はAIサービス提供者として、当該ウルトラマン著作物と実質的に類似する画像を生成しないように防止する技術措置（キーワードフィルタリング等）を採らなければならないと判示されている。

（出典）本判決で類似性が認められた生成画像の1部

AIによる著作権侵害のリスク

AI開発・学習段階（著作権法第30条の4※等）
※平成30年著作権法改正により新たに規定

- 著作物を学習用データとして収集・複製し、学習用データセットを作成
- データセットを学習に利用して、AI（学習済みモデル）を開発

非享受目的の利用行為（著作権法30条の4）
AI開発のような情報解析等において、**著作物に表現された思想又は感情の享受を目的としない利用行為は、著作権者の許諾なく行うことができる。**但し、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。

✓ AI学習のために行われる著作物の複製等のうち、以下のような場合は、既存の著作物に表現された思想又は感情を享受する目的が併存していることから、「非享受目的」の要件を満たさず、法第30条の4は適用されないと考えられる。

AI学習の場面での著作物の利用（学習データの収集等）

✓ 生成AIの基盤モデルに対する追加学習（ファインチューニング）のうち、意図的な「過学習」等、学習データである著作物の類似物（創作的表現が共通したもの）を生成させること目的としたものを行うための、学習データ（著作物）の収集

AI学習以外の場面での著作物の利用

✓ 一部の検索拡張生成（RAG）等※で用いるための、生成AIへの入力用データ（著作物）の収集

※RAG等のうち「既存の著作物の創作的表現の全部又は一部を、生成AIを用いて出力させること」を目的としたもの。

（出典）文化庁「AIと著作権に関する考え方について（概要）」7頁

AIによる著作権侵害のリスク

非享受目的の利用行為（著作権法30条の4）
AI開発のような情報解析等において、著作物に表現された思想又は感情の享受を目的としない利用行為は、著作権者の許諾なく行うことができる。但し、**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。

✓ AI学習のためのデータ収集と本ただし書との関係は、以下のように考えられる。

- インターネット上のデータ（データベースの著作物）が情報解析に活用できる形で有償提供されている場合、有償で利用することなく、当該データベースの著作物（その創作的表現が認められる一定の情報のまとまり）を情報解析目的で複製する行為は、本ただし書に該当し得る。
- 「AI学習のための著作物の複製等を防止する技術的な措置※2が講じられている」といった一定の事情※3から、「あるウェブサイト内のデータを情報解析（AI学習等）に活用できる形で整理したデータベースの著作物が、将来販売される予定がある」ということが推認できる場合がある。
- このような推認ができる場合に、上記の技術的な措置を回避して、AI学習のために当該データベースの著作物の複製等をする行為※4は、本ただし書に該当し、法第30条の4による権利制限の対象とはならないと考えられる。

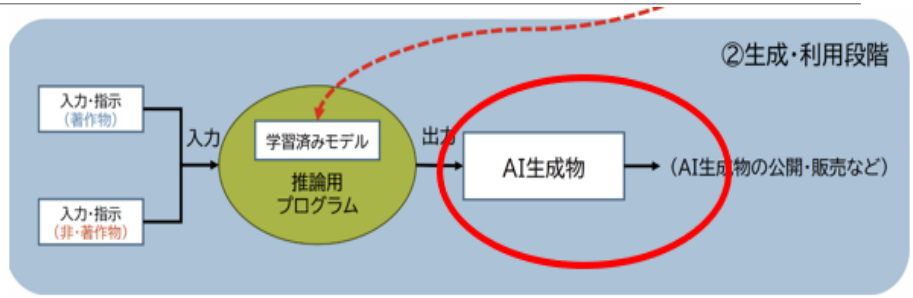
※2 ウェブサイト内のファイル”robots.txt”への記述や、ID・パスワードによる認証によって、AI学習のための複製を行うクローラによるウェブサイト内へのアクセスを制限する措置。
※3 上記の技術的な措置が講じられていることや、過去の販売実績など。
※4 複製等の方法としては「クローラにより当該ウェブサイト内に掲載されている多数のデータを収集する」ことなどが考えられます。

（出典）文化庁「AIと著作権に関する考え方について（概要）」9頁

AIによる著作権侵害のリスク

生成・利用段階

- AIを利用して画像等を生成
- 生成した画像等をアップロードして公表、生成した画像等の複製物（イラスト集など）を販売



✓ 通常の著作権侵害と同様の基準で、生成された画像等に既存の画像等（著作物）との**類似性（創作的表現が共通していること）及び依拠性(既存の著作物をもとに創作したこと)が認められ、かつ、権利制限規定の対象外である場合は、既存の著作物の著作権侵害**となる。AI生成物の依拠性については、以下のように考えられる。

