岩田合同法律事務所 ニュースレター
2026 年 9 月

情報・テクノロジー

# 【連載】AI 関連法務シリーズ
# 第 2 回：EU AI 規制法の最新動向
# （2026 年改正と実務上の留意点）

弁護士　草留　夕雅

第 1　はじめに
第 2　前提の確認――AI 規制法の基本構造
　1　規制対象とリスクベース・アプローチ
　2　適用主体と域外適用
　3　制裁金
　4　ガイドライン等
第 3　2026 年改正法の主な内容
　1　適用時期の変更
　2　AI リテラシー義務の修正
　3　ハイリスク AI システムの範囲と重複規制の調整
　4　AI バリューチェーン上の協力及び契約
　5　基本的権利の保護及び監督体制に関する変更
第 4　日本企業における実務上の留意点
　1　AI マッピングと適用関係の再確認
　2　ハイリスク AI システム該当性の判断と技術文書等の準備
　3　生成コンテンツの公表手続を確認する


© IWATA GODO 2026

4　日本の AI 事業者ガイドライン対応との接続
第 5　おわりに

## 第 1　はじめに

EU の AI 規制法（Regulation (EU) 2024/1689）（以下「2026 年改正前 AI 規制法」という。）[1]は、EU 域内に適用される統一ルールを定めることにより、人間中心の信頼できる AI の導入の促進、AI システムの有害な影響に対する基本的権利の高水準の保護及びイノベーションの支援を目的とする法律である。その基本的な枠組みについては、当事務所ニュースレター「欧州 AI 規制法の概要」（2025 年 1 月）で紹介した[2]。また、本連載第 1 回[3]では、日本の AI 推進法及び AI 事業者ガイドラインを中心に、日本の AI 法制の現在地を概観した。

2026 年改正前 AI 規制法は 2024 年 8 月 1 日に発効し、各規定が段階的に適用されてきた。その後、EU は、実施負担の軽減、法的明確性の向上及び監督体制の整理を目的として、Regulation (EU) 2026/1744（Digital Omnibus on AI。以下「2026 年改正法」という。）[4]を制定した（2026 年改正法前文(2)(3)）。2026 年改正法は 2026 年 7 月 8 日に採択され、同月 24 日に EU 官報に掲載され、同月 27 日に発効された（2026 年改正法 4 条参照）[5]。

2026 年改正法により、ハイリスク AI システムに関する主要な規律の適用時期は延期された。もっとも、Regulation (EU) 2026/1744 適用後の Regulation (EU) 2024/1689（以下「AI 規制法」という。）[6]に関しては、2026 年 8 月 2 日から透明性義務、禁止される AI の利用行為、AI リテラシー義務及び汎用目的型 AI モデルに関する規律の適用が開始されている（AI 規制法（以下法名略）113 条 (a)号・(b)号参照）。

本稿では、2026 年 9 月 14 日を基準日として、AI 規制法の基本構造を確認したうえで、2026 年改正法のうち日本企業に関係し得る事項、既に適用が始まった規律及び実務上の留意点を整理する。

## 第 2　前提の確認――AI 規制法の基本構造

[1] Regulation (EU) 2024/1689（https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:02024R1689-20260727）
[2] 岩田合同法律事務所「欧州 AI 規制法の概要」（2025 年 1 月）（https://www.iwatagodo.com/publications/uploads/file/NL2501_DT.pdf）
[3] 岩田合同法律事務所「【連載】AI 関連法務シリーズ　第 1 回：日本の AI 法制の現在地（AI 推進法・AI 事業者ガイドラインを中心に）」（2026 年 8 月）
[4] Regulation (EU) 2026/1744（Digital Omnibus on AI）（https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202601744）
[5] 改正に関するタイムラインにつき、European Commission, Timeline for the Implementation of the EU AI Act（https://ai-act-service-desk.ec.europa.eu/en/ai-act/timeline/timeline-implementation-eu-ai-act）参照。
[6] 全文につき、The Future of Life Institute (FLI) , Regulation (EU) 2024/1689 The AI Act Explorer（https://artificialintelligenceact.eu/ai-act-explorer/#article-1）参照。


© IWATA GODO 2026

## 1　規制対象とリスクベース・アプローチ

AI 規制法は、「AI システム」と「汎用目的型 AI モデル（General-purpose AI model。以下「GPAI モデル」という。）」を規制対象としている。AI システムとは、様々なレベルの自律性で動作するよう設計され、導入後に順応性を示す可能性のある機械ベースのシステムであって、明示又は黙示の目的のため、受け取ったインプットから、現実の又は仮想の環境に影響を与え得る予測、コンテンツ、推奨又は決定等のアウトプットを生成する方法を推論するものをいう（3 条 1 号）。GPAI モデルとは、大きな汎用性を示し、市場投入の方法にかかわらず広範で異なるタスクを有能に実行することができ、様々な川下のシステム又はアプリケーションに統合することができる AI モデルをいい、市場投入前の研究、開発又はプロトタイピング活動に用いられるものを除く（3 条 63 号）。

