2026 年 1 月 23 日

EU と日本の AI 規制を実務でどう捉えるか
クロスボーダーAI ビジネスのための実践ガイド

創・佐藤法律事務所
弁護士　斎藤　　創
ﾊﾟﾗﾘｰｶﾞﾙ　ｼｬｰﾛｯﾄ　ﾄﾞｩﾙｰｽﾞ

エグゼクティブ・サマリー

AI(人工知能)を巡る規制は、もはや技術部門や法務部門だけの問題ではなく、企業の事業戦略そのものを左右する重要な要素となっています。特に、EU と日本の両市場で AI を開発・提供・利用する企業にとっては、両者の規制アプローチの違いを正確に理解することが不可欠です。本稿は、EU と日本における AI 規制の考え方の違いを整理し、それが企業実務にどのような影響を与えるのかを、実務の視点から解説するものです。

EU は、EU AI 法(EU Artificial Intelligence Act)により、AI をリスクに応じて分類し、高リスクと位置付けられる AI については、市場投入前から詳細なガバナンス体制、技術文書の整備、適合性評価等を求める包括的かつ拘束力のある制度を採用しました。EU 市場への進出やサービス提供を行う企業にとって、AI 規制対応は付随的なコンプライアンス事項ではなく、プロダクト設計や市場参入戦略の中核的な検討事項となりつつあります。

これに対し、日本は、AI に特化した包括的なハードローを導入するのではなく、「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」(いわゆる AI 推進法)を中心に、研究開発・社会実装を促進しつつ、個人情報保護法や労働法、消費者保護法等の既存法制によって具体的なリスクに対応するという政策を採っています。このイノベーション重視・事後的責任追及型のモデルは、初期段階での規制負担を抑える一方、企業には内部ガバナンスや説明可能性の確保が強く求められます。

クロスボーダーで AI ビジネスを展開する企業にとって、こうした違いは、コンプライアンスコスト、開発スケジュール、組織体制の設計に直接的な影響を及ぼします。EU 基準に合わせた対応が一つのベースラインとなる場合もありますが、それだけで日本法上の論点が解消されるわけではありません。逆に、日本市場を前提に設計された AI システムは、EU 市場に展開する際に大幅な見直しを迫られることもあります。本稿が、こうした判断を行う際の実務的な指針となることを意図しています。

1. はじめに：AI 規制はなぜ事業戦略の問題なのか

なぜ各国の AI 規制はこれほど異なる方向に進んでいるのか、そしてその違いは企業実務にどのような影響を与えるのか。

AI 規制を巡る議論は、「EU は厳しい」「日本は緩やか」といった単純な対比で語られがちです。しかし、この捉え方だけでは、企業実務にとって本質的な問題を見誤るおそれがあります。重要なのは、規制の厳しさそのものではなく、各国がどのような制度設計によって AI リスクに向き合い、その結果として企業の意思決定や事業運営にどのような影響が生じるのかという点です。

EU と日本の対比が特に示唆的なのは、両者が「信頼できる AI の実現」や「社会的リスクの抑制」といった政策目的を共有しながらも、まったく異なる法的枠組みを選択している点にあります。EU は、AI 専用の包括的な法制度を通じて、事前のリスク管理と市場投入前の統制を重視するアプローチを採用しました。一方、日本は、既存の法制度と行政実務の中に AI ガバナンスを位置付け、問題が顕在化した段階で対応するという枠組みを基本としています。

こうした制度設計の違いは、企業にとって抽象的な法政策論にとどまりません。それは以下のような日常的な実務判断に直結します。

- どの段階で法務レビューが必要になるのか
- どの程度の文書化が市場投入前に求められるのか
- 規制当局の執行リスクをどのように評価すべきか
- 製品開発のタイムラインにどの程度の余裕を見込むべきか
- 組織内のどの部署が主導的に対応すべきか

本稿では、いずれの制度が規範的に望ましいかを論じることを目的とはせず、EU と日本の AI 規制が実務上どのように機能しているのか、そして両市場で AI を活用する企業が何を理解しておくべきかを明らかにします。まず両者の規制思想を整理し、次に各制度の具体的内容を確認した上で、実務的な比較とケーススタディを通じて企業への影響を検討し、最後に企業が取るべき対応のポイントを提示します。

2. EU と日本の規制思想: ハードローとソフトロー

本章では、EU と日本の AI 規制を理解するための概念的枠組みを提示します。

2.1. 規制手法の選択: 拘束力か柔軟性か

EU と日本の AI 規制を比較する際の出発点は、「新しい技術をどのような法形式で規

律するか」という根本的な問いにあります。すなわち、法的拘束力を伴う明確な義務を事前に課すべきか、それとも柔軟性を重視したガイドラインや既存法制による事後的な対応を中心とすべきか、という問題です。

