NAGASHIMA OHNO & TSUNEMATSU
長島・大野・常松法律事務所
NO&T Technology Law Update
テクノロジー法ニュースレター

2025年4月
テクノロジー法ニュースレター　No. 60
欧州最新法律情報　No. 34

<AI Update>
欧州AI法「禁止されるAIプラクティス」に関するガイドラインの公表

弁護士　殿村　桂司
弁護士　今野由紀子
弁護士　丸田　颯人

はじめに

2024年8月1日、EUで、世界初となるAIに関する包括的な法規制である「人工知能に関する調和の取れたルールを定める規則（Artificial Intelligence Act）[1]」（以下、「AI法」といいます。）が発効しました。当事務所のニュースレター[2]でも触れているとおり、AI法は厳しい罰則規定を含むものであり、また、EU域内に事業拠点を有しない企業も対象となることから、多くの日本企業にも大きな影響を与えることが予想されます。

AI法は、対象となるAIシステムをそのリスクに応じてカテゴリー分けしてそれぞれ異なる規制を課すリスクベースのアプローチを採用しており、カテゴリーごとに段階的に適用されますが、かかるカテゴリーのうち、もっとも厳しい規制がかかる「禁止されるAIプラクティス（Prohibited AI Practices）」に関する規制については、2025年2月2日から先行して適用が開始されています[3]。そして、適用開始後の同年2月4日、欧州委員会は、禁止されるAIプラクティスに関するガイドライン（以下、「本ガイドライン」といいます。）を公表しました[4]。本ガイドラインは、法的拘束力を持つものではなく、最終的な判断は欧州司法裁判所が行うこととされていますが、AI法が列挙する禁止されるAIプラクティスの内容などの、より詳細な説明や具体例を示すものであり、企業としては本ガイドラインを参照することが有益と考えられます。

本稿では、AI法における禁止されるAIプラクティスの主な内容を概観しつつ、本ガイドラインで明らかとなった内容について、日本企業が留意すべき点とともに示します。

---

[1] 正式名称は、”Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts”。

[2] NO&T Technology Law Update テクノロジー法ニュースレター No.50/NO&T Europe Legal Update 欧州最新法律情報 No.31「<AI Update>「欧州AI法」の概要と日本企業の実務対応」（2024年6月）

[3] 2025年2月2日よりも前から欧州市場に投入などされていたAIシステムにも適用があります。なお、違反に対する執行や罰則などについては、2025年8月2日から適用が開始されます。

[4] https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act、正式名称は、”Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act)“。
なお、本ガイドラインは欧州委員会によって承認されていますが、本書作成時点でまだ採択はされていません。

© 2025 Nagashima Ohno & Tsunematsu

本ガイドラインの概要

本ガイドラインは、本文 135 頁と大部にわたりますが、その構成は以下のとおりです。

<本ガイドラインの項目>

1. 背景および目的
2. 禁止される AI プラクティスの概要
3. AI 法 5 条 1 項(a)および(b) - 有害な操作、欺瞞および悪用
4. AI 法 5 条 1 項(c) - ソーシャルスコアリング
5. AI 法 5 条 1 項(d) - 犯罪の個別リスク評価および予測
6. AI 法 5 条 1 項(e) - 顔画像の無差別なスクレイピング
7. AI 法 5 条 1 項(f) - 感情認識
8. AI 法 5 条 1 項(g) - 特定の「センシティブ」な特性に基づく生体分類
9. AI 法 5 条 1 項(h) - 法執行目的のためのリアルタイム遠隔生体識別（RBI）システム
10. 例外のための保護措置および条件（AI 法 5 条 2 項～7 項）
11. 適用開始
12. ガイドラインの見直しおよび更新

以下では、禁止される AI プラクティスの主な内容について、本ガイドラインで示された解釈も含めつつ概説し、いかなる行為が禁止される AI プラクティスとして規制対象であるのかを解説します。

禁止される AI プラクティスの主な内容

AI 法はリスク・ベース・アプローチに基づいて AI システムをいくつかのカテゴリーに分類し、それぞれに適切な要件や義務を定めています。なかでも、AI 法は、人の安全、生命や基本的人権に対する明白な脅威をもたらすものと考えられる以下の 8 つの AI プラクティスについては、対象となる AI システムの欧州市場への投入、サービスに供することおよび使用を禁止しています [5]（5 条 [6]、本ガイドライン(9)）。以下では、本ガイドラインで示された、各禁止される AI プラクティスの概要と具体例 [7]をご紹介し、それらの AI プラクティスに関する解釈のポイントを解説します。