AI システムについては、それが生み出すリスクの強度と範囲に応じて規制内容を調整するリスクベース・アプローチが採用されており、リスクレベルは 4 段階に分類される。

**表 1：AI 規制法におけるリスク分類[7]**

| リスクレベル | リスクレベルの概要・具体例 | 規制内容 |
|---|---|---|
| 許容できないリスク（Unacceptable Risk） | 生命や基本的人権に対して直接的な脅威をもたらすと考えられる AI システム。<br>例：サブリミナル技術、ソーシャルスコアリング | 原則禁止（5 条 1 項） |
| ハイリスク（High Risk） | 健康や安全、基本的人権等に影響を与える可能性がある AI システム。附属書 I 型（医療機器、玩具、昇降機等の製品の安全構成要素等）と附属書 III 型（雇用・人事、教育、信用評価、重要インフラ、生体認証等の独立型ユースケース）の二系統がある（6 条 1 項・2 項、附属書 I、附属書 III） | リスク管理体制、データガバナンス、技術文書の作成、人間による管理、適合性評価手続、ログ保存等の厳格な義務（8 条から 15 条まで、16 条） |
| 特定の透明性のリスク（Specific Transparency Risk） | 自然人とやり取りする AI に係る AI システム、生成 AI、感情認識システム、生体分類システム等（50 条 1 項から 4 項まで） | AI により生成されたコンテンツである旨の標識や AI 使用の告知等の情報提供・透明性義務（50 条） |
| 最小リスク（Minimal Risk） | 上記以外。なお AI 規制法に「最小リスク」の定義はない。 | 制限なし。ただし、AI リテラシー義務や自主的な行動規範の推奨あり（4 条、95 条） |

[7] 前掲「欧州 AI 規制法の概要」参照。


© IWATA GODO 2026

なお、附属書 III に掲げる AI システムであっても、意思決定の結果に重大な影響を与えないことを含め、自然人の健康、安全又は基本的権利を害する重大なリスクを示さない場合には、ハイリスクなものとはみなされない（6 条 3 項）。すなわち、①手続上の狭いタスクの実行を目的とする場合、②以前に行われた人間の活動の結果の改善を目的とする場合、③意思決定パターン又は以前の意思決定パターンからの逸脱の検知を目的とし、かつ、人間による適切な検証なく、以前に行われた人間の評価に置き換えることや、それに影響を与えることを目的とするものでない場合、④附属書 III に掲げる利用事例の目的に関する評価のために準備タスクを実行することを目的とする場合である（同項(a)号から(d)号まで）。ただし、自然人のプロファイリングを実行する AI システムは、常にハイリスクなものとみなされる。附属書 III に規定される AI システムが高リスクではないと判断した提供者は、市場投入又は運用開始前にその評価を文書化し、登録義務を負う（6 条 4 項、49 条 2 項）。特に、人事採用、与信審査、保険引受等に用いるシステムは附属書 III の射程に入る可能性が相応にあるため、当該システムが、ハイリスク AI システムに該当するか否か、及び、該当するとしても、上記除外に依拠し得るか否かの判断は早期に行い、上記除外に依拠する場合には、当該判断について記録に残す必要がある。

6 条の実務的適用を明確化する欧州委員会ガイドラインは現時点で採択されていない[8]が、ガイドライン案は、附属書 I 型の分類を第 3 章で、附属書 III 型の分類を第 4 章で解説しており、6 条 3 項に基づきハイリスクとはみなされない要件の解釈及び具体例も要素を区切って示されている。特に、採用や選考、職場における従業員等の管理に AI システムを用いる場合について、附属書 III 第 4 項に該当する範囲が広く解釈されている点は、AI を実装した HR テックを利用する日本企業に広範な影響を及ぼし得る[9]。

これに対し、50 条の透明性義務に関するガイドライン（Guidelines on transparency obligations for providers and deployers of AI systems 。以下「透明性義務に関するガイドライン」という。）[10]は、2026 年 8 月 2 日から適用が開始されている[11]。本ガイドラインは法的拘束力を有さないが、

---

[8] ただし、ガイドライン案として、European Commission, Draft guidelines on the classification of high-risk AI systems（2026 年 5 月 19 日公表）（https://digital-strategy.ec.europa.eu/en/library/draft-commission-guidelines-classification-high-risk-ai-systems）が公表されている。なお、最終ガイドラインは 2026 年末までに採択予定である（European Commission, Targeted consultation on the draft guidelines for the classification of high-risk artificial intelligence systems（https://digital-strategy.ec.europa.eu/en/consultations/targeted-consultation-draft-guidelines-classification-high-risk-artificial-intelligence-systems）。

[9] ガイドライン案の内容の詳細な分析として、石川＝服部＝山﨑「EU AI 法：2026 年以降のガイドライン類のアップデートと、今後の動向を踏まえた実務対応――透明性義務・ハイリスク AI システムの分類に関するガイドライン案の公表と透明性義務に係る行動規範の最終版の確定――」（西村あさひ法律事務所、ヨーロッパニューズレター2026 年 7 月 13 日号）（https://www.nishimura.com/sites/default/files/newsletters/file/europe_260713_ja.pdf）参照。