ハードローとは、一般に、法的拘束力を有し、違反した場合に裁判所や行政機関による制裁が科され得る規範を指します。法律、政令、省令といった形式で明文化され、執行機関による強制が可能です。ハードローの利点は、法的確実性が高く、権利義務関係が明確になる点にあります。企業にとっては、何が許され何が禁じられているかが事前に分かるため、長期的な投資判断やコンプライアンス体制の構築がしやすくなります。

ソフトローとは、法的拘束力自体は有しないものの、行政指導や業界慣行、レピュテーション(評判)、市場の期待を通じて行動を方向付ける規範を意味します。ガイドライン、ベストプラクティス、原則声明などがこれに該当します。ソフトローの利点は、技術進展や社会状況の変化に応じて柔軟に更新できる点、そして事業者の創意工夫の余地を残せる点にあります。

2.2. AIにおけるハードローとソフトローのトレードオフ

AIのように技術進展が速く、社会的影響の射程が不確定な分野においては、この選択は特に重要な意味を持ちます。

(1) ハードローの利点と課題

利点として、ハードローは責任の所在を明確にし、基本的権利を強く保護できます。特に、AIが雇用、信用評価、社会的サービスへのアクセスといった重要な場面で用いられる場合、明確な法的保護があることで、個人の権利が侵害されるリスクを低減できます。また、域内での統一的な基準を設けることで、企業にとっても複数国での展開が容易になり得ます。

他方で課題もあります。技術の進展速度が速い分野では、法制度が実態に追いつかず、時代遅れになるリスクがあります。また、詳細な規制は、特に資金や人材に限りのあるスタートアップや中小企業にとって過度な負担となり、イノベーションを阻害する可能性があります。

(2) ソフトローの利点と課題

ソフトローは、変化への適応力に優れています。ガイドラインであれば、新たなリスクが判明した際に速やかに更新することができます。また、事業者に自主的な工夫の

余地を残すことで、多様なアプローチが試され、社会全体として最適な解決策が見つかりやすくなる可能性があります。

しかし、ソフトローには予見可能性の低さという課題があります。何が法的に許容されるのかが明確でないため、企業は慎重にならざるを得ず、かえって萎縮効果が生じることもあります。また、実効性や説明責任のメカニズムが弱く、実際に問題が生じた際の対応が後手に回るリスクもあります。

2.3. EU と日本の選択

EU と日本は、このトレードオフに対して明確に異なる解を示しました。
EU の選択は、域内での統一的なルールと高い法的確実性を優先するものです。単一市場を形成する EU にとって、加盟国間での規制の断片化を防ぎ、企業が複数国で一貫した対応をとれるようにすることは重要な政策目標です。また、基本的人権の保護を重視する EU 法の伝統からも、AI による権利侵害リスクに対して明確な法的保護を設けることは自然な選択でした。

日本の選択は、国際競争力の維持や実証実験の促進を重視するものです。日本政府は、AI 分野において諸外国に遅れをとっているという認識を持っており、規制による過度な制約を避けることで、企業による積極的な研究開発と社会実装を後押しすることを選びました。既存の法制度が一定の安全網として機能するという前提のもと、AI 特有のハードローは最小限にとどめる判断をしています。

3. EU AI 法: リスク分類に基づく事前規制モデル

前章で示した概念的枠組みを踏まえ、本章では EU AI 法の具体的内容を検討します。

3.1. EU AI 法の成立経緯と基本構造

EU AI 法は、2021 年に欧州委員会から提案され、欧州議会と理事会での立法交渉を経て 2024 年に正式に成立しました。2025 年から段階的に適用が開始されており、条項によって施行時期が異なります。

本法の中心的な組織原理は、リスクベース・アプローチです。AI システムをその利用態様や社会的影響に応じて分類し、リスクが高いと評価される AI ほど厳格な義務を課すという構造を採っています。この枠組みは、すべての AI に一律の規制を課すのではなく、真にリスクの高い領域に規制資源を集中させるという考え方に基づいています。

3.2. 適用範囲と域外適用

(1) 地理的適用範囲

EU AI 法は、EU 域内に設立された事業者に限らず、以下の場合にも適用されます。

- AI システムを EU 市場に投入する場合
- AI システムの出力が EU 域内で利用される場合

この広範な域外適用により、日本企業や他の第三国企業であっても、EU 市場を対象とする場合には規制対象となる可能性があります。これは、EU 一般データ保護規則(GDPR)が採用したアプローチと類似しており、EU の規制が実質的にグローバルスタンダードとして機能する可能性を示唆しています。

(2) 適用除外

一方で、以下のような活動は適用除外とされています。

- 軍事、防衛、国家安全保障目的での利用
- 外国の公的機関や国際機関による法執行目的での利用(個人の権利保護の保障措置を条件とする)
- 個人的・非業務的な利用
- 研究開発段階にある場合(特定の条件下)