(1) 有害な操作および欺瞞（Harmful manipulation and deception）（5条1項(a)）

<規制対象の概要>
人の意識を超えたサブリミナル技術や意図的に操作的または欺瞞的な技術を使用し、行動を実質的に歪める目的または効果を持ち、重大な害を引き起こすか、引き起こす可能性が合理的に高いAIシステム
<本ガイドラインで示された適用対象となるAIプラクティスの具体例>
聞こえない聴覚信号を利用したり、広告で利用者の感情的依存や特定の脆弱性を利用したりして消費者の購買決定に無意識に影響を与え、著しく有害な金銭的決定を下させるAIシステム
<本ガイドラインで示された適用対象とならないAIプラクティスの具体例>
サブリミナル技術を用いて、ユーザーをより健康的なライフスタイルに導き、喫煙などの悪い習慣をやめるように誘導する治療用チャットボット

- 「人の意識を超えたサブリミナル技術や意図的に操作的または欺瞞的な技術」
  本ガイドラインでは、禁止される AI に使用される技術として、以下の 3 つが挙げられています。

[5] ただし、法執行目的のためのリアルタイム遠隔生体識別（RBI）システムについては使用のみが禁止されます。
[6] 以下、単に条文または前文の番号のみを引用しているものは、AI 法における条文または前文を指します。
[7] 本項ではイメージしやすい具体例を抜粋しておりますが、本ガイドラインではこれ以外にも豊富な具体例が列挙されておりますのでそちらもご覧ください。

© 2025 Nagashima Ohno & Tsunematsu

類型	概要
サブリミナル技術	本人がそのような影響や仕組み、本人の意思決定や価値観・意見形成への影響に気づかないまま、行動に影響を与えることができる技術
意図的に操作する技術	個人の自律性と自由な選択を損なうような方法で、個人の行動に影響を与えたり、変えたり、コントロールしたりするように設計されたりする技術
欺瞞的な技術	人の自律性、意思決定、自由な選択を、その人が意識していない、あるいは意識していても欺くことができる、あるいはそれを制御したり抵抗したりすることができないような方法で、破壊したり損なったりする技術

上記 3 つの技術の他、これらの技術の組み合わせも規制対象の技術に該当する可能性があるとされています。

- 「行動を実質的に歪める目的または効果」
  サブリミナル技術、意図的に操作する技術または欺瞞的な技術を利用することで、十分な情報に基づいた意思決定を行う能力を著しく損なうような形で人々の行動に影響を与えることができ、それによって、そうでなければ取らなかったであろう行動を取らせたり、意思決定をさせたりすることをいうとされています。
- 「重大な害」
  ここでの「害」には、身体的、心理的、経済的、経済的損害が含まれるとされています。その上で、「重大」であるかどうかは具体的状況や累積的影響、損害の規模と強度、影響を受ける者の脆弱性（子どもや高齢者など）、持続期間と可逆性が主な考慮要素であるとされています。

(2) 脆弱性の有害な悪用（Harmful exploitation of vulnerabilities）（5条1項(b)）

＜規制対象の概要＞
年齢、障害、特定の社会的または経済的状況による脆弱性を悪用し、行動を実質的に歪める目的または効果を持ち、重大な害を引き起こすか、引き起こす可能性が合理的に高い AI システム
＜本ガイドラインで示された適用対象となる AI プラクティスの具体例＞
子どもと交流する AI 搭載のおもちゃが、デジタルな報酬などと引き換えに子どもを家具に上らせたりするなど次第に危険な課題をクリアするように仕向ける場合や、オンライン上で障害を持つ少女や女性を特定し、より効果的なグルーミング手法でターゲットにする AI システム
＜本ガイドラインで示された適用対象とならない AI プラクティスの具体例＞
顧客の年齢や特定の社会経済的状況をインプットとして使用する、住宅ローンやローンなどの銀行サービスの提供に使用される AI システム（年齢、障害、または特定の社会経済的状況により脆弱であると特定された人々を保護・支援するために設計され、それらのグループにとって有益であり、それらのグループにとって公平で持続可能な金融サービスにも貢献する場合）