[10] European Commission, Guidelines on transparency obligations for providers and deployers of AI systems（https://digital-strategy.ec.europa.eu/en/library/guidelines-transparency-obligations-providers-and-deployers-ai-systems）

[11] Guidelines on transparency obligations for providers and deployers of AI systems のほか、European Commission, Code of Practice on Transparency of AI-generated Content（https://digital-strategy.ec.europa.eu/en/policies/code-practice-ai-generated-content#1720699867912-1）参照。


© IWATA GODO 2026

各国所轄当局及び AI オフィスの運用指針となることが見込まれる。

## 2　適用主体と域外適用

AI 規制法の適用を受ける主体は 2 条 1 項に列挙されており、EU 域内に拠点を持たない日本企業は、主に、①EU 域内において、AI システムを市場に投入する又は運用を開始する、又は GPAI モデルを市場に投入する提供者（提供者の設立場所・所在地が EU 域内か否かを問わない）、及び、②AI システムによって生成されたアウトプットが EU 域内で利用される場合における、EU 域外において設立され又は所在する AI システムの提供者及び導入者の類型に該当し、域外適用を受ける可能性がある。このほか、EU 域内において設立され又は所在する導入者、輸入者及び流通事業者、並びに、自社の名称・商標の下で自社の製品と共に AI システムの市場投入や運用開始をする製品製造者も適用対象に含まれる。

## 3　制裁金

違反に対する制裁として、違反類型に応じて、全世界売上ベースでの制裁金が課され得る（99 条、101 条）。禁止される AI の利用行為（5 条）に違反した場合は、3,500 万ユーロ又は前会計年度の世界年間総売上高の 7%のいずれか高い方を上限とする制裁金が課される（99 条 3 項）。提供者の義務（16 条）、正規代理人の義務（22 条）、輸入者の義務（23 条）、流通事業者の義務（24 条）、AI バリューチェーン上の提供者その他のオペレータの義務（25 条 2 項及び 4 項）、導入者の義務（26 条）並びに提供者及び導入者の透明性義務（50 条）に違反した場合は、1,500 万ユーロ又は前会計年度の世界年間総売上高の 3%のいずれか高い方が上限となる（99 条 4 項）。認証機関又は各国所轄当局に対する不正確、不完全又は誤導的な情報の提供については、750 万ユーロ又は 1%が上限とされる（99 条 5 項）。GPAI モデルの提供者に対しては、欧州委員会が、前会計年度の世界年間総売上高の 3%又は 1,500 万ユーロのいずれか高い方を上限とする制裁金を課し得る（101 条 1 項）[12]。

中小企業（SME。従業員数 250 人未満その他の一定の要件を満たす事業者）[13]については、99 条 3 項から 5 項までの金額又は割合のいずれか低い方が上限となり（99 条 6 項）、2026 年改正法により新設された 99 条 6a 項は、小規模中堅企業（SMC。従業員数 750 人未満その他の一定の要件を満たす事業者）[14]について同 4 項及び 5 項の金額又は割合のいずれか低い方を上限とする（99 条 6a 項）。

[12] European Commission, AI Act Service Desk, Article 101: Fines for providers of general-purpose AI models（https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-101）
[13] Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises（https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32003H0361#:~:text=%282003%2F361%2FEC%29）
[14] Commission Recommendation (EU) 2025/1099（https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202501099#:~:text=Done%20at%20Brussels%2C%2021%20May%202025.）


© IWATA GODO 2026

## 4　ガイドライン等

2026 年 9 月 14 日時点における、AI 規制法に関連するガイドライン等の状況は下表のとおりである。

| 正式名称 | 概要 | 公表、採択等の状況 |
|---|---|---|
| Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act) | 禁止 AI（5 条）について、要件、例外、実務例等を示している。 | 2025 年 2 月 4 日に採択・公表済み。 |
| Guidelines on the definition of an artificial intelligence system established by Regulation (EU) 2024/1689 (AI Act) | 「AI system」（3 条 1 項）の構成要素を解説し、ソフトウェアが AI 規制法の適用対象となるかを判断するための実務的基準を示している。 | 2025 年 2 月 6 日に採択・公表済み。 |
| Guidelines on the scope of the obligations for providers of general-purpose AI models established by the AI Act | GPAI 規制（3 条、51～55 条）に関する概念を整理し、その適用範囲を明確化している。 | 2025 年 7 月 18 日に採択・公表済み。 |
| General-Purpose AI Code of Practice | 56 条に基づく、GPAI 規制に関する Code of Practice（行動規範）。透明性及び著作権（並びに、システミックリスクを伴う GPAI モデルについては、安全性とセキュリティ）に関する論点について実務的基準を示している。 | 2025 年 7 月 10 日に最終版が公表され、同年 8 月 1 日に欧州委員会及び AI Board が適切なコンプライアンス手段であると評価済み。 |


