

EUのAI規則案の欧州議会修正案と 顔識別システム等に対する規制動向

2023年 7月 6日

国際社会経済研究所 小泉 雄介

○ EUの法規制だが、日本企業にとっても無関係ではない

- 域外適用条項がある

- EU域外に事業拠点を持つプロバイダー（AI製品・サービス提供事業者）やディプロイヤー（利用事業者）も規制対象となりうる。

- 各国の制度とのハーモナイズが意図されている

- 欧州委員会のベステア一副委員長は2021年5月にAI規則案について、「同じ考えを持った民主主義国家との連合を作るために、私たちの模範を示し、それを拡大する必要がある」と発言。
- 日本政府はAIに対して法的拘束力のないソフトローで対応する方向性が示しているが、2023年5月のG7広島首脳コミュニケでは「信頼できるAIという共通のビジョンと目標を達成するためのアプローチと政策手段が、G7諸国間で異なり得ることを認識しつつも、AIガバナンスに関する国際的な議論とAIガバナンスの枠組み間の相互運用性の重要性を強調する」とし、G7としてはAI技術標準、リスク評価フレームワーク、監査・認証制度などの相互運用性のためのツールの開発と採用が目指されている。
- なお米国は、従来からAIに関する新法は制定せず業界の自主規制に委ねる方針だったが、バイデン大統領が議会に法案策定を呼びかけるなど、風向きが変わりつつある。

- 関連EU規制であるGDPR（一般データ保護規則）は世界標準になりつつある

- アジア、南米、北米などでGDPRと類似の個人情報保護法が増えている。
- EUのAI倫理ガイドライン等を参考に社内ポリシー・ルールを策定する（国内）企業も増えている。

- AI規則案（AI法案）
 - [欧州委員会が2021年4月21日に公表。](#)
 - 「Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts」
 - <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELLAR%3Ae0649735-a372-11eb-9585-01aa75ed71a1>
 - [EU理事会では2022年12月に合意案（general approach）の採択済み。](#)
 - 欧州議会傘下のIMCO委員会とLIBE委員会で議会修正案に対する投票が2023年5月11日に行われ、賛成多数。
 - 欧州委員会案に対する修正箇所が771件
 - https://www.europarl.europa.eu/doceo/document/A-9-2023-0188_EN.html
 - [欧州議会は2023年6月14日の総会で議会修正案を採択。](#)
 - 上記IMCO委員会とLIBE委員会が可決した議会修正案がそのまま採択された。
 - 中道右派のEPPはリアルタイムリモート生体識別の禁止から「犯罪被害者の捜索」や「テロ攻撃等の防止」の例外を残そうとしたが、失敗。
 - 今後、[欧州委員会・欧州議会・EU理事会で非公式な三者協議（trilogue）](#)が行われ、2023年内の合意が目指されている。早ければ、2024年春にAI規則（AI法）が制定される見込み。同規則の適用（施行）はその2年後。

日付	欧州委員会、欧州議会、EU理事会等の取組み
2019年4月8日	欧州委員会の設立したAIハイレベル専門家グループ（HLEG）が「 信頼できるAIのための倫理ガイドライン 」を公表。
2020年2月19日	欧州委員会は「 AIに関するホワイトペーパー：優越と信頼に向けた欧州アプローチ 」を公表。
2021年4月21日	欧州委員会がAIホワイトペーパーに対する法規制面でのフォローアップ文書である「 AI規則案 」を公表。
4月26日	AI規則案に対する パブリックコンサルテーション を開始（～8月6日）。304件のフィードバック（JEITA含む）。
6月18日	EDPBとEDPS が「AI規則案に関する共同意見書」を公表。
2021年12月	欧州議会で IMCO（域内市場・消費者保護委員会） と LIBE（市民的自由・司法・内務委員会） がAI規則案の審議を共同で主導することに決定。
2022年4月20日	欧州議会 IMCO-LIBE がAI規則案に対する ドラフトレポート を公表。約3300件の修正提案。
4月～7月	欧州議会ENVI、ITRE、CULT、TRANがIMCO-LIBEに意見を提出。
2023年5月11日	欧州議会IMCOとLIBEで修正案への投票が行われ、賛成多数で可決。
6月14日	欧州議会（総会）が AI規則案に対する議会修正案 を採択。
2021年11月29日	EU理事会 スロベニア議長国 がAI規則案に対する（部分的な）第一妥協案を公表。
2022年6月17日	EU理事会 フランス議長国 がAI規則案に対する（包括的な）第一妥協案を作成。
7月15日	EU理事会 チェコ議長国 がAI規則案に対する第二妥協案を公表。
12月6日	EU理事会が AI規則案に対する合意案（general approach） を採択。
2022年9月28日	欧州委員会が（AI規則案を補完する）「製造物責任指令改正案」と「AI責任指令案」を公表。