- 「年齢、障害、特定の社会的または経済的状況による脆弱性を悪用し」
  脆弱性について、本ガイドラインでは、認知的、感情的、身体的、その他、個人または集団が十分な情報を得た上で意思決定を行ったり、その他行動に影響を与えたりする能力に影響を及ぼしうる感受性の形態を含む、広範なカテゴリーを包含するものとされています。ただし、「年齢」、「障害」および「特定の社会的または経済的状況」[8]による脆弱性に限定されています。
- 「行動を実質的に歪める目的または効果」および「重大な害」
  これらの解釈については上記(1)と同様です。

(3) ソーシャルスコアリング（Social scoring）（5条1項(c)）

＜規制対象の概要＞
一定期間の社会的行動や個人的または性格的特徴に基づいて自然人または人のグループを評価または分類し、ソー

[8] 「特定の」とは、固有の個人的特性として解釈されるべきではなく、法的地位や特定の社会的・経済的弱者の一員であることを意味するとされています。一時的な失業、債務超過、移住状況などの一過性の状況も特定の社会経済的状況としてカバーされるとされています。

© 2025 Nagashima Ohno & Tsunematsu

シャルスコアが無関係な社会的文脈からのデータに基づく不利または不利益な扱いをもたらすか、そのような扱いが社会的行動に対して不当または過剰である場合

<本ガイドラインで示された適用対象となる AI プラクティスの具体例>

家計手当の不正受給の確率を推定するために、職場の成績や特定の国籍や民族出身の配偶者がいるなどの明らかに関連性や妥当性のない社会的文脈から収集または推論された特徴に依拠している AI システム

<本ガイドラインで示された適用対象とならない AI プラクティスの具体例>

オンラインショッピングプラットフォームが、購入履歴が豊富で返品率の低いユーザーに対して、より迅速な返品申請プロセスや返品不要の返金などの特典を提供する AI を活用したスコアリング

- 「評価または分類」
  性別、身長などの特徴に基づく人または人の集団の単純な「分類」には評価や判断を要さず、したがって「評価」よりも広い概念であるとされています。そのため、自然人または人の集団とその特性または行動に関する特定の評価または判断を必ずしも伴わない基準に基づく他の種類の分類または類型化も禁止される AI システムの対象となります。なお、EU データ保護法における「プロファイリング」は、AI 法で禁止されるソーシャルスコアリングに含まれる可能性があるとされています。
- 「不利または不利益な扱い」
  「不利」と「不利益」は区別されており、前者はスコアリングの結果その人や集団が他の人と比べて不利な扱いを受けなければならないことを意味し、必ずしも特定の損害や不利益を必要としない一方で、後者は特定の損害や不利益を被ることをいうとされています。
- 「そのような扱いが社会的行動に対して不当または過剰」
  社会的行動の重大性と、ソーシャルスコアリングから生じる関係者の基本的権利への影響と干渉の重大性を比較して、そのような扱いが追求される正当な目的に対して不釣り合いであるかどうかが、比例性の一般原則を考慮して決定されるべきであるとされています。

(4) 犯罪の個別リスク評価および予測（Individual risk assessment and prediction of criminal offences）（5条1項(d)）

<規制対象の概要>

自然人が犯罪をするリスクを評価または予測するために、自然人のプロファイリングまたは人格的特徴または特性の評価のみに基づき、自然人のリスク評価を行うための AI システム

<本ガイドラインで示された適用対象となる AI プラクティスの具体例>

個人の年齢、国籍、住所や配偶者の有無などのみからテロなどの犯罪行動を予測する AI システムを利用し、それらの個人的特徴のみに基づいて将来犯罪をする可能性が高いとみなされる場合

<本ガイドラインで示された適用対象とならない AI プラクティスの具体例>

群衆の中で誰かが犯罪を準備中であり、犯罪をする可能性が高いと合理的に疑われる危険な行動をしていることを人間の評価者に伝えてプロファイリングを支援する AI システム [9]

- 「自然人が犯罪をするリスクを評価または予測するため」
  犯罪予測 AI システムとは、過去のデータ内のパターンを特定し、犯罪発生の可能性と指標を関連付け、予測出力としてリスクスコアを生成するものとされています。また、その対象は、原則として、将来的なものであり、（まだ実行されていない）将来の犯罪や、犯罪を実行するために行われた未遂や準備行為の場合を含め、現時点で実行される危険性があると評価されている犯罪に関するものであるとされています。
- 「自然人のプロファイリングまたは人格的特徴または特性の評価のみに基づき」
  プロファイリングの概念については、AI 法 3 条(52)が GDPR4 条 4 項の定義 [10]を参照しています。「人格的特徴または特性」について前文(42)は「国籍、出生地、居住地、子供の数、負債額、車のタイプ」など、