また、自由でオープンソースのライセンスの下で開発・公開される AI については、高リスクに該当しない限り、一定の配慮がなされています。

3.3. 執行体制

EU AI 法の執行は、複層的な体制を採用しています。
EU レベルでは、欧州委員会内に新設された AI Office が中核的な調整・監督機能を担います。特に、汎用 AI モデル(General-Purpose AI Models)については、AI Office が直接的な監督権限を持ちます。

加盟国レベルでは、各国が指定する所管当局および市場監視当局が、日常的な執行を担当します。これは、製品安全規制やデジタル規制における他の EU 法制と同様の枠組みであり、中央での政策調整と現場での執行能力を組み合わせる意図があります。

3.4. リスク分類の詳細

EU AI 法は、AI システムを以下の 4 つのカテゴリーに分類しています。

3.4.1. 禁止される AI(許容できないリスク)

EU AI 法第 5 条は、基本的人権に対するリスクが許容できないと判断される AI 手法について、全面的に禁止しています。これには以下が含まれます。

- 潜在意識への働きかけや脆弱性の悪用: 個人の行動を実質的に歪める形で、潜在意識に働きかける技術や、年齢・障害等による脆弱性を悪用する技術
- ソーシャルスコアリング: 社会的行動や個人的特性に基づいて個人を評価・分類し、その結果として不利益な取扱いを受けるシステム(一定の公的機関による利用)
- 予測的警察活動: プロファイリングに基づいて、誰が犯罪を犯しやすそうかを予測するシステム
- 顔画像の大規模スクレイピング: インターネット上や監視カメラ映像から顔画像を無差別に収集してデータベースを構築する行為
- 感情認識 AI: 職場や教育機関における感情認識技術の利用(例外的に医療目的や安全目的で正当化される場合を除く)

これらの禁止は、違反した場合に最も重い制裁の対象となります。

3.4.2. 高リスク AI

AI システムが以下のいずれかに該当する場合、高リスク AI として分類されます。

(1) 類型 1: 製品の安全コンポーネント

既存の EU 製品安全法制(Annex I に列挙)の対象となる製品の安全コンポーネントまたは当該製品自体としての AI。例えば、医療機器、自動車、航空機などに組み込まれた AI が該当し得ます。

(2) 類型 2: 特定の高影響領域での利用

Annex III に列挙される用途での AI。主なものとして以下があります。

- 生体認証および分類
- 重要インフラの管理・運営
- 教育および職業訓練(入学・評価等)
- 雇用、労働者管理、自営業へのアクセス
- 必須の民間サービスおよび公的給付へのアクセス
- 法執行
- 移民・亡命・国境管理
- 司法・民主的プロセスの運営

ただし、Annex III に列挙されていても、個別の事案において重大なリスクを生じさせないことについて、堅固な文書化と正当化理由を提示できる場合には、例外的に高リスク分類から除外され得ます。

3.5. 高リスク AI に対する義務

高リスク AI のプロバイダー(提供者)およびデプロイヤー(利用者・導入者)には、詳細な義務が課されます。

(1) 用語の定義

プロバイダー: AI システムを開発し市場に提供する者
デプロイヤー: AI システムを自らの権限・管理下で使用する者(導入企業等)

(2) プロバイダー(提供者)の主な義務

① **リスク管理システム**: AI システムのライフサイクル全体を通じた継続的なリスク管理体制の構築・維持
② **データガバナンス**: 訓練・検証・テストに用いるデータセットが、関連性を有し、十分に代表性があり、バイアスの可能性について検証されていることの確保
③ **技術文書の作成**: 規制当局がコンプライアンスを評価できる詳細な文書の準備
④ **記録保持(ロギング)**: 適切な場合にはログの自動記録
⑤ **透明性と利用説明書**: デプロイヤーに対し、意図された目的、限界、適切な運用方法を明示
⑥ **人間による監視(Human Oversight)**: 適切に訓練された人間が AI の出力を監督し、必要に応じて介入できる設計
⑦ **正確性、堅牢性、サイバーセキュリティ**: 利用文脈に照らして適切な性能基準の達成
⑧ **適合性評価と登録**: 市場投入または運用開始前に、関連する適合性評価手続を完了し、必要に応じてシステムを登録

(3) デプロイヤーの主な義務

デプロイヤー(AI システムを自らの権限・管理下で使用する者、すなわち導入企業等)にも以下のような義務が課されます。

① プロバイダーの利用説明書に従った使用
② 人間による監視措置の実施
③ 重大なインシデントが発生した場合の報告
④ 入力データの関連性確保

3.6. 制裁

EU AI 法違反に対しては、以下のような行政制裁金が科され得ます。

① **禁止行為違反**: 最大 3,500 万ユーロまたは全世界年間売上高の 7%のいずれか高い方
② **その他の義務違反**: 最大 1,500 万ユーロまたは全世界年間売上高の 3%のいずれか高い方
③ **不正確な情報提供:** 最大 750 万ユーロまたは全世界年間売上高の 1%のいずれか高い方