© IWATA GODO 2026

| 正式名称 | 概要 | 公表、採択等の状況 |
|---|---|---|
| Code of Practice on Transparency of AI-generated Content | 透明性義務（50 条）の一部の類型に関する Code of Practice（行動規範）。Section 1 は提供者による AI 生成・操作コンテンツの機械可読なマーキングと検出、Section 2 は導入者によるディープフェイク及び一定の公益事項に関する AI 生成テキストのラベリングを取り扱っている。 | 2026 年 6 月 10 日に最終版が公表され、同年 7 月 9 日に欧州委員会及び AI Board が適切なコンプライアンス手段であると評価済み。 |
| Guidelines on the implementation of the transparency obligations for certain AI systems under Article 50 of the AI Act | 透明性義務（50 条）について、要件、例外、実務例等を示している。 | 2026 年 7 月 20 日に採択・公表済み。 |
| Draft Guidance on Article 73 AI Act — Incident Reporting / Incident Report for Serious Incidents under the AI Act (High-risk AI Systems) | ハイリスク AI システムの重大インシデント報告（73 条）について、定義、具体例、報告期限、他の EU 報告制度との関係を整理し、共通報告様式を示している。ドラフトであり、最終版ではない。 | 2025 年 9 月 26 日にドラフトが公表され、同年 11 月 7 日まで意見公募に付されていた。 |
| Draft Guidelines on the classification of high-risk artificial intelligence systems | ハイリスク AI システム規制（6 条及び附属書 I・III）について、製品組込み型 AI 及び特定分野・ユースケースの AI がハイリスク AI システムに該当するかを判断するための説明と実例を示している。ドラフトであり、最終版ではない。 | 2026 年 5 月 19 日にドラフトが公表され、2026 年 7 月 23 日まで意見公募に付されていた。最終版は 2026 年末までに採択予定。 |

## 第 3　2026 年改正法の主な内容

### 1　適用時期の変更

2026 年改正法は、113 条を改正し、ハイリスク AI システムに関する第 III 章第 1 節から第 3 節


© IWATA GODO 2026

まで（6 条 5 項を除く。）の適用日を、6 条 2 項及び附属書 III に従ってハイリスクに分類される AI システムについては 2027 年 12 月 2 日、6 条 1 項及び附属書 I に従ってハイリスクに分類される AI システムについては 2028 年 8 月 2 日とした（113 条(c)号(i)・(ii)）。改正後の主な適用日程は、次のとおりである。

**表 2：2026 年改正法の主な適用スケジュール（2026 年 9 月 14 日現在）[15]**

| 適用日 | 状況 | 主な規律 |
|---|---|---|
| 2026 年 8 月 2 日 | 適用済み | 一般適用日（113 条） |
| 2026 年 12 月 2 日（予定） | 今後適用 | ・新たな禁止類型（5 条 1 項 (ba)号・(bb)号、5 条 1a 項・1b 項）（113 条 (a)号）<br>・2026 年 8 月 2 日より前に市場投入された生成 AI システムに係る 50 条 2 項遵守の期限（111 条 4 項） |
| 2027 年 8 月 2 日（予定） | 今後適用 | ・2025 年 8 月 2 日より前に市場投入された既存 GPAI モデルに関する経過措置の期限（111 条 3 項）<br>・重複規制の調整に係る委任法令の制定期限（2 条 13 項）<br>・国内の正規 AI サンドボックスの稼働期限（57 条 1 項） |
| 2027 年 12 月 2 日（予定） | 今後適用 | 附属書 III 型（6 条 2 項）のハイリスク AI システムに関する第 III 章第 1 節から第 3 節まで（6 条 5 項を除く）の適用（113 条 (c)号(i)） |
| 2028 年 8 月 2 日（予定） | 今後適用 | 附属書 I 型（6 条 1 項）のハイリスク AI システムに関する第 III 章第 1 節から第 3 節まで（6 条 5 項を除く）（113 条 (c)号(ii)） |

（表 2 注）このほか、市販後モニタリング計画に関する欧州委員会ガイダンスは 2027 年 9 月 2 日までに採択される（72 条 3 項）。附属書 I 第 A 節の EU 調和法に基づき認定された認証機関は、2028 年 1 月 28 日までに AI 規制法に基づく認定を申請する必要がある（43 条 3 項）。附属書 I 掲記のハイリスク AI システムの事業者向け欧州委員会ガイドラインは、遅くとも 2027 年 8 月 1 日までに公表される（2026 年改正法前文(37)）。

なお、既存のハイリスク AI システムについては、AI 規制法上のハイリスク AI システムに関する規制を直ちに全面適用すると、既存システムの改修、再評価、適合性評価等について事業者に大きな負担が生じることから、同規制の適用が猶予されている（111 条 2 項）。具体的には、AI 規制法 113 条に基づく各ハイリスク AI 類型の適用日前に市場投入又は使用開始されたハイリスク AI システムについては、同日後に設計上の重大な変更がない限り、関連するハイリスク AI システ