既存の著作物が学習データに含まれているか不明な場合

■ 生成物と類似する既存の著作物が学習データに含まれているか不明な場合でも、権利者としては「AI利用者が既存の著作物にアクセス可能であったこと」や「生成物に既存の著作物との高度な類似性があること」等を立証すれば、依拠性ありと推認させることができる（そのため、既存の著作物が学習データに含まれているか不明でも、依拠性を立証することは可能）。

既存の著作物が学習データに含まれていることが立証できる場合

■ また、生成AIの開発・学習段階で当該既存の著作物が学習されていた場合は、AI利用者が既存の著作物を認識していない場合でも、通常、依拠性があったと推認される※。

※ ただし、当該生成AIについて「学習に用いられた著作物の創作的表現が、生成・利用段階において出力される状態となっていない」場合には、AI利用者がこの事情を主張・立証することで、依拠性がないと判断される場合はあり得ます。

（出典）文化庁「AIと著作権に関する考え方について（概要）」12頁

知的財産権と優越的地位の濫用

「知的財産権・ノウハウ・データの適切な取引のための優越的地位の濫用等に関する指針」

AI 技術の急速な進展により、データの経済的価値も一層高まっている。これらの知的財産権等の価値を適切に評価し、取引価格に反映させることは、サプライチェーン全体での公正な競争環境を確保し、新たな製品・サービスの創出といったイノベーションの促進に資するものであることから、我が国が持続的な経済成長を実現していく上で極めて重要である。

知的財産権の取引の態様によっては、独占禁止法上の優越的地位の濫用（２条９項５号）として問題となるおそれがあるとともに、取適法又はフリーランス法の適用対象取引に該当する場合、不当な経済上の利益の提供要請（取適法５条２項２号、フリーランス法５条２項１号）、買いたたき（取適法５条１項５号、フリーランス法５条１項４号）又は協議に応じない一方的な代金決定の禁止（取適法５条２項４号）として問題となるおそれがある。

知的財産権と優越的地位の濫用

行為類型		具体的な問題行為
情報の管理	ノウハウ等の一方的な開示要請	技術情報/設計図面・設計加工データ/工場見学の要請/産業データ等の一方的な開示要請
	NDAの締結拒否等	—
	片務的なNDAの締結	—
知的財産権等の価値の適切な評価	知的財産権等の不当な対価設定等	取引の対価の一方的決定/対価の不設定/対価設定方法の一方的決定
	知的財産権等の不当な譲渡要請等	著作権の無償譲渡の要請/無償ライセンスの要請/著作権の帰属条項の設定/著作権人格権の不行使条項の設定/中間成果物等の譲渡要請等/無償の技術指導、PoC、試作品製造等
その他の行為類型	出願干渉	—
	知財訴訟等のリスク転嫁	—
	共同研究開発等	共同研究開発の成果物の不当な帰属・条件設定等

知的財産権等の不当な譲渡要請等ー著作権の無償譲渡の要請

X社は、プログラムの開発に係る取引において、取引先から、一方的に、成果物の著作権の無償譲渡が記載されている請負契約書の締結を要請された。当該成果物には、X社のノウハウやアイデアが含まれていたため、契約内容は納得いくものではなかったが、今後の取引への影響を懸念し、契約を締結せざるを得なかった。

知的財産権等の不当な譲渡要請等 – 著作権の帰属条項の設定

X社は、製品の使用に必要なプログラム製作を含む製品の製造に係る取引において、取引先から、製品に搭載したプログラムについて、一方的に、当該プログラムを製作した時点から、取引先に当該プログラムの著作権が当該取引先に帰属する取引条件となっている契約を締結させられ、取引先との関係を考慮し、著作権を無償で譲渡せざるを得なかった。

知的財産権等の不当な譲渡要請等 – 無償ライセンスの要請

X社は、プログラムの開発に係る取引において、立場の強い取引先に対し、開発に必要な自社のソフトウェア使用に係るライセンス料を求めたところ、一方的に拒否され、見積書に記載することができなかった。取引の打切りをほのめかされたため、無償でのライセンスに応じざるを得なかった。

無償の技術指導、技術検証（PoC）、試作品製造等

X社は、システム開発に係る PoC について、取引先から、一方的に、無償でPoCの成果物を提供するよう要請された。X社は、今後の取引への影響を考慮し、これに応じざるを得なかった。