【ご参考】欧州委員会提案のAI規則案：適用範囲

○第2条 適用範囲（Scope）

1. 本規則は以下に適用される。

- (a) そのプロバイダーがEU域内に拠点があるか第三国に拠点があるかに関係なく、EU域内でAIシステムの市場投入（上市）またはサービス提供を行うプロバイダー。
- (b) EU域内に位置するAIシステムのユーザー。
- (c) そのシステムによって生成されたアウトプットがEU域内で使用される場合、第三国に位置するAIシステムのプロバイダーとユーザー。

2. AnnexIIのセクションBの対象となる製品またはシステムの安全コンポーネントであるハイリスクAIシステム、またはそれ自体がそのような製品またはシステムであるハイリスクAIシステムの場合、本規則の第84条（評価と見直し）のみが適用される。

民間航空のセキュリティの分野における共通ルールに関する規則（EC） No 300/2008	二輪車等の認可と市場監視に関する規則（EU） No 168/2013
農林業用車両の認可と市場監視に関する規則（EU） No 167/2013	船用機器に関する指令2014/90/EU
鉄道システムの相互運用性に関する指令（EU） 2016/797	自動車とトレーラーの認可と市場監視に関する規則（EU） 2018/858
自動車の型式認可要件に関する規則（EU） 2019/2144	民間航空分野における共通ルールと欧州連合航空安全庁の設置に関する規則（EU） 2018/1139

3. 本規則は、軍事目的のみで開発される、または使用されるAIシステムには適用されない。

4. 本規則は、それらの機関や組織がEUまたは1つ以上の加盟国との法執行および司法協力のための国際協定の枠組みの中でAIシステムを使用する場合、第1項に従い本規則の適用範囲内にある第三国の公的機関にも国際組織にも適用されない。

5. 本規則は、指令2000/31/ECの第II章第IV節に規定されている仲介サービスプロバイダーの責任に関する条項[デジタルサービス法の条項で置換される]の適用に影響を与えない。

- 本規則の「適用範囲」（第2条1項）に(ca)～(cc)を追加。(a)と(c)でEU域外の事業者に対する「域外適用」を規定。
 - (a) そのプロバイダーがEU域内に拠点があるか第三国に拠点があるかに関係なく、EU域内でAIシステムの市場投入（上市）またはサービス提供を行うプロバイダー。
 - (b) EU域内に拠点がある、または位置するディプロイヤー。
 - (c) 加盟国法が国際公法に基づいて適用される場合、または当該システムによって生成されたアウトプットのEU域内での使用が意図されている場合、第三国に拠点がある、または位置するプロバイダーとディプロイヤー。
 - (ca) 第5条で言及されたAIシステム（禁止AI）をEU域外で市場投入またはサービス提供するプロバイダーであって、当該システムのプロバイダーまたは販売者がEU域内に位置する場合。
 - (cb) AIシステムの輸入者および販売者、並びにAIシステムのプロバイダーの権限のある代理人（これらの輸入者、販売者または権限のある代理人がEU域内に拠点があるか、または位置する場合）。
 - (cc) EU域内に居住し、EU域内で市場投入またはサービス提供されるAIシステムの使用によって健康・安全・基本的権利に対する悪影響を受ける、第3条（8a）に定義された影響を受ける人々。
- ※ 「ディプロイヤー」：個人的で非職業的なアクティビティの過程でAIシステムが使用される場合を除き、自らの権限でAIシステムを使用する自然人もしくは法人、公的機関、部局、またはその他の組織。（←欧州委員会案では「ユーザー」だった）
- また、無料のOSSには適用されないことを明確化（第2条5e項）。ただし基盤モデルは除く。
 - 「本規則は、ハイリスクAIシステムの一部または第II編もしくは第IV編に該当するAIシステムの一部としてプロバイダーによって市場投入またはサービス提供される場合を除き、無料のオープンソースライセンスに基づいて提供されるAIコンポーネントには適用されない。ただしこの除外は、第3条に定義されている基盤モデルには適用されない。」