[15] 2026 年改正法参照。


© IWATA GODO 2026

ム規制が適用されない。この点、2026 年改正法前文(39)は、AI 規制法 111 条 2 項の猶予について、当該ハイリスク AI システムの少なくとも 1 個体が同項所定の日より前に適法に市場投入されていれば、同一の型式及びモデルの他の個体も猶予の対象となり、設計が変更されない限り追加の義務を負わないとする一方、同日後に設計に重大な変更が加えられた場合には適合性評価要件を含む全ての関連規定を遵守する義務が生じるとする。既に EU 市場で稼働している型式・モデルについては猶予の利益を確認し、設計変更の管理手続を整備することが具体的な課題となる。

## 2　AI リテラシー義務の修正

2026 年改正前 AI 規制法 4 条は、提供者及び導入者に対し、従業員等に対し、可能な限り十分なレベルの AI リテラシーが確保されるよう措置を講じる義務を定めていた（…“shall take measures to ensure, to their best extent, a sufficient level of AI literacy of their staff”…）。しかし、2026 年改正によって、提供者及び導入者の義務は職員等の AI リテラシーの発達を支援する措置を講ずる義務(…”shall take measures to support the development of AI literacy of their staff”…)とされ、また、当該義務は、個人について特定のレベルを保証する義務ではないことが明記された（4 条 1 項。なお、提供者及び導入者の技術的知識、経験、教育及び訓練、利用される文脈並びに対象者を考慮するという要素は維持されている。）。欧州委員会は遵守方法の実例を単一情報プラットフォーム上で公表するものとされ、欧州 AI 委員会（AI Board）は共通目標を含む勧告を採択するものとされている（4 条 2 項・3 項）。なお、4 条のリテラシー要件は、50 条の適用対象となる AI システムの提供者及び導入者にも及ぶ（透明性義務に関するガイドライン(25)）。

AI 規制法 4 条の下でも、職員等の AI リテラシーの発達を支援する措置として研修その他の措置が求められ、当該措置の例としては、AI システムの使用に関する社内規則の策定、役職員に対する研修、並びに担当部署・担当者及び社内相談窓口の設置等が考えられる。日本の AI 事業者ガイドラインに基づく社内研修を実施している企業であれば、その枠組みに EU 向けの利用場面を追加して設計することが効率的である。

## 3　ハイリスク AI システムの範囲と重複規制の調整

附属書 I 型のハイリスク AI システムに関しては、「安全構成要素」（safety component）の定義及び判断基準が明確化された（3 条 14 号）。利用者支援、性能最適化、業務効率化、自動化、利便性又は品質管理の安全性に関連しない側面のためだけに用いられる AI システムは、原則として安全構成要素に該当しない（6 条 1a 項）。ただし、その故障又は誤作動が健康・安全を危険にさらす場合は、安全構成要素に該当する（同条 1b 項）。また、健康・安全以外のリスク（電波の分配や電磁干渉等）のみを理由として第三者による適合性評価が要求される製品は、6 条 1 項(b)号の要件を満たさないものとされる（同条 1c 項）。これらを踏まえると、製造業においては、例えば、工場内で用いる AI が「品質管理目的」か「安全確保目的」かという区分が、規制類型を分けるうえで重要となり得る（2026 年改正法前文(7)参照）。なお、ハイリスク AI システムの分類に関


© IWATA GODO 2026

するガイドライン案は、「安全機能」が AI システムの意図目的に基づき判断されるのに対し、「故障又は誤作動」は当該システムが故障又は誤作動した場合の結果に基づき判断されるとしており、安全構成要素の範囲は相応に広くなると考えられる[16]。

また、附属書 I 第 A 節の EU 調和法（Union harmonisation legislation）が AI 規制法と同等以上の保護を与え、保護水準を低下させない場合には、欧州委員会が委任法令により 9 条から 15 条まで及び 17 条から 25 条までの特定の要求事項又は義務の適用を限定できる仕組みが導入された（2 条 13 項、2026 年改正法前文(5)）。具体的な対象及び限定範囲は、2027 年 8 月 2 日までに制定される委任法令を待つ必要がある（2 条 13 項）。そのほか、簡易な技術文書（11 条 1 項）及び品質管理体制の比例的な実施（17 条 2 項）等の措置が中小企業又は小規模中堅企業に拡張された。さらに、サイバーレジリエンス法（Regulation (EU) 2024/2847）[17]12 条 1 項の要件を満たす場合に AI 規制法 15 条に定めるサイバーセキュリティ要件への適合が推定される規定が新設された(42 条 3 項、2026 年改正法前文(19))。