個人情報・プライバシーの問題

- 改正個人情報保護法とAI開発
- プロファイリング
- プライバシー

個人情報保護法上の問題

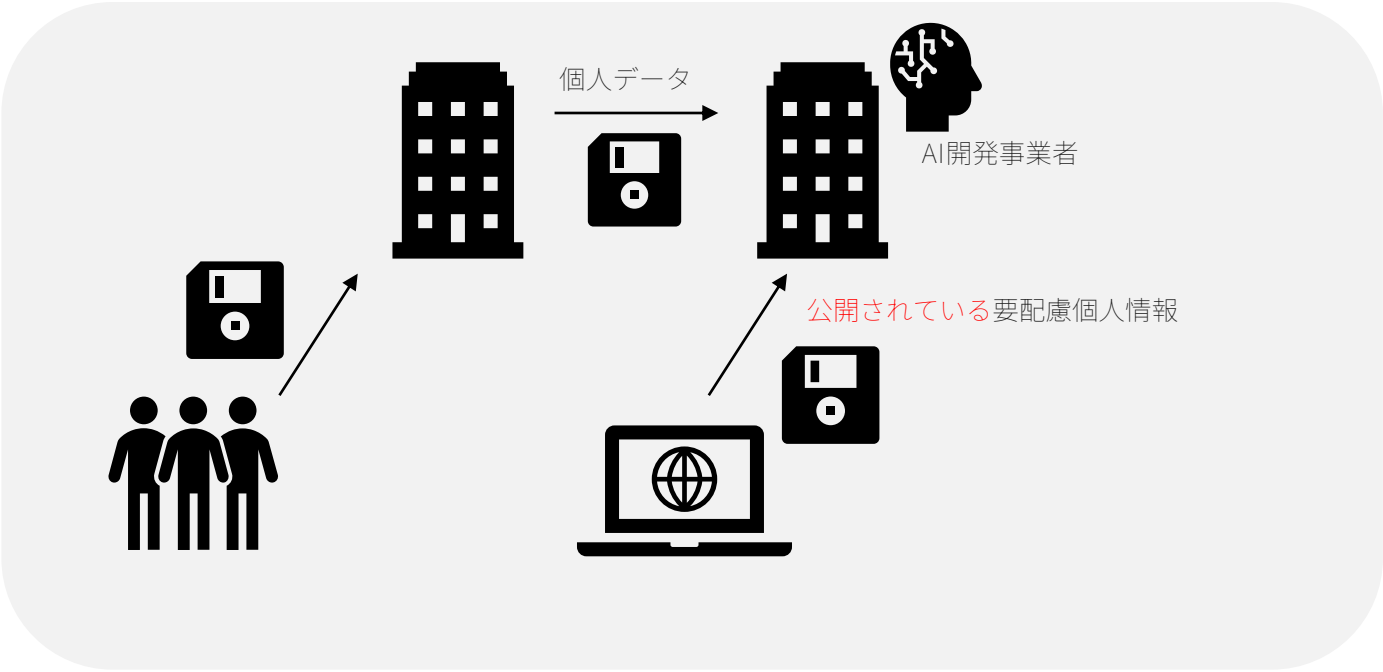
個人情報保護委員会のAIに関する対外的措置

2023年6月2日	OpenAI に対する注意喚起	OpenAIに対して、以下の事項を注意喚起 I. 要配慮個人情報を取得しないこと 特に、機械学習のための情報収集については、 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り組みを行う ② 収集後できる限り即時に、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 ③ 要配慮個人情報が含まれることが発覚した場合には、削除等の対応を行う　など II. 利用者・非利用者の双方に対して、日本語を用いて、利用目的の通知・公表を行うこと
2023年6月2日	生成 AI サービスの利用に関する注意喚起等	生成AIの利用事業者に対して、以下の事項を注意喚起 I. 個人情報を含むプロンプトを入力する場合には、特定された利用目的の範囲内か確認すること II. 本人同意なく個人データを含むプロンプトを入力し、そのデータが出力以外の目的で用いられた場合（ex. 機械学習に利用された場合）には、違法となる可能性があること
2025年2月3日	DeepSeek社に関する情報提供	DeepSeek社が取得した個人情報は、中国のサーバに保管され、同国の法令が適用されることについて一般に情報提供

改正個人情報保護法とAI開発

✓改正個人情報保護法が本国会で審議中。改正法が成立した場合には、2028年に改正法が全面施行される可能性。

✓**現行法では、①個人データの第三者提供や②要配慮個人情報の取得は、原則として本人同意が必要であるが、AI開発等の「統計作成」の目的であれば、一定の条件下で本人同意が不要となる。**