[9] これは、AI の支援を受けて人間が行うリスク評価は、個人的特徴やプロファイリングのみに基づくのではなく、行動を起こす前に人間によって検討された、その人物による犯罪行動に関連する客観的で検証可能な事実に基づくものであるからと説明されています。

[10] 「自然人と関連する一定の個人的側面を評価するための、特に、当該自然人の業務遂行能力、経済状態、健康、個人的嗜好、興味関心、信頼性、行動、位置及び移動に関する側面を分析又は予測するための、個人データの利用によって構成される、あらゆる形式の、個人データの自動的な取扱い」（GDPR4 条 4 項）

© 2025 Nagashima Ohno & Tsunematsu

人が犯罪をするリスクを予測するために評価されうる人格的特徴または特性の例を示していますが、これは例示列挙であることが明らかにされています。

(5) 顔画像の無差別なスクレイピング（Untargeted scraping of facial images）（5条1項(e)）

＜規制対象の概要＞
インターネットや監視カメラの映像から対象を絞らずに顔画像をスクレイピングすることで顔認識データベースを作成または拡張するAIシステム
＜本ガイドラインで示された適用対象となるAIプラクティスの具体例＞
ソーシャルメディアから自動でスクレイピングされた画像を関連情報（画像の出所（URL）、地域、場合によっては個人名など）とともに収集し、ユーザーが個人の画像をAIシステムにアップロードすると、AIがその画像がデータベース内の顔画像と一致するかを判断するようなAIシステム
＜本ガイドラインで示された適用対象とならないAIプラクティスの具体例＞
顔画像以外の生体データ（音声サンプルなど）のスクレイピングの場合、スクレイピング自体にAIが関与していない場合、顔画像データベースを人物の認識のために利用しない場合（AIモデルのトレーニングやテストの目的での使用であり、人物が特定されない場合）

- 「顔認識データベース」
  コンピュータによる迅速な検索と取得のために特別に編成されたデータまたは情報の集合体を指し、デジタル画像またはビデオフレームから顔を顔のデータベースとして、人間の照合データベース内の画像と比較し、両者が一致する可能性が高いかどうかを判断することができるものであることが想定されています[11]。
- 「対象を絞らずに顔画像をスクレイピングする」
  「対象を絞らずに」とは、特定の個人やグループに焦点を絞らないことを意味し[12]、「スクレイピング」とはウェブクローラ、ボット、またはその他の手段を使用して、監視カメラ、ウェブサイト、ソーシャルメディアを含むさまざまなソースからデータやコンテンツを自動的に抽出することをいいます。
- 「インターネットや監視カメラの映像から」
  この点については、ある人がソーシャルメディア上で自分の顔画像を公開したからといって、その人が顔認識データベースにその画像が含まれることに同意したことにはならないことが明らかにされています。

(6) 感情認識[13]（Emotion recognition）（5条1項(f)）

＜規制対象の概要＞
職場および教育機関の領域で感情を推測するAIシステム。ただし、医療または安全上の理由がある場合を除く
＜本ガイドラインで示された適用対象となるAIプラクティスの具体例＞
カメラを利用して従業員の幸福感などの感情を追跡するAIシステムや入学試験において受験者の感情を認識するAIシステムを利用する場合
＜本ガイドラインで示された適用対象とならないAIプラクティスの具体例＞
タイピングのキーストロークまたは顧客の音声メッセージ（例えば、チャットメッセージ、仮想音声アシスタントの使用）に基づいて感情認識を可能にするAIシステム（職場や教育機関における利用ではないため）[14]

---

[11] データベースの唯一の目的が顔認証に使用されることが必要であるわけではなく、データベースが顔認証に使用可能であれば十分であるとされています。

[12] したがって、特定の個人またはあらかじめ定義されたグループの人間の顔を含む画像または映像のみを収集するよう指示されている場合は規制対象になりません。

[13] AI 法 3 条(29)では、感情認識システムを「自然人の生体情報に基づいて自然人の感情または意図を識別し、推論することを目的とする AI システム」と定義しています。5 条 1 項(f)で直接的に感情認識システムについて言及されているわけではありませんが、本ガイドラインは前文(44)を参照し、感情認識システムは 5 条 1 項(f)で禁止される AI システムと関連するものであると位置づけています。