## 4　AI バリューチェーン上の協力及び契約

既存の AI システムに自己の名称・商標を付し、実質的な変更を加え、又は意図目的を変更してハイリスク AI システムとした事業者は、一定の場合に新たな提供者として扱われる（25 条 1 項(a)号から(c)号まで）。2026 年改正法は、この場面で、当初の提供者が、新たな提供者による義務履行に必要な技術文書、既知の限界・不具合態様、試験・検証のための技術的アクセス等を提供して協力すべきこと（…"shall closely cooperate with new providers and shall make available the necessary information and provide the reasonably expected technical access and other assistance"…）を具体化した（25 条 2 項。ただし、当該協力義務の存在は、知的財産権、秘密情報及び営業秘密の保護の必要性を低減させるものではない（同条 5 項）。）。もっとも、当初の提供者が、その AI システムがハイリスク AI システムに変更されるべきものではないことを明確に特定している場合には、この協力義務は適用されない（同条 2 項）。したがって、第三者由来の AI システムをハイリスク AI システムに変更する場合には、当初の提供者による利用条件や技術文書等に当該特定がないかを確認する必要があろう。

さらに、ハイリスク AI システムの提供者と、そのシステムに用いられ、又は組み込まれる AI システム、AI モデル、ツール、サービス、構成要素又はプロセスを供給する第三者は、提供者が AI 規制法上の義務を履行するために必要な情報、能力、技術的アクセスその他の支援を書面による合意で定めなければならない(25 条 4 項)。ただし、当該書面合意義務は、GPAI モデル以外のツール、サービス、プロセス又は構成要素を、フリーでオープンソースのライセンスに基づき公衆に提供する第三者には適用されない。

---

[16] 前掲「EU AI 法：2026 年以降のガイドライン類のアップデートと、今後の動向を踏まえた実務対応――透明性義務・ハイリスク AI システムの分類に関するガイドライン案の公表と透明性義務に係る行動規範の最終版の確定――」参照。

[17] Regulation (EU) 2024/2847（https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng）


© IWATA GODO 2026

前記のとおり、これらの協力義務又は書面合意義務の違反は 1,500 万ユーロ又は前会計年度の世界年間総売上高の 3%のいずれか高い方を上限とする制裁金の対象とされた（99 条 4 項(da)号）。

## 5　基本的権利の保護及び監督体制に関する変更

### (1)　バイアスの検出・訂正のための特別な種類の個人データの処理

2026 年改正法は 4a 条を新設し、ハイリスク AI システムの提供者が、バイアスの検出及び訂正のために厳密に必要な範囲で、特別な種類の個人データを例外的に処理できる根拠を定めた。同条に基づき特別な種類の個人データを処理するには、合成データ又は匿名化されたデータでは目的を達成し得ないこと、変名にすることを含む最先端の安全・プライバシー保護措置、アクセスの厳格な管理及び文書化、他の当事者への送信・転送及び他の当事者によるアクセスの禁止、バイアスの訂正後又は保存期間の終了後の消去、並びに取扱活動の記録における必要性の理由の記載といった条件を全て満たす必要がある（4a 条 1 項各号）。同条 2 項は、ハイリスク AI システム以外の AI システム・モデルの提供者及び導入者並びにハイリスク AI システムの導入者にも同様の根拠を拡張する一方、当該各主体がバイアスの検出及び訂正を実施すべき義務を創設するものではない旨を明記している。また、別途 GDPR 等の双方の要件を別個に検討する必要がある（改正法前文(9)、AI 規制法 2 条 7 項、同法 4a 条 1 項柱書参照）。

### (2)　自然人・児童の性的素材を生成・操作する AI の禁止

また、2026 年 12 月 2 日からは、禁止される AI（上記第２・１表１「許容できないリスク」参照）として、有効な本人の同意なく、識別可能な自然人の身体の秘部又は性的に露骨な行為に従事する当該自然人の写実的な素材を生成・操作する AI システム、及び児童性的虐待素材を生成・操作する AI システムが追加される（5 条 1 項(ba)号・(bb)号）。ただし、2026 年改正法前文(12)は、禁止措置は提供者による AI システムの技術的能力の開発を妨げるものであってはならないとしており、提供者については、当該生成・操作が意図目的である場合のほか、合理的に予見可能かつ再現可能であり、十分な技術的安全措置その他の保護措置を欠く場合が対象となり得る（5 条 1a 項(a)号(i)・(ii)、2026 年改正法前文(12)）当該保護措置の例として、2026 年改正法前文(12)は、データクリーニング、拒否学習、安全なプロンプト設計及び出力管理、ランタイム・プロンプト・ガードレール、コンテンツ分類・フィルタリング機構、利用制限、誤用検知機構並びに通知・対応機構を挙げている。導入者については、当該生成・操作を目的として当該 AI システムを利用する場合に限り禁止規制に違反したと評価され得る（5 条 1a 項(b)号、2026 年改正法前文(12)）。既存素材の操作のうち、秘部の露出度を増加させず性的行為の性質を変更しないものは「操作」に当たらない（同条 1b 項）。違反した場合の制裁金は最も重い水準である（3,500 万ユーロ又は前会計年度の世界年間総売上高の 7%のいずれか高い方を上限とする。）（99 条 3 項）。

上記のとおり、提供者については、自然人・児童の性的素材の生成・操作が、当該 AI システムの意図された目的でなくても、十分な技術的安全措置その他の保護措置を欠く等の一定の要件を満たす場合には、禁止規制に違反したと評価される点を踏まえると、画像・音声生成機能を提供