改正個人情報保護法とAI開発

- ✓「統計の作成その他の大量の情報から当該情報を構成する要素に係る情報を抽出して分類、比較その他の解析を行うことにより、当該大量の情報の傾向又は性質に係る情報（個人に関する情報であるものを除く。）を作成する行為」（要件A）のうち、「個人の権利利益を害するおそれが少ないものとして個人情報保護委員会規則で定めるもの」（要件B）を「統計作成等」と定義している（改正案2条13項）。AI開発に際して行われるAIモデルの学習は、膨大なデータを用いてモデル内部のパラメータ（重み）を調整することによって行われるため、要件Aを満たすと考えられる。

- ✓「公開されている要配慮個人情報の取得」は、病歴や犯罪歴を含み得るデータをインターネット上で大規模にスクレイピング及びクローリングする場合が適用場面として考えられる。統計作成等の目的で要配慮個人情報を取得した事業者は、法定事項を公表する必要がある（改正案30条の2第1項）。

- ✓統計作成等の目的による個人データの提供にあたっては、受領者・提供者ともに法定事項を公表する必要があり、提供者・受領者間で提供が統計作成等の目的によるものであることが書面で合意されていることが必要である（改正案30条の2第5項、第6項）。

改正個人情報保護法とAI開発

個人情報の保護に関する法律等の一部を改正する法律案に対する附帯決議（抜粋）

- ✓我が国における人工知能（AI）開発等を含む研究開発及び事業活動が過度に萎縮することのないよう配慮すること。
- ✓AI開発等を含む統計作成等の取扱いについては、他の情報と照合して特定の個人を識別することができないようにするための措置を確実に講ずること。また、統計作成等の概念が限定的に解釈され、実質的な適用範囲が狭められることのないよう留意すること。
- ✓広告の閲覧履歴や商品の購入履歴等から信条等の機微な情報を推知する等の精度の高いプロファイリングの手法が普及しているという指摘を踏まえ、プロファイリングに係る規制の在り方について、諸外国における法制度等を基に引き続き検討を行うこと。
- ✓プライバシー強化技術（PETs）の活用に当たっては、我が国の産業競争力の向上にも資する観点から、適切なインセンティブの在り方について検討すること。

プロファイリング

Cambridge Analytica事件

✓Facebookユーザー最大約8700万人分の個人データが本人の同意なく収集され、心理分析を用いた政治広告に利用された事案。データは性格診断アプリを通じて取得され、当該データから性格傾向・政治傾向・投票行動を分析・推測し、2016年米大統領選やBrexitに係る英国の国民投票において、有権者ごとに異なる政治広告が配信されていた。

リクナビ事件

✓リクナビと契約した企業のウェブサイトや就職情報サイトの閲覧履歴から就活生の選考離脱率・内定辞退率という個人の将来行動を予測する分析を行い、企業に情報提供していた事案。学生本人の十分な同意がないまま、心理的傾向や意思決定の可能性を数値化して第三者に提供した点が問題となった。

プライバシー

プライバシー権
個人の私生活上の情報や行動が、他人によってみだりに公開・干渉されない権利。

自己情報コントロール権
現代的には、自分の情報が誰に、どの目的で収集・利用されるか、情報の公開や削除を積極的に求めることができる、より能動的な権利に発展している。

破産者マップ事件

✓官報に掲載された破産情報を収集し、個人名・住所を地図上に可視化して公開したウェブサイトが大きな社会問題となった事例。プライバシー侵害や差別助長の懸念が強く批判された。個人情報の不適正な利用であるとして、個人情報保護委員会からの行政指導等により、結果としてサイトは閉鎖され、運営者は損害賠償請求を受けるなど法的責任を問われた。

人格権の問題

- 肖像権/パブリシティ権

肖像権/パブリシティ権

肖像権

みだりに自己の容貌、姿態を撮影されたり、撮影された写真等をみだりに公表されないことについて、法律上保護されるべき人格的利益

肖像権の侵害と言えるかについては、被撮影者の社会的地位、撮影された被撮影者の活動内容、撮影の場所、撮影の目的、撮影の態様、撮影の必要性等を総合考慮して、人格的利益の侵害が社会生活上受忍の限度を超えるものといえるかにより判断
（最判H17.11.10民集59巻9号2428頁〔法廷内撮影事件〕等）