[14] ただし、広告目的のためのオンラインマーケティングで使用する行為は AI 法 5 条 1 項(a)および(b)の有害な操作、欺瞞及び悪用の禁止規定が適用される可能性があるとされています。

© 2025 Nagashima Ohno & Tsunematsu

- 「感情」
  感情や意図の概念は広い意味で理解されるべきであり、制限的に解釈されるべきではないとされています。前文(18)には、「幸福、悲しみ、怒り、驚き、嫌悪、困惑、興奮、恥、軽蔑、満足、娯楽」などの感情が列挙され、その詳細が示されていますが、これらは例示列挙であることが明らかにされています。
- 感情の「推測（Inferring）」と「識別（Identification）」
  5 条 1 項(f)では、感情を「推測」する AI を禁止していますが、前文(44)は「感情を識別または推測する」AI システムを禁止の対象としてします。本ガイドラインにおいては、「推測」するためには通常「識別」を必要とするため、感情の「推測」だけでなく、「識別」についても禁止の対象となることを明らかにしています。なお、感情の「識別」は、自然人の生体データ（例えば、声や顔の表情）の処理によって、感情認識システムにあらかじめプログラムされている感情と直接比較して識別することができる場合に行われるものです。一方で、感情の「推測」は、システム自身による分析その他の処理によって生成された情報から感情を推測することによって行われるものであるとされています。
- 「職場および教育機関」
  禁止される感情推測 AI は、「職場および教育機関」における利用などに限定されていますが、ここでいう「職場」は非常に広く捉えられており、仕事が行われるあらゆる環境（物理的・仮想的）が含まれ、従業員、請負業者、研修生といった地位とは無関係であり、選考および採用プロセス中の候補者にも適用されるとされています。また、「教育機関」も広く解されており、公的か私立かを問わず、また、生徒の年齢も問わず、修了書（certificate）を出すことができるか否かが重要な特徴とされています。

(7) 特定の「センシティブ」な特性に基づく生体分類（Biometric categorization for certain 'sensitive' characteristics）（5条1項(g)）

＜規制対象の概要＞
人々を生体データ[15]に基づいて分類し、人種、政治的意見、労働組合のメンバーシップ、宗教的または哲学的信念、性生活または性的指向を推定または推測する生体分類システム。ただし、法執行目的を含む適法に取得された生体認証データセットのラベリングまたはフィルタリングを除く
＜本ガイドラインで示された適用対象となるAIプラクティスの具体例＞
声から個人の人種を特定するAIシステム
＜本ガイドラインで示された適用対象とならないAIプラクティスの具体例＞
ある民族グループのメンバーが面接に招かれる確率が低くなるようなケースを回避するために生体データにラベル付けをする場合

- 「生体分類システム」
  AI 法 3 条(40)は、生体分類システムを「他の商用サービスに付随するもので、客観的な技術的理由により厳密に必要な場合を除き、自然人をその生体データに基づいて特定のカテゴリーに割り当てることを目的とする AI システム」と定義しています。本ガイドラインにおいて、「他の商用サービスに付随するもので、客観的な技術的理由により厳密に必要な場合」とは、他の商業サービスと本質的に結びついている機能であり、客観的な技術的理由により、その機能が主たるサービスなしには使用できないことを意味するとされています。

(8) 法執行目的のためのリアルタイム遠隔生体識別（RBI）システム（Real-time remote biometric identification (RBI) Systems for law enforcement purposes）（5条1項(h)）

＜規制対象の概要＞
法執行の目的で、公的にアクセス可能な空間でリアルタイムの遠隔生体識別を行う AI システム。ただし、特定の被害者を狙った捜索、テロ攻撃などの特定の脅威の防止、または特定の犯罪の容疑者の捜索に必要な場合を除く
＜本ガイドラインで示された適用対象となる AI プラクティスの具体例＞
万引き犯を特定し、その顔画像を犯罪データベースと比較するために、警察がリアルタイムの RBI システムを使

[15]「生体データ」は、AI 法 3 条(34)で定義されており、「顔画像や指紋データなど、自然人の身体的、生理学的または行動的特徴に関連する特定の技術的処理から生じる個人データ」であるとされています。