© IWATA GODO 2026

する事業者は、少なくとも 2026 年 12 月 2 日までに保護措置の実装状況を点検する必要があろう。

(3)　AI オフィスの権限の強化

AI オフィスとは、AI システム及び GPAI モデルの実施、監視及び監督並びに AI ガバナンスに貢献するための欧州委員会の機能をいう（3 条 47 号）。2026 年改正法により、①GPAI モデルに基礎を置く AI システムであって、モデルとシステムが同一の提供者又は同一の事業体（undertaking）に属する提供者により開発されたもの（例外規定あり）、及び、②Regulation (EU) 2022/2065 に基づき指定された超大規模オンラインプラットフォーム又は超大規模オンライン検索エンジンを構成し又はこれらに統合された AI システムに関する提供者（及び、当該提供者と同一の事業体に属する導入者）の義務について、一定の例外を除き、AI オフィス（AI Office）に監督・執行権限を集中させることとなった（75 条 1 項）。また、同改正法により、情報請求、立入検査、調査、是正措置、制裁金、定期的支払命令等に係る AI オフィスの権限も新設された（75a 条から 75d 条）。

## 第 4　日本企業における実務上の留意点

### 1　AI マッピングと適用関係の再確認

最初に取り組むべきは、自社が開発、提供又は利用する AI システムの棚卸し、すなわち AI マッピングである[18]。棚卸しに当たっては、システム名、用途、EU 域内での市場投入・運用開始の有無、アウトプットの EU 域内での利用の有無、自社の立場、リスク分類、適用日、対応責任者、根拠資料等を一覧化した社内対応表を作成することが有用と考えられる。社内対応表では、適用済みの義務と将来適用される義務を明確に区別し、前者については直ちに遵守状況を点検する必要がある。2026 年 9 月 14 日時点で、透明性義務、GPAI モデル規律、禁止される AI の利用行為及び AI リテラシー義務については、原則として、既に適用が開始されている。特に生成 AI の社内利用が部門単位で進んでいる企業等では、法務部門が把握していないツールが存在することも多いため、棚卸しは事業部門への照会を伴う形で行うことが望ましい。例えば、職場及び教育機関内において、感情推定を含む従業員のエンゲージメント測定、オンライン会議における表情分析といった用途で AI を利用することは、EU 域内の従業員を対象とする限り、医療上又は安全上の理由による利用が意図されている場合を除き、原則として禁止類型（5 条 1 項(f)号）に該当し得る。このように、日本国内では欧州に比して相対的に緩やかな基準により許容され得る類型であっても、AI 規制法の問題が生じ得ることが想定され、グループ共通の HR ツールを欧州拠点に展開する場面で問題が顕在化しやすい。

### 2　ハイリスク AI システム該当性の判断と技術文書等の準備

[18] 前掲「欧州 AI 規制法の概要」（2025 年 1 月）参照。


© IWATA GODO 2026

ハイリスク AI システム該当性については、附属書 I／附属書 III のいずれに該当する AI システムかを確定したうえで、6 条 3 項の除外事由の適否を検討する（6 条 1 項ないし 4 項）。判断に当たっては、ハイリスク AI システムの分類に関するガイドライン案が掲げる具体例が参考となり得る。

(1) 提供者側の準備

ある AI システムがハイリスク AI システムに該当する場合、提供者には、リスク管理体制（9 条）、データ及びデータガバナンス（10 条）、技術文書（11 条・附属書 IV）、記録保存及び管理下にある場合の自動生成されたログの保存（12 条・19 条）、導入者に対する使用説明書の提供（13 条）、人間による管理（14 条）、精度・堅牢性・サイバーセキュリティの確保（15 条）、品質管理体制（17 条）、文書の保管（18 条）、適合性評価（43 条）、EU 適合宣言書（47 条）、CE マーキング（48 条）及び EU データベースへの登録（49 条 1 項）等の一連の義務が課される（16 条参照）。これらは相応の準備期間を要するため、附属書 III に基づくハイリスク AI システムに係る規制の適用日である 2027 年 12 月 2 日から逆算し、例えば 2027 年前半には技術文書のひな形作成とギャップ分析を完了しておくことが考えられる。

また、EU 域内に拠点を持たない提供者は、ハイリスク AI システムを EU 市場において利用に供する前に、書面による委任により、EU 域内に設立された正規代理人を選任する必要がある（22 条 1 項）。正規代理人は、EU 適合宣言書及び技術文書の作成確認、当該文書の 10 年間の保管、所轄当局への情報提供及び協力、登録義務の履行等を担う（同条 3 項）。選定と委任範囲の調整には相応の時間を見込むべきである。

なお、ある会社（A 社）がハイリスク AI システムの提供者である場合において、A 社の欧州グループ会社（B 社）がそのシステムを業務で使用すれば、A 社は提供者としての義務を、B 社は導入者としての義務を、それぞれ負うことになり得るため、グループコンプライアンス担当者としては、提供者の義務だけでなく、導入者の義務にも気を配る必要がある。