これに加え、是正措置、市場からの撤回、リコールといった行政措置も可能です。

4. 日本の AI ガバナンス: イノベーション重視・事後的責任モデル

本章では、日本の AI 規制アプローチを詳しく検討します。

4.1. 立法意図と基本的枠組み

日本の「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 推進法)は、2024 年に成立し、同年中に全面施行されています。この法律は、EU のような包括的な規制法ではなく、政策推進法としての性格を持っています。

法律の目的は、第 1 条で「人工知能関連技術の研究開発及び活用を推進し、もって経済社会の発展及び国民生活の向上に寄与すること」と明記されており、「規制」よりも「推進」に重心が置かれています。

(1) 立法者の問題意識

立法過程の資料によれば、日本政府は、AI 技術の開発・実装において主要国に遅れをとっているという認識を持っています。同時に、AI の社会的影響に対する国民の関心も高まっています。このような状況下で、新たな包括的規制を導入するのではなく、イノベーションを促進しつつリスクは既存法制で対応するというバランスを選択しました。

この考え方は、日本の行政法の伝統とも整合的です。日本では、規制目的を達成する手段として、法的拘束力のあるハードローだけでなく、行政指導、ガイドライン、業界団体との協議といった柔軟な手法が広く用いられてきました。レピュテーション(評判)や「お上」との関係性が重視される日本の企業文化においては、こうしたソフトな手法も一定の実効性を持ち得ます。

(2) 基本理念(第 3 条)

AI 推進法は、以下のような基本理念を掲げています。

- 人間の尊厳を重視し、人間の能力を補完・拡張するものであること
- 多様性を尊重し、公平性・透明性を確保すること
- 安全性・信頼性を確保すること
- プライバシーを保護すること
- 公正な競争を促進すること

これらは、ソフトローとしての指針であり、直接的に私人間の権利義務を創設するものではありませんが、後述する「合理的な措置」の内容を解釈する際の基準となります。

(3) 事業者の責務(第 7 条)

AI 関連事業者(活用事業者)には、第 7 条により以下の 2 つの責務が課されています。

① **AI 活用の努力義務**: 自ら積極的な AI 関連技術の活用により事業活動の効率化および高度化ならびに新産業の創出に「努める」こと

② **施策への協力義務**: 国・地方公共団体が実施する施策に「協力しなければならない」こと

①は努力義務にとどまりますが、②は「協力しなければならない」という義務であり、協力しない場合は後述する第 16 条に基づく指導・助言その他の必要な措置の対象となり得ます。ただし、EU のような明確な罰則規定や詳細な義務内容が定められているわけではありません。

4.2. 適用範囲

AI 推進法には EU AI 法のような明示的な域外適用条項は設けられていません。しかし、政府の政策文書および大臣答弁により、日本市場で事業活動を行う国外企業(日本語でのサービス提供や日本のユーザーを対象とする場合等)は、適用対象から一律に除外されるものではないことが明らかにされています。

同法の規定は努力義務として定められていますが、日本国内で活動する企業(国内・国外を問わず)は、個人情報保護法、労働法、消費者保護法、業法等の既存法制の全面的な適用を受けます。

4.3. 調査研究等と指導・助言の権限

AI 推進法第 16 条は、国に対して以下の権限を付与しています。

- 国内外の AI 関連技術の研究開発・活用動向に関する情報収集
- 不正な目的・不適切な方法による権利侵害事案の分析・対策の検討
- その他の AI 関連技術の研究開発・活用の推進に資する調査研究
- これらの結果に基づく、活用事業者等に対する指導、助言、情報提供その他の必要な措置

第 16 条後段(上記 4)は、「講ずることができる」ではなく「講ずるものとする」という規定となっており、国による指導・助言が積極的に実施される可能性を示唆しています。ただし、具体的な措置の内容や判断基準については、今後の運用において明らかになると考えられます。

4.4. 既存法制との関係: 実質的なリスク管理の場

日本の AI ガバナンスにおいて最も重要なのは、既存法制が AI に関する実質的な法的リスクの源泉となるという点です。AI 推進法は理念と方向性を示すにとどまり、具体的な法的責任は、以下のような既存法によって判断されます。

4.4.1. 個人情報保護法(APPI)

AI システムの開発・運用において個人情報を取り扱う場合、個人情報保護法の全面的な適用を受けます。

(1) 訓練データの収集

機械学習モデルの訓練に個人情報を用いる場合、以下が問題となります。

- 取得時の利用目的の特定・通知(第 21 条)
- 本人同意の要否(第 18 条、第 27 条)
- 要配慮個人情報(人種、病歴等)の取得制限(第 20 条)
- 安全管理措置(第 23 条)