© 2025 Nagashima Ohno & Tsunematsu

用すること

<本ガイドラインで示された適用対象とならない AI プラクティスの具体例>

子供が誘拐され、誘拐犯が子供をある場所から別の場所に車で連れて行こうとしているという具体的な兆候がある場合に、警察がその子供を対象とした捜索のために RBI システムを使用する場合（5 条 1 項(h)(i)に該当）、ある人物が、通常テロ攻撃やテロ集団に関連する暴力的な過激派スローガンを叫びながら、ナイフで攻撃する人を探して公園を走り回っているとの情報が警察に入った場合に当該人物の位置特定のため RBI システムを使用する場合（5 条 1 項(h)(ii)に該当）、および警察が RBI システムを導入してフェスティバルを監視し、違法薬物売買や性犯罪で逮捕状が出ている指名手配者を特定する場合

- 「遠隔生体識別」
  遠隔生体識別システム（以下、「RBI システム」といいます。）とは、遠隔地から、人の生体認証データと参照データベースに含まれる生体認証データとを比較することにより、自然人の積極的な関与なしに自然人を識別することを目的とした AI システムであるとされています（AI 法 3 条(41)）。
- 「リアルタイム」
  AI システムが生体データを「瞬時に、ほぼ瞬時に、またはいかなる場合も重大な遅延なく」捕捉し、さらに処理することを意味します（前文(17)）。
- 「公的にアクセス可能な空間」
  アクセスに一定の条件が適用されるかどうか、また収容人数の制限の有無にかかわらず、不特定多数の自然人がアクセスできる公的または私的所有の物理的な場所をいいます（AI 法 3 条(44)）。

禁止される AI プラクティスに関する留意点

本ガイドラインでは、禁止される AI プラクティスに関する規律について、前提となる以下の点についても示されています。

1. 禁止される行為（「市場への投入」、「サービスに供する」および「使用」）、プロバイダおよびディプロイヤなどの定義

AI 法は、禁止される AI システム（RBI システム（5 条 1 項(h)）を除きます[16]。）の「市場への投入」、「サービスに供すること」および「使用」を禁止しています（5 条 1 項）。これらの定義は AI 法に定められているものもありますが、本ガイドラインでは、それぞれの用語の定義についてさらに詳しく解説するとともに、具体例を示しています。また、AI 法は、AI システムに関連する事業者を、プロバイダ、ディプロイヤ、輸入者、販売業者、製品製造者といった異なるカテゴリに区別しているところ、本ガイドラインは、禁止される AI プラクティスの範囲を踏まえ、プロバイダおよびディプロイヤの範囲について解釈を示しています。

項目	概要	具体例
市場への投入（placing on the market）	・ AI システムの「市場への投入」とは、AI システムを欧州市場に初めて提供することをいい、「提供」とは、商業活動の一環として、対価の有無にかかわらず、欧州市場での頒布または使用のためにシステムを供給することをいう（AI 法 3 条(9)）。 ・ AI システムの提供はその供給の態様にかかわらず、API、クラウド、直接ダウンロード、物理的なコピー、または製品に組み込まれた形態を	・ 第三国のプロバイダが EU 域外で開発した RBI システムを、1 つ以上の加盟国において有償または無償で提供する場合。市場への投入は、API やその他のユーザーインターフェースを通じてオンラインでシステムへのアクセスを提供する形態で行われる場合もある。