パブリシティ権

肖像等が、商品の販売等を促進する顧客吸引力を有する場合、かかる顧客吸引力を排他的に利用する権利

パブリシティ権の侵害と言えるかについては、肖像等の無断利用が、専ら肖像等の有する顧客吸引力の利用を目的とするといえるか否かにより判断
(a)肖像等それ自体を独立して鑑賞の対象となる商品等として使用する場合、(b)商品等の差別化を図る目的で肖像等を商品等に付す場合、(c)肖像等を商品等の広告として使用する場合
(最判H24.2.2民集66巻2号89頁〔ピンク・レディー事件〕等)

肖像権/パブリシティ権

✓有名声優がAIで声を無断模倣された動画の削除を求め、TikTok運営事業者を被告として東京地裁に提訴。原告は、不正競争防止法違反とパブリシティ権侵害を主張、TikTok側は「普遍的な男性の声」だと反論し棄却を求めている。

✓本人の声に類似するものであり、その使用を通じて、本人の声が有する顧客吸引力を利用するものであると認められる場合には、本人の「肖像等」を使用していると認められる。他方、声については、識別力が相対的に弱いとされており、ある合成された音声情報から、その声の主体を特定することは一般的には容易ではないとされ、声の同一性又は類似性の判断要素をどう考えるかは検討課題となり得る。

（出典）肖像、声等の無断利用による民事責任の在り方に関する検討会「想定事例に関する検討資料(1)」

違法・有害情報の拡散に関する問題

- 情報流通プラットフォーム対処法
- コンテンツモデレーション

情報流通プラットフォーム対処法

情報流通プラットフォーム対処法（旧プロバイダ責任制限法）

（特定電気通信による情報の流通によって発生する権利侵害等への対処に関する法律（平成13年法律第137号））

インターネット上の違法・有害情報の流通が社会問題となっていることを踏まえ、**「被害者救済」**と発信者の**「表現の自由」**という重要な権利・利益のバランスに配慮しつつ、プラットフォーム事業者等がインターネット上の権利侵害等への対処を適切に行うことができるようにするための法制度を整備するもの。

①プラットフォーム事業者等の免責要件の明確化

被害者に対する責任

第３条第1項

①権利が侵害されているのを知っていたとき
又は
②これを知りえたと認めるに足る相当の理由があるとき

以外は免責

発信者に対する責任

第３条第２項

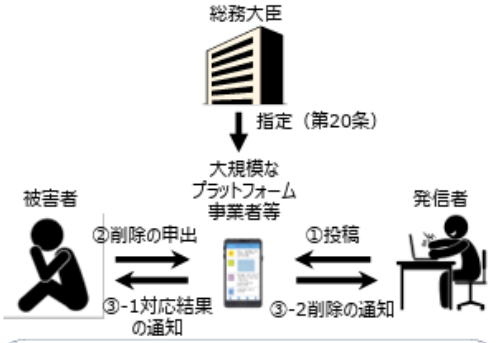
①権利が不当に侵害されていると信じるに足る相当の理由があるとき
又は
②発信者に削除に同意するか照会したが７日以内に反論がないとき

は免責

②発信者情報の開示

- 権利侵害情報の発信者を特定して損害賠償請求等を行うことができるよう、発信者情報開示請求権を規定（第５条）
- 元来２回の手続を要する発信者情報の開示を一つの手続で行うことを可能とする裁判手続（非訟事件手続）を規定（第８条～）

③大規模なプラットフォーム事業者等の義務（R7.4.1施行）



削除対応の迅速化（権利侵害情報に限定）

- 削除申出窓口の整備・公表（第22条）
- 削除申出への対応体制の整備（第24条）
- 削除申出に対する判断・通知（第25条）

※自ら定めた削除基準に基づき、削除するかしないかを事業者自身が判断。申出者に７日以内に通知。

運用状況の透明化

- 削除基準の策定・公表（第26条）
- 削除した場合、発信者への通知（第27条）
- 運用状況の公表（第28条）

（出典）「情報流通プラットフォーム対処法（概要）」

コンテンツモデレーション

✓情プラ法の適用は、名誉毀損等の権利侵害情報に限定される。有害情報についてPF事業者に削除を求めることは表現の自由の観点から慎重であるべき。PF事業者の自主的な取り組みに委ねる。