判例・実務上、AI 訓練目的が「当初の取得目的」に含まれていない場合、新たな目的での利用として本人同意が必要となる場合があります。

(2) プロファイリングと本人関与

AI によるプロファイリング(個人の行動・関心等を分析・予測すること)は、個人情報保護法上、「保有個人データ」の利用として位置付けられます。本人は、開示請求権(第 33 条)や利用停止請求権(第 35 条)を有するため、AI による判断のロジックや根拠についての説明が求められる場合があります。

(3) 海外事業者への委託・移転

AI モデルの訓練や推論を海外のクラウドサービスで行う場合、外国にある第三者への提供(第 28 条)の問題が生じます。本人同意または適切な体制整備が求められます。

4.4.2. 労働法制

AI 採用ツールや人事評価 AI は、以下の法的リスクを伴います。

- 募集・採用段階での情報収集制限: 職業安定法により、業務遂行に必要な範囲を超えた個人情報の収集は制限されます
- 差別的取扱いの禁止: 労働基準法第 3 条(国籍・信条・社会的身分による差別禁止)、男女雇用機会均等法による性別差別禁止などが適用されます。AI の判断結果が間接的に差別的効果を持つ場合も問題となり得ます
- 解雇・配置転換における合理性: AI が示唆する判断を機械的に適用して解雇や配置転換を行う場合、裁判所は「客観的に合理的な理由」と「社会通念上の相当性」(労働契約法第 16 条)の有無を厳格に審査します

4.4.3. 消費者保護法制

消費者向けに AI サービスを提供する場合、以下が適用され得ます。

① **不当表示規制(景品表示法)**: AI の性能や精度について、実際よりも著しく優良であると誤認させる表示は規制対象

② **不当な勧誘(消費者契約法)**: AI による自動勧誘が、不実告知や重要事項の不告知に該当する場合、契約取消事由となり得る

③ **製造物責任法**: AI を組み込んだ製品に「欠陥」がある場合、製造業者は損害賠償責任を負う

4.4.4. その他の法制

- 知的財産法: AI による生成物の著作権、他者の著作物を訓練データとして利用することの適法性(著作権法第 30 条の 4 など)
- 競争法: AI による価格カルテルや取引条件の不当な差別
- 金融規制: 信用スコアリングや投資助言における AI 利用に対する業法上の規制

5. EU と日本の規制の違いは実務にどう影響するか

ここまでで両規制の内容を確認しました。本章では、その違いが企業実務に与える具体的な影響を整理します。

5.1. 規制の主要な相違点: 一覧比較

以下の表は、EU と日本の AI 規制アプローチを実務的な観点から対比したものです。

項目	EU(EU AI 法・ハードロー)	日本(AI 推進法+既存法・ソフトロー+α)
規制の基本的性格	拘束力のある AI 専用規制により、法的に強制可能な義務を設定	政策主導のガバナンス。既存の分野別法制と組み合わせて対応
規制の重点	基本的人権の保護を、リスク管理と事前統制によって実現	イノベーション促進。リスクは事後的責任によって対応
リスク分類	明示的なリスクベース分類(許容不可・高リスク・限定的リスク・最小リスク)	AI 特有のリスク分類体系なし。リスクは既存法の枠内で個別評価
主要な義務	市場投入前の適合性評価、技術文書、リスク管理、人間による監視	ガバナンス体制、合理的措置の努力、個人情報保護法・労働法・消費者保護法の遵守
執行モデル	EU レベルでの調整の下、各国の監督当局が行政執行	行政指導、公表、既存法による執行
罰則・制裁	重大な行政制裁金、是正措置、市	AI 法自体の罰則なし。既存法

	場からの撤回	令違反に基づく制裁
域外適用	あり。AI システムが EU 市場または域内個人に影響する場合に適用	原則として国内中心。ただし既存法(個人情報保護法等)の域外適用はあり
企業への実務的影響	高い初期コンプライアンスコストと長い上市期間。ただし法的確実性は高い	初期の規制負担は低いが、内部ガバナンスと行政対応力が重要

5.2. 実務への影響: コンプライアンス、時間、予見可能性、執行リスク

前章までで説明した制度的相違は、企業実務において以下の形で具体化します。

(1) コンプライアンス体制とコスト

EU では高リスク AI について、市場投入前にリスク管理システム、データガバナンス、技術文書、適合性評価等の完了が必須です。これには専門人材や外部アドバイザーの関与が必要となり、相当な初期投資を要します。

日本では AI 特有の事前承認制度がないため初期コストは抑えられますが、問題発生時に合理的な判断プロセスを説明できる記録整備と、既存法制(個人情報保護法、労働法等)への対応が求められます。

(2) 市場投入までの期間

EU 高リスク AI の適合性評価と社内準備には数ヶ月を要する場合があり、競争の激しい市場では重大な考慮要素となります。日本では技術的準備が整い次第のサービス開始が可能ですが、事後的リスクは企業が自ら管理する必要があります。