- AIシステムの定義は、急速に発展する技術と市場を考慮に入れて、可能な限り技術的に中立で、時代遅れとならないものにすることを目的としている。（説明覚書5.2.1）

○AIの定義（第3条（1））

- 「人工知能システム（AIシステム）」とは、Annex Iに記載されている手法とアプローチの1つ以上を用いて開発され、人間が定義した特定の目的について、当該システムが相互作用する環境に影響を与えるようなコンテンツ、予測、レコメンデーション、意思決定などのアウトプットを生成できるソフトウェアを意味する。

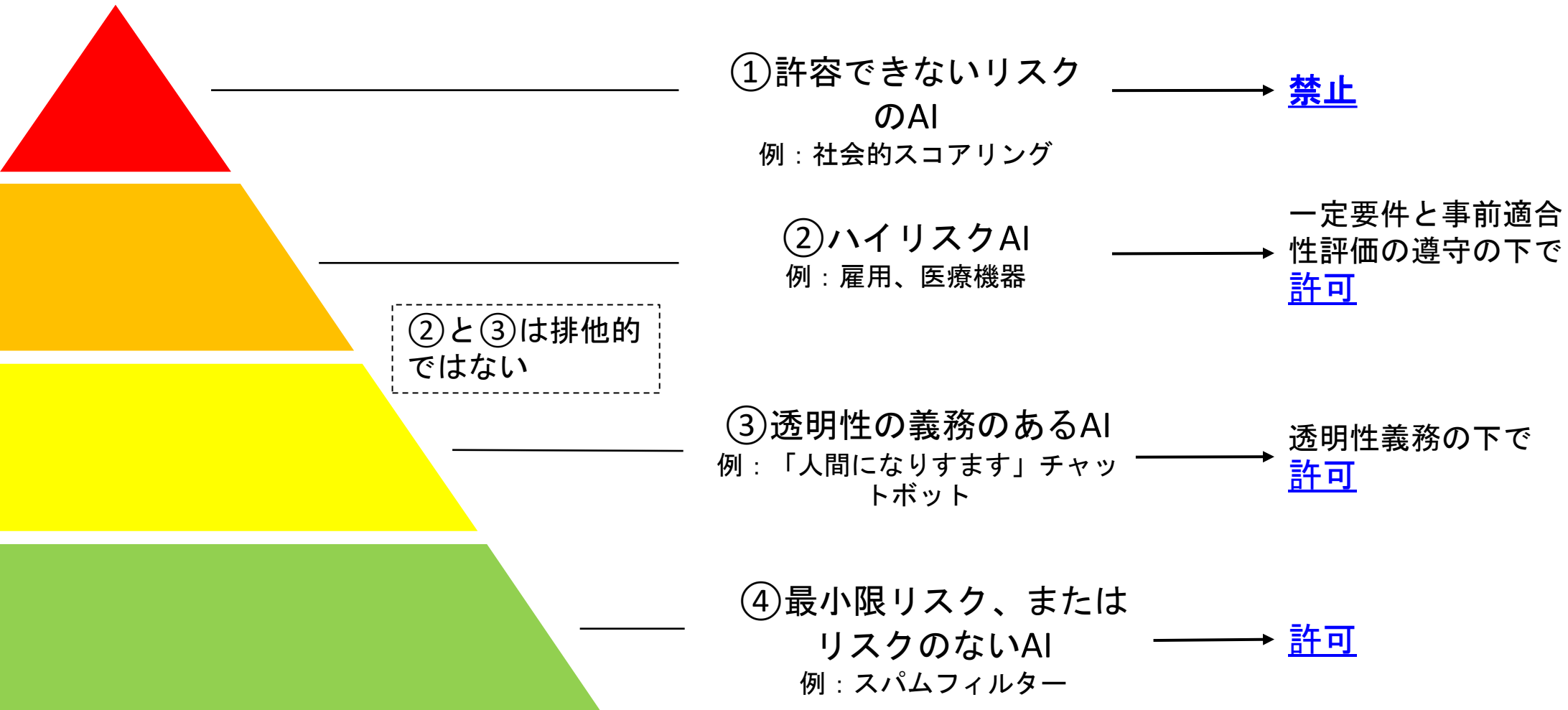
○Annex I 人工知能の手法とアプローチ

- （a）機械学習アプローチ：ディープラーニングを含む様々な方法を使用した、教師あり学習、教師なし学習、強化学習を含む
- （b）論理・知識ベースのアプローチ：知識表現、帰納（論理）プログラミング、知識ベース、推論および演繹エンジン、（記号）推論、エキスパートシステムを含む
- （c）統計的アプローチ、ベイズ推定、検索および最適化手法

- 「AIシステム」の定義を以下に修正（第3条（1））。
 - 「人工知能システム」（AI システム）：様々なレベルの自律性で動作するように設計され、明示的または暗黙的な目的のために、物理的またはバーチャルな環境に影響を与える予測、レコメンデーション、決定などのアウトプットを生成できるマシンベースのシステム。
 - ※「AIに関するOECD理事会の勧告」（2019年5月）の定義に合わせたもの。
- 「基盤モデル」と「一般目的AI（汎用AI）」に関する定義も追加された（第3条）。
 - 「基盤モデル（foundation model）」：広範なデータで大規模にトレーニングされ、アウトプットの汎用性を考慮して設計され、幅広いタスクに適応させることができるAIシステムモデル。