課題	サービス設計による対応	中間取りまとめにおける提言
違法・有害情報の流通・拡散	レコメンダ（推奨）機能の透明化等	・①レコメンダシステムの透明性の確保、②プロファイリングに基づかない情報表示の選択肢の利用者への提供等、**制度的対応を中心に検討を深めていくことが適当**
	収益化停止措置	・インプレッション数獲得目当ての投稿を減らす等、一定の効果が見込まれるが、表現内容に一定の制約を与えるものであり、有害情報に対する一律の収益化停止措置は、現時点では慎重な検討を要する。 **・まずは事業者自らが取組を約束する※ことで対応することが望ましい。** ・事業者の取組が不十分な場合、速やかに制度的対応を検討することが適当。 **・ただし、災害時など速やかな対応が求められる状況では、制度的対応もあり得る。**
	リスク評価・軽減措置	・事業者ごとにサービスの内容は様々であり、当該サービスに具備される機能がもたらす様々なリスクへの対応はサービスを設計する事業者自身が実施すべきものである。**まずは事業者自らが取組を約束する※ことで対応することが望ましい。** ・事業者の取組が不十分な場合、速やかに制度的対応を検討することが適当。
適切な情報表示	信頼できる情報の優先表示	
	AI生成物へのラベル付与	
利用者の確認	アカウント開設時の本人確認	・匿名表現の自由の保障の観点から、合憲性の評価の際には慎重な比較衡量を行うことが必要。

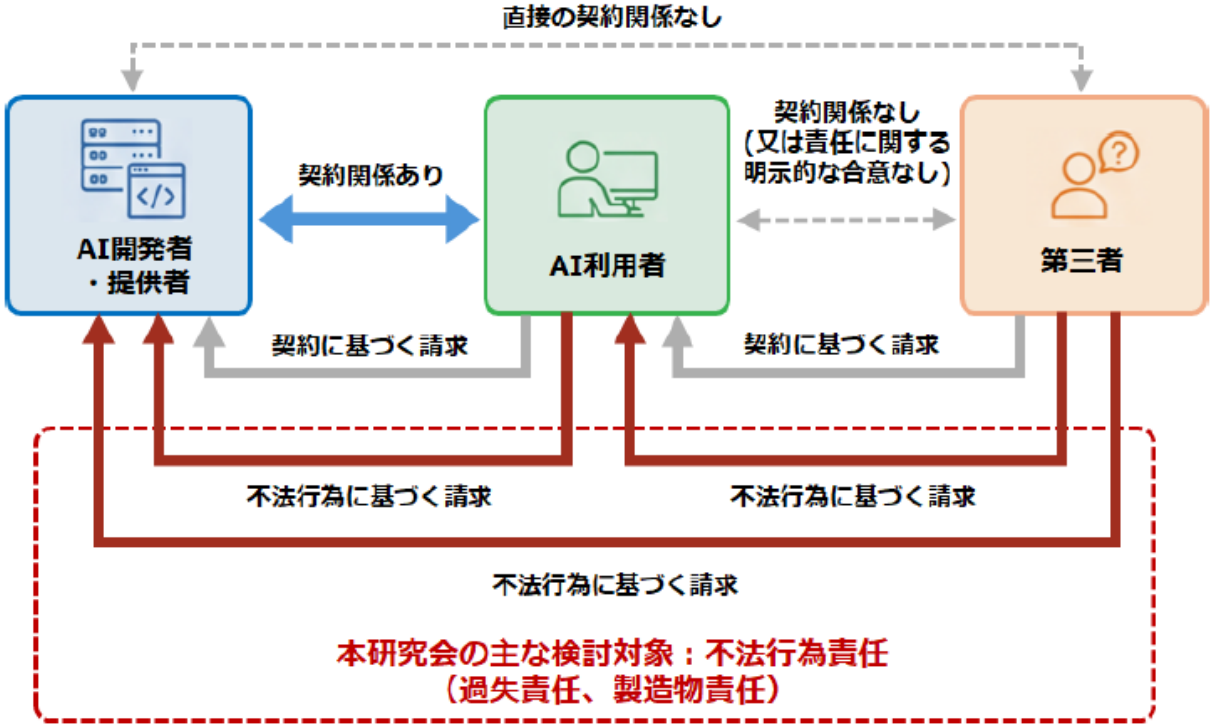
（出典）「デジタル空間における情報流通の諸課題への対処に関する検討会制度WG 中間取りまとめ（概要）」4頁

民事責任の問題

- 不法行為責任、製造物責任

AI利活用における民事責任の解釈適用に関する手引き

✓ 手引き案は、主として一般不法行為（民法709条）と、いわゆるフィジカルAIを念頭に製造物責任を検討対象としている。契約責任も排除されるわけではないが、本手引き案の中心的対象ではない。