(3) 法的予見可能性

EU は禁止行為、リスク区分、義務内容が明文化され全加盟国に統一適用されるため、予見可能性が高く長期投資判断がしやすくなります。日本は既存法制の解釈・適用による事後判断が中心で、新規利用態様については不確実性が残る場合があります。

(4) 執行リスク

EU 違反には最大 3,500 万ユーロまたは全世界売上高 7%の制裁金に加え、製品撤回や是正命令のリスクがあります。日本の AI 推進法自体に制裁はありませんが、既存法令違反による行政処分や、行政指導・公表によるレピュテーション毀損リスクには注意が必要です。

5.3. クロスボーダー事業展開への示唆

(1) EU 基準をベースラインとする戦略

両市場で事業を行う企業にとって、EU AI 法の高リスク要件を満たす体制構築が、堅牢なガバナンスのベースラインとなります。ただし、日本固有の法的論点(個人情報保護法の詳細要件、労働法上の慣行、消費者保護法制)は別途検討が必要です。

(2) 日本を起点とする場合の課題

日本市場を主眼に開発された AI システムを EU 市場に展開する際は、技術文書の遡及的作成、リスク管理プロセスの形式化、適合性評価手続への対応といった追加作業が発生します。早期段階から EU 要件を意識することで手戻りを最小化できます。

6. ケーススタディ: 採用 AI を EU と日本で使う場合

本章では、具体的な利用場面を通じて、両規制の違いが実務にどのように現れるかを検討します。

6.1. 想定事例

ある企業が、AI を用いた採用スクリーニングシステムを開発しました。このシステムは、応募者の履歴書、オンライン適性検査の結果、ビデオ面接での応答を分析し、採用候補者を推奨します。この企業は、同じシステムを EU と日本の両方で使用することを検討しています。

この事例が重要なのは、以下の理由からです。

- 雇用という高い影響力を持つ領域での利用である
- 差別リスクが内在する
- 大量の個人情報を処理する
- 多国籍企業が一貫して展開したいと考える典型的な用途である

6.2. EU における取扱い: 高リスク AI としての厳格な義務

(1) リスク分類

EU AI 法の下、雇用、採用、選考に関する意思決定に用いられる AI は、Annex III に明示的に列挙されており、原則として高リスク AI に該当します。
これは、個人の雇用機会へのアクセスに実質的な影響を与え得るためです。

(2) 課される義務(詳細)

高リスク AI として分類される場合、プロバイダー(AI システム開発・提供者)およびデプロイヤー(利用者、この場合は採用を行う企業)には、以下のような詳細な義務が課されます。

(3) プロバイダー(AI システム開発・提供者)の義務

① **リスク管理**: システムのライフサイクル全体を通じた継続的なリスク管理体制の構築・維持。特に、バイアスや差別的効果のリスクを特定・評価・軽減する措置

② **データガバナンス**:

- 訓練データセットが、対象となる人口集団を適切に代表していることの確認
- 既知のバイアス(性別、人種、年齢等)の検証と是正
- データ品質の継続的な監視

③ **技術文書と記録保持**:

- システムの設計、開発、テストに関する詳細な文書の作成
- 規制当局がコンプライアンスを評価できる情報の整備
- 必要に応じたログの自動記録

④ **透明性と利用説明書**:

- デプロイヤー(この場合、採用を行う企業)に対する、システムの意図された目的、限界、適切な使用方法の明示
- システムがどのような要素を重視し、どのような判断をするかの説明

⑤ **人間による監視**:

- 適切に訓練された人間が AI の出力を監督し、必要に応じて介入できる設計
- 採用の最終判断を人間が行うことを担保する仕組み

⑥ **正確性、堅牢性、サイバーセキュリティ**:

- 採用文脈において適切な性能基準の達成
- 不正アクセスや操作への耐性

⑦ **適合性評価と登録:**

- 市場投入前に、関連する適合性評価手続(多くの場合、内部管理に基づく評価)を完了
- EU データベースへの登録

(4) デプロイヤー(採用企業)の義務

デプロイヤー(この場合、採用 AI を実際に使用する企業)には以下の義務が課されます。

- プロバイダーの利用説明書に従った使用

- 人間による監視措置の実施(例: AI の推奨を参考情報とし、最終判断は人間が行う)
- 重大なインシデント(例: 明らかな差別的結果)が発生した場合の監督当局への報告
- 入力データの品質確保

(5) 違反の場合の帰結

これらの義務に違反した場合、以下のリスクがあります。

- 行政制裁金(最大 1,500 万ユーロまたは全世界売上高の 3%)
- システムの市場撤回や使用停止の命令
- 是正措置の要求
- レピュテーション毀損

6.3. 日本における取扱い: AI 特有の事前規制なし、ただし既存法の適用

(1) AI 推進法上の位置づけ

日本では、同じ採用スクリーニングシステムは、AI 特有の適合性評価や事前承認の対象とはなりません。AI 推進法は、「合理的に実行可能な範囲での必要な措置」を努力義務として求めるのみです。