[16] RBI システム（5 条 1 項(h)）については使用のみが禁止されます。

© 2025 Nagashima Ohno & Tsunematsu

	通じたシステムおよびそのサービスへのアクセスを広く含む。	
サービスに供する（putting into service）	・ AI システムを「サービスに供する」とは、AI システムを、初めて使用する目的で直接ディプロイヤに提供する場合、またはディプロイヤ自身がその本来の目的のために使用する場合をいう（AI 法 3 条(11)）。ここでいう「本来の目的」とは、プロバイダが意図する使用方法を意味し、提供する情報やより広い文脈を踏まえて判断される。 ・ したがって、この定義には、第三者への初回使用のための提供と、社内での開発および導入の両方が含まれる。	・ プロバイダが EU 域外で RBI システムを開発し、当該システムを加盟国の法執行当局または民間企業に対してその初めての使用のために供給し、それによってサービスを開始する場合。 ・ 公共機関が組織内でスコアリングシステムを開発し、当該システムを展開して家計補助金の受給者の不正リスクを予測し、それによってサービスを開始する場合。
使用（use）	・ AI 法において「使用」は定義されていないものの、市場に投入された後、またはサービスに供された後のあらゆる使用を広く含むものとして解釈される。 ・ これには、AI システムをより複雑なシステムに統合することや、予見可能か否かにかかわらず発生しうる AI システムの誤用も含まれる。	・ 医療や安全の目的で使用される場合を除き、使用者が職場での感情を推論するために AI システムを使用することは禁止される（5 条 1 項(f)）。この禁止規定は、プロバイダ（システムのサプライヤ）が利用規約においてそのような使用を禁止しているかどうかにかかわらず、ディプロイヤにも適用される。
プロバイダ（provider）	・ 「プロバイダ」とは、AI システムを開発する、あるいは他者に開発させた上で、EU 市場に投入する、または自らの名称や商標の下で提供・運用する自然人または法人、行政機関、その他の団体いう（AI 法 3 条(3)）。	・ 自己の商標の下で EU 域内で RBI システムを販売するシステムのメーカーがプロバイダに該当する。システムを自社開発し、自らの利用のためにサービスを開始する公共機関が当該システムのプロバイダである場合もある。
ディプロイヤ（deployer）	・ 「ディプロイヤ」とは、個人的かつ非専門的な利用を除き、自然人または法人、公的機関、当局、その他の機関で、自己の権限に基づき AI システムを使用する者をいう（AI 法 3 条(4)）。この定義における「権限」とは、システムを導入する決定およびその実際の使用方法について責任を負うことを意味する。 ・ AI システムのディプロイヤが、自己の権限に基づき AI システムを使用する法人（法執行当局や民間警備会社など）である場合、当該法人の手順に従い、またはその管理下で活動	・ （本ガイドラインで示された具体例なし）

© 2025 Nagashima Ohno & Tsunematsu

	する個々の従業員は、ディプロイヤに該当しない。また、法人が第三者（請負業者、外部スタッフなど）を関与させる場合も、当該法人はディプロイヤに該当しうる。	

また、AI システムの運用者は、複数の役割を同時に担う場合があり、例えば、ある事業者が自社利用のために AI システムを開発し、それを実際に利用する場合には、（当該 AI システムの提供を受けて利用する他のディプロイヤが存在したとしても）当該事業者はプロバイダにもディプロイヤにも該当する可能性があるとされています。

2. 禁止される AI と除外規定・ハイリスク AI システムとの関係

本ガイドラインは、禁止される AI プラクティスに該当する場合でも、AI 法 2 条に定める除外規定（国家安全保障、研究開発、個人使用など）により AI 法の適用外となる可能性があることを示しています。ただし、除外規定の適用には条件があり、例えば国家安全保障目的での使用が「唯一の目的」である必要があるほか、研究開発の除外は現実環境でのテストには及ばず、個人使用の除外はディプロイヤに限られます。また、無償のオープンソース（OSS）ライセンスとして提供される AI システムに対する除外は、禁止される AI プラクティスには適用されないとされています。

また、禁止される AI プラクティスに該当しない場合でも、依然として「ハイリスク AI システム」に該当する可能性は残されており、感情認識など特定の用途ではハイリスク AI システムと判断される可能性があることも強調されています。

今後の見通し

上記のとおり、本ガイドラインに法的拘束力はなく、禁止される AI プラクティスについては、個別の事案ごとの判断が必要です。

本ガイドラインは、もともと、AI 法上、欧州委員会がガイドラインを策定することとされている項目に含まれており（96 条(b)）、以下に記載する他の項目についても、今後、欧州委員会がガイドラインを策定することが見込まれます。なお、2025 年 2 月 6 日には、「AI システム」の定義に関するガイドライン[17]も公表されています。当事務所でも引き続き、最新の動向を情報発信して参ります。

（欧州委員会がガイドラインを策定することとされている項目の例）

- ハイリスク AI の要求事項（8 条から 15 条）、バリューチェーン上の責任（25 条）に関するガイドライン（96 条(a)）
- 禁止されるプラクティス（5 条）に関するガイドライン（96 条(b)）
- 重大な変更（Substantial modification）に関するガイドライン（96 条(c)）
- 透明性義務に関するガイドライン（96 条(d)）
- AI 法と付属書 I の Union harmonization legislation の関係の詳細に関するガイドライン（96 条(e)）
- AI システムの適用に関するガイドライン（96 条(f)）
- ハイリスク AI に関するガイドライン（ハイリスク AI の該非に関するユースケースの包括的なリスト）（6 条 5 項、前文(53)）
- 零細企業によるシンプルな品質管理システムの要件に関するガイドライン（63 条 1 項、前文(146)）

2025 年 4 月 1 日

[17] https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-ai-system-definition-facilitate-first-ai-acts-rules-application