出典：経済産業省「AI利活用における民事責任の解釈適用に関する手引き」5頁

AI利活用における民事責任の解釈適用に関する手引き

	補助／支援型 AI	依拠／代替型 AI
概要	• AI が**判断の補助ないし支援**としてのみ用いられ、最終的に人の判断や行動を介在させることが予定されている類型。 • 以下①～③のように補助／支援型 AI としてのみ用いるべき場合がある。 ① AI の機能や利用場面を踏まえると人の判断を代わりに行っているとはいえないケース ② 規制法上の理由により人の最終的な判断が要求されるケース ③ AI の出力内容が潜在的に第三者の権利を侵害するリスクを内包しており、この点について人の評価や検証が必要なケース	• 人の判断や行動を代替する前提で提供され、**AI の出力に依拠しながら用いる**ことが予定されている類型。 • 以下の 2 つの要件が求められる。 (a) 人による判断や行動を介在させることでは実現困難な効用が見込まれること（必要性） (b) AI が一定の精度や安全性を備えていること（精度及び安全性） →個々の業務によって求められる水準は異なるが、同種業務における通常人の作業水準と比較して同等以上の精度や安全性※を備えている場合、AI に判断を委ねることの合理性が認められると考えられる。

出典：経済産業省「AI利活用における民事責任の解釈適用に関する手引き」18頁

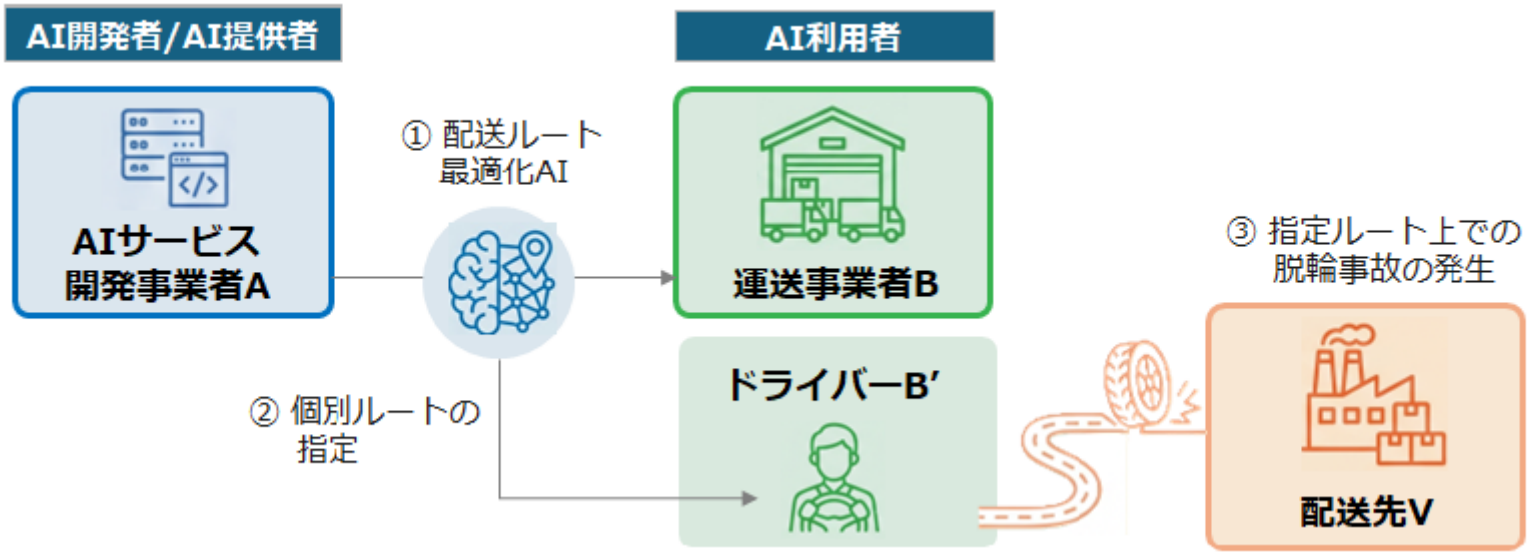
AI利活用における民事責任の解釈適用に関する手引き

責任判断の方向性	補助/支援型AI	依拠/代替型AI
AI 利用者の責任	• 個々の状況下で **AI 利用者が本来払うべき適切な注意の下で AI を用いる**ことが求められる※。 • 具体的には、AI の出力の正確性や適切性を評価しながら AI を用いること、そのために必要な情報収集を行うことや利用上の措置を講ずること等が注意義務の内容となり得る。	• AI 利用者の判断が介在するわけではないため、注意義務の対象は、適切な判断や行動を行うことから **AI システムを組み込んだ業務プロセスの適正な構築及び運用**へと転換する。 • AI の不適切な出力の全てを AI 利用者が検証する等の方法で是正するまでの結果回避義務は認められない。
AI 開発者・提供者の責任	• 性能限界や重要なリスク等についての**説明**を行うことにより、AI の出力の適切性は AI 利用者が是正・検証することが前提となる。 • AI 利用者による予見・対処が容易でないリスクについて一定の**設計上の措置**が求められ得る。	• 上記の安全性を発揮・維持するため合理的に可能な**設計上の措置**や、リスクコントロールの上で重要な情報を分析し AI 利用者への情報提供を行う等の**説明上の措置**が求められる

出典：経済産業省「AI利活用における民事責任の解釈適用に関する手引き」19頁

A社が配送ルート最適化AIシステムを提供し、運送事業者Bが当該AIを使用し、日々の配送ルートを決定していた。ドライバーB'が、悪路を「最適ルート」と表示されたため、これに従ったところ脱輪し、配送先Vに荷物損壊等の損害が生じた事例