しかし、これは法的リスクがないことを意味しません。実際の法的リスクは、以下の既存法制から生じます。

(2) 関連する法的論点

① 雇用・採用規制

- **職業安定法**: 募集に際して収集できる個人情報の範囲は、業務遂行に必要な範囲に限定されます。AI が過度に広範な情報(例: SNS の投稿内容、趣味嗜好)を分析する場合、問題となり得ます
- **労働基準法第 3 条**: 国籍、信条、社会的身分による差別的取扱いの禁止。AI の判断が結果的に特定の属性を持つ者を不利に扱う場合、間接差別として問題視される可能性
- **男女雇用機会均等法**: 性別による差別的取扱いの禁止。AI のアルゴリズムが、訓練データのバイアスにより女性応募者を不利に評価する場合、法令違反のリスク
- **実務上の採用慣行**: 日本では、採用プロセスにおける説明責任が重視されます。AI による不採用判断について、応募者から説明を求められた場合に対応できる体制が求められます

② 個人情報保護法(APPI)

- **取得時の利用目的の特定・通知(第 21 条)**: 応募者の個人情報を AI 分析に用いることを、明確に利用目的として示す必要があります
- **本人同意の要否**: 応募者から直接取得する場合は通知で足りますが、第三者(例: SNS、リファレンスチェック業者)から取得する場合は原則として本人同意が必要(第 27 条)
- **要配慮個人情報の取扱い(第 20 条)**: 人種、病歴、犯罪歴等の要配慮個人情報は、原則として本人同意なしに取得できません。AI がこうした情報を推測・利用する場合、慎重な検討が必要
- **安全管理措置(第 23 条)**: 応募者データの漏洩・不正アクセスを防ぐための技術的・組織的措置
- **開示請求・利用停止請求への対応(第 33 条、第 35 条)**: 応募者から、AI による判断の根拠や利用停止を求められた場合の対応体制

(3) 消費者保護・不当表示のリスク(該当する場合)

採用 AI システムを外販する場合、その性能や精度について、実際よりも著しく優良であると誤認させる表示を行うと、景品表示法違反となり得ます。

① AI 推進法に基づくガバナンス期待

法的強制力はないものの、AI 推進法とそれに関連するガイドラインは、以下のような期待を示しています。

- 透明性: AI の判断プロセスについて説明可能であること
- 公平性: バイアスの検証と是正の取組
- 人間中心: 最終判断を人間が行うこと

② 実務上の対応

日本で採用 AI を用いる企業は、形式的な事前承認は不要ですが、以下の対応が推奨されます。

- **データセット選定の記録**: どのようなデータを訓練に用いたか、バイアステストをどのように実施したかの文書化
- **判断プロセスの可視化**: AI がどのような要素を重視して判断しているかを、人事・法務部門が理解し説明できる状態にする
- **エスカレーション手続**: AI の推奨に疑問がある場合や、応募者から問い合わせがあった場合の対応プロセスの整備
- **定期的なレビュー**: AI の判断結果を定期的に分析し、意図しない差別的効果が生じていないかをモニタリング

6.4. 実務上の核心的相違: 事前適合 vs 事後説明

このケーススタディが示す最も重要な違いは、タイミングと責任の所在です。

(1) EU のアプローチ

EU では、企業は市場投入前またはシステム運用開始前に、高リスク要件を満たしていることを実証しなければなりません。構造化された文書と適合性評価が中心的な役割を果たします。

この枠組みは、初期コストは高いものの、規制当局との関係において防御的な立場を確保できます。

(2) 日本のアプローチ

日本では、システムの運用開始に際して AI 特有の障壁はありませんが、問題が生じた際に、既存法に照らして合理的であったことを事後的に説明する責任が企業にあります。

この枠組みは、柔軟性と速度を提供しますが、事後的なリスクを自ら管理する能力が企業に求められます。

(3) 両市場で同一ツールを展開する戦略

両市場で同じ採用 AI ツールを展開する企業にとって、効果的な戦略は以下の通りです。

① 設計段階から EU 高リスク要件を意識: リスク管理、データガバナンス、透明性をシステム設計に組み込む

② 日本固有の論点を別途確認: 個人情報保護法の利用目的特定、労働法上の慣行、人事部門との協議

③ 文書化を共通基盤とする: EU で求められる技術文書は、日本でも事後的説明の基礎として有用

7. 企業が取るべき実務対応

本章では、EU と日本の両市場で AI を活用する企業が、実務上どのような対応を取るべきかを整理します。

7.1. EU 基準を軸としつつ、日本の個別論点を見落とさない

EU AI 法の高リスク要件は詳細かつ包括的であり、これを満たす体制を構築することで強固なガバナンス基盤が得られます。リスク管理プロセス、データガバナンス、技術文書、人間による監視メカニズムは、日本を含む他市場でも有益です。