© 2025 Nagashima Ohno & Tsunematsu

[執筆者]

殿村 桂司（弁護士・パートナー）
keiji_tonomura@noandt.com
TMT（technology, media and telecoms）分野を中心に、M&A・戦略的提携、ライセンス・共同開発その他の知財関連取引、テクノロジー関連法務、ベンチャー投資・スタートアップ法務、デジタルメディア・エンタテインメント、ゲーム、テレコム、宇宙、個人情報・データプロテクション、ガバナンスなど企業法務全般に関するアドバイスを提供している。
2018 年～2019 年 経済産業省「AI・データの利用に関する契約ガイドライン」検討会作業部会構成員。2024 年～内閣府「AI 制度研究会」構成員、経済産業省「AI 利活用に伴う契約時の留意事項検討会」委員。
日本経済新聞社の 2024 年「企業法務税務・弁護士調査」の AI・テック・データ分野にて第 1 位に選出。国際的にも ALB の Asia Super 50 TMT Lawyers 2024 のほか、Chambers Asia-Pacific、Legal 500 Asia Pacific 等の国際的な評価媒体においても日本の TMT 分野等で Band 1 等に選出されている。

今野 由紀子（弁護士）
yukiko_konno@noandt.com
主な取扱分野は、クロスボーダーを中心とする企業法務一般のほか、国内外の個人情報・データプロテクション、ガバナンス、サイバーセキュリティ、データセキュリティその他データにまつわる様々な法律問題に関する助言。2005 年慶應義塾大学経済学部卒業、2008 年中央大学法科大学院修了。2015 年 Columbia Law School 卒業（LL.M, Harlan Fiske Stone Scholar）。2015 年～2017 年三菱商事株式会社勤務、2019 年～2022 年経済産業省勤務。

丸田 颯人（弁護士・情報処理安全確保支援士）
hayato_maruta@noandt.com
2019 年長島・大野・常松法律事務所入所。情報漏えい、製品不正やパワハラに関する調査等、危機管理・企業不祥事対応、コンプライアンス等に関する案件を主に取り扱っている。その他、テクノロジー関連法務やコーポレートを中心に広く企業法務一般に携わっている。
2023 年経済産業省「AI ガバナンスのルールに関する調査研究及び検討会運営有識者検討委員会」委員（AI 事業者ガイドラインワーキンググループ委員）。

本ニュースレターは、各位のご参考のために一般的な情報を簡潔に提供することを目的としたものであり、当事務所の法的アドバイスを構成するものではありません。また見解に亘る部分は執筆者の個人的見解であり当事務所の見解ではありません。一般的情報としての性質上、法令の条文や出典の引用を意図的に省略している場合があります。個別具体的事案に係る問題については、必ず弁護士にご相談ください。

© 2025 Nagashima Ohno & Tsunematsu

[編集者]

殿村 桂司（弁護士・パートナー）
keiji_tonomura@noandt.com
企業買収（M&A）取引・知財関連取引を中心に企業法務全般に関するアドバイスを提供している。TMT 業界の案件にも幅広い経験を有しているほか、シェアリング・エコノミー、Fintech、IoT、AI などテクノロジーの発展が生み出す新しい事業分野の案件も数多く取り扱っている。

長島･大野･常松 法律事務所 www.noandt.com

〒100-7036　東京都千代田区丸の内二丁目７番２号　ＪＰタワー
Tel: 03-6889-7000（代表）　Fax: 03-6889-8000（代表）　Email: info@noandt.com

長島・大野・常松法律事務所は、600 名以上の弁護士が所属する日本有数の総合法律事務所であり、東京、ニューヨーク、シンガポール、バンコク、ホーチミン、ハノイ、ジャカルタ*及び上海に拠点を構えています。企業法務におけるあらゆる分野のリーガルサービスをワンストップで提供し、国内案件及び国際案件の双方に豊富な経験と実績を有しています。
（*提携事務所）

NO&T Technology Law Update ～テクノロジー法ニュースレター～の配信登録を希望される場合には、<https://www.noandt.com/newsletters/nl_technology/>よりお申込みください。本ニュースレターに関するお問い合わせ等につきましては、<newsletter-technology@noandt.com>までご連絡ください。なお、配信先としてご登録いただきましたメールアドレスには、長島・大野・常松法律事務所からその他のご案内もお送りする場合がございますので予めご了承いただけますようお願いいたします

© 2025 Nagashima Ohno & Tsunematsu