- ✓ このAIは、機能面からみると、個々の局面における安全判断を包含するものではなく、現場の道路状況を踏まえた安全判断を代替するものではないことから、補助／支援型AIと整理されている。
- ✓ ドライバーB'には安全運転義務があり、AIの出力に依拠したことは、安全運転義務の水準を変化させる要素とはならず、通常はAI出力とは独立に安全な走行経路を選択すべきものと整理されている。
- ✓ 開発者・提供者Aについては、AIに望ましくない出力があったとしても最終的にAI利用者の判断や行動によって検証・是正することが予定されているから、Aの不法行為責任が認められるのは限定的であると整理されている（因果関係が否定されることも含めての趣旨と思われる）。
- ✓ Aは、性能限界や使用方法等について必要な説明をしている限り、第三者との関係で責任を負う場面は限定的と整理されている。



サイバーセキュリティの問題

- セキュリティ関連法令

セキュリティ関連法令

- ✓ サイバー攻撃者の刑事責任の追及

①**電磁的記録不正作出及び供用罪**（刑法161条の2）

第三者の事務処理を誤らせる目的で、事務処理に際して使用される権利、義務又は事実証明に関する電磁的記録を不正に作出する行為

②**不正指令電磁的記録作成・提供罪**（刑法168条の2第1項）

正当な理由なく、第三者のコンピューターで実行され得る状態に置く目的で、ウィルス、マルウェアなどを作成・提供する行為

③**電子計算機損壊等業務妨害罪**（刑法234条の2）

第三者が業務に使用するコンピュータ・電磁的記録を損壊・虚偽情報、不正な指令を与えて業務を妨害する行為

④**電子計算機使用詐欺**（刑法246条の2）

コンピューターを使用した詐欺

⑤**電磁的記録毀棄罪**（刑法258条、259条）

公用・権利義務に関する電磁的記録を毀棄

⑥**不正アクセス禁止法違反**（不正アクセス禁止法3条）

不正ログイン、セキュリティホール攻撃、フィッシング行為、識別符号の入力を求める迷惑メールなど

AIガバナンス

AIガバナンス

環境・リスク分析	ゴール設定	システムデザイン	運用	評価
				
把握する ✓ AIの便益とリスク ✓ AIの社会的な受容 ✓ 自社のAI成熟度	策定する ✓ AIポリシー ✓ 社内行動基準	設計・構築する ✓ ゴールとの乖離の評価・対応方法 ✓ 組織間の連携体制 ✓ インシデント予防・対策 ✓ 社員の教育体制	説明可能な状態を確保しつつ、運用する ✓ AIマネジメントシステム全体の運用状況 ✓ AIシステムごとの運用状況	チェックする・改善点を見つける ✓ 第三者による評価 ✓ 関係者の意見収集・対応

✓社内横断的なワーキング・グループや倫理委員会などを設置
✓AIに関する指針・ガイドライン・原則等を策定
✓企画・開発段階において、AI利活用の倫理上のリスクについて、各部門でレビューを実施
✓情報漏洩の際に対応すべき事項に関する社内規定を策定するなどセキュリティ確保のためのルールを整備
✓社員向けのAI倫理やAIリテラシー等に関する教育を実施

出典：経済産業省「AI事業者ガイドライン活用の手引き（案）」

ご清聴ありがとうございました。