(2) 導入者側の準備

導入者がハイリスク AI システムを用いようとする場合、使用説明書に従った利用のための技術的・組織的措置、必要な能力、訓練及び権限並びに必要な支援を備えた自然人への人間による管理の割当て、入力データの関連性及び代表性の確保、運用の監視及び重大インシデントの通知、ログの 6 か月以上の保存、職場での稼働に係る労働者代表及び当該労働者への事前通知、公的機関等による登録義務、データ保護影響評価への情報の活用、附属書 III 型システムによる意思決定の対象となる自然人への通知、並びに所轄当局への協力等の義務を負う（26 条 1 項）。一定の場合には基本的権利に対する影響の分析（FRIA）も求められるが（27 条 1 項）、データ保護影響評価（DPIA）で要件が充足されている場合には相互参照又は取込みが認められる（同条 4 項、46 条参照）。

### 3　生成コンテンツの公表手続を確認する


© IWATA GODO 2026

広告、広報、顧客対応その他の対外発信に生成 AI を用いる場合、提供者が行うべき標識の付与と、導入者が行うべき開示とを混同しないよう、自社がいずれ（ないし両方）に該当するかを確認する必要がある（50 条）。

### 4　日本の AI 事業者ガイドライン対応との接続

上述のとおり、EU AI 規制法は域外適用を伴う規制法であり、違反には高額の制裁金が課され得る（99 条、101 条）。これに対し、日本は、現時点では、AI ガバナンスに関する横断的な法令による行為規制や制裁によるアプローチではなく、民間事業者の自主的な取組を重んじるソフトローアプローチを志向している。すなわち、日本の AI 推進法（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。2025 年 6 月 4 日公布・一部施行、同年 9 月 1 日全面施行）は基本法的性格を有し、個別具体的な行為規制や制裁を定めるものではなく、AI 事業者ガイドライン（第 1.2 版、2026 年 3 月）にも法的拘束力はない。[19]

もっとも、日本の AI 事業者ガイドラインは、リスクの大きさに応じて対策の程度を決定するリスクベース・アプローチを採用しており、この思考枠組み自体は EU AI 規制法と共通するため、同ガイドラインに沿って構築した社内体制（データ収集の適切性の確保、学習データのバイアスへの配慮、安全性の確保、利用上の留意点の設定等）には、EU 対応の土台として活用できる部分もあり得る。ただし、日本の AI 事業者ガイドライン上の「AI 開発者・AI 提供者・AI 利用者」と EU AI 規制法上の「提供者・導入者」とでは概念が異なるなど、両国の法的枠組みには本質的な差異も多く含まれるため、日本向けの社内体制をそのまま EU 向けのものとして流用することはできないことには留意が必要である。

## 第５　おわりに

本稿では、2026 年改正法のうち、企業法務に影響を与え得る事項を概観した。まずは、AI システムごとに自社の立場と適用時期を確認し、現在必要な対応と、将来必要になる対応（ハイリスク AI 対応を含む。）とを分けて検討することが必要になるが、同時に、今後公表されるガイドライン等に関するアップデートを継続してモニタリングすることも肝要である。

[19] 「【連載】AI 関連法務シリーズ　第 1 回：日本の AI 法制の現在地（AI 推進法・AI 事業者ガイドラインを中心に）」参照。


© IWATA GODO 2026

【執筆者】



草留　夕雅（弁護士）
E-mail: yuka.kusadome@iwatagodo.com

2018 年慶應義塾大学法学部卒業、2020 年東京大学法科大学院修了。2022 年弁護士登録、2024 年弁理士登録。2025 年 JPAA 知財経営コンサルタント（日本弁理士会認定）。知的財産（特許、商標、意匠等）に関する鑑定、契約、紛争解決等を専門とし、AI・データを含む先端技術分野に関する紛争予防等も手掛ける。

**岩田合同法律事務所**

1902 年(明治 35 年)、司法大臣や日本弁護士連合会会長を歴任した故・岩田宙造弁護士が「岩田宙造法律事務所」を開設したことに始まる、我が国において最も歴史のある法律事務所の一つです。開設当初より、我が国を代表する企業等の法律顧問として多数の企業法務案件に関与しております。日本法弁護士約 120 名が東京・札幌の両オフィスに所属し、日本語対応も可能な中国法弁護士、フランス法弁護士、米国各州弁護士資格を有する多数の弁護士のほか、特別招聘顧問として元最高裁判所長官大谷直人氏、特別顧問として前公正取引委員会委員長古谷一之氏、前金融庁長官井藤英樹氏が在籍しております。

〒100-6315 千代田区丸の内二丁目 4 番 1 号　丸の内ビルディング 15 階
岩田合同法律事務所　広報：　newsmail@iwatagodo.com

※本ニュースレターは一般的な情報提供を目的としたものであり、法的アドバイスではありません。また、その性質上、法令の条文や出展を意図的に省略している場合があり、また情報としての網羅性を保証するものではありません。個別具体的な案件については、必ず弁護士にご相談ください。


© IWATA GODO 2026