ただし、EU 適合だけでは不十分です。個人情報保護法の詳細要件(利用目的の特定、

第三者提供、開示請求対応等)、労働法制における慣行、業界自主規制、消費者保護法制における表示規制といった日本固有の論点は別途検討が必要です。

7.2. 早期段階での AI 利用場面の洗い出しとリスク評価

企業は、AI の出力が個人・顧客・取引先にどのような影響を与えるか、雇用・信用・価格設定・適格性判断など高影響領域での利用か、大量の個人情報を処理するか、自動化の程度(人間の関与の余地)といった観点から、AI 利用場面を早期に特定しリスク評価を行うべきです。

早期評価により、EU 高リスク分類該当の可能性予測、日本で適用される既存法制の特定、設計段階からのコンプライアンス組込みによる手戻り最小化が可能になります。

7.3. 説明可能性と文書化への投資

EU では高リスク AI について技術文書と透明性が明示的な義務です。日本でも、行政指導、監査、苦情対応、訴訟リスクに備えて説明可能性は実務上不可欠です。

AI システムの設計意図と限界、訓練データの出所と品質、バイアステストの実施方法と結果、人間による監視・介入の仕組み、インシデント対応手順といった事項を文書化すべきです。文書化は単なる規制対応ではなく、内部意思決定の質向上、インシデント時の迅速対応、関係者とのコミュニケーション基盤として機能します。

7.4. 執行環境の違いへの備え

EU では明示的なルールベースの執行と重大な制裁が想定されるため、法令遵守を実証できる証拠の整備、監督当局の照会・調査への対応体制、違反リスクの早期発見と是正のための内部監査を準備すべきです。

日本では関係性重視・裁量的執行が中心であり、規制当局との良好な関係構築、業界動向への注視、公表や行政指導のリスク評価、レピュテーション管理に注意が必要です。AI 特有の制裁はなくとも、既存法令違反や公表措置による影響は軽視できません。

7.5. 法務アドバイザーの戦略的活用

AI 規制対応では、企画段階での利用場面のリスク評価と規制適用可能性判断、設計段階でのガバナンスメカニズム組込みとデータ取得方法の適法性確認、開発段階での文書化の並行実施、市場投入前の EU 適合性評価と日本既存法制への最終確認が重要です。

EU 向けには早期からの体系的関与により後の設計変更・文書追加コストを削減でき、日本向けには定期的レビューとガイドライン・執行動向のモニタリングが効果的です。

8. おわりに: クロスボーダーAI 戦略の構築に向けて

EU と日本は、AI の台頭に対して、その制度設計において対照的なアプローチを選択しました。EU AI 法は、包括的で拘束力のあるリスクベースの枠組みを通じて、事前統制と市場全体での統一性を優先しています。日本の AI 推進法は、政策主導のアプローチを採り、既存法制と行政実務を通じてリスクに対応しつつ、イノベーションを促進することを選びました。

クロスボーダーで AI ビジネスを展開する企業にとって、いずれのモデルも無視することはできません。両規制がどのように機能し、既存法制とどのように相互作用するかを理解することは、責任ある AI 活用と競争力維持の両立に不可欠です。

AI 技術と規制環境が進化を続ける中、先を見越した戦略的な法務対応が、持続可能な AI 事業の中核的要素であり続けるでしょう。

参考資料

本稿の執筆に際しては、以下の資料を参照しました。

EU AI Act 関連

EU Artificial Intelligence Act 公式サイト:
https://artificialintelligenceact.eu/implementation-timeline/

日本の AI 規制関連

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(法令データ):
https://laws.e-gov.go.jp/law/507AC0000000053

同法律の概要(日本法令外国語訳):
https://www.japaneselawtranslation.go.jp/outline/168/905R744.pdf

AI 関連技術の研究開発・活用の推進に関する法律が全面施行，政府広報オンライン(2025 年 11 月):
https://www.gov-online.go.jp/hlj/ja/november_2025/november_2025-08.html

国際的な比較分析

Understanding Japan's AI Promotion Act: An "Innovation-First" Blueprint for AI Regulation, Future of Privacy Forum:

https://fpf.org/blog/understanding-japans-ai-promotion-act-an-innovation-first-blueprint-for-ai-regulation/
How Japan is regulating AI: Inside the AI Promotion Act, Nemko Digital: https://digital.nemko.com/regulations/ai-regulation-japan

本稿は、2026 年 1 月時点での情報に基づいており、今後の法改正や執行実務の変化により内容が変わる可能性があります。個別の案件については、専門家にご相談ください。