 - 「一般目的AI（general purpose AI）システム」とは、幅広いアプリケーションで使用および適応できるAIシステムであって、意図的かつ特定の用途向けに設計されていないもの。
 - ※画像認識・音声認識、オーディオ・ビデオ生成、パターン検出、質問応答、翻訳など、一般的に適用可能な機能を実行するもの（EU理事会の定義）。
 - ※いわゆる「強いAI、AGI」（汎用型AI）ではない。
- 「生成AI」についても、第28b条（新規追加）の中で言及。
 - 「生成AI（generative AI）」：様々な自律性レベルで複雑なテキスト・画像・オーディオ・ビデオなどのコンテンツを生成することを特に目的としたAI システム。

【ご参考】 欧州委員会提案のAI規則案： リスクベースアプローチ

- AI規則案では、リスクベースアプローチ、すなわち（AIを一律に規制するのではなく）AI機器・サービスがもたらすリスクに応じて規制をかけるアプローチが取られている。欧州委員会によれば、ほとんどのAIシステムは④に相当するという。



出典：欧州委員会資料を和訳、加筆

【ご参考】欧州委員会提案のAI規則案： 禁止されるAIシステム

○許容できないリスクをもたらすため、禁止されているAIシステム（第5条）

説明	条文	例
(a) <u>サブリミナル操作</u> （身体的・精神的危害を引き起こすもの）	本人または他の人の身体的または精神的危害を引き起こしたり、引き起こす可能性の高い仕方でも個人の行動を実質的に歪めるために、個人の意識を超えたサブリミナル技術を用いるAIシステムの市場投入、サービス提供、または使用。	トラック運転手に可聴域でない音を聞かせて、健康かつ安全な範囲を超えて長時間運転させるようにする。AIはこのような効果を最大化する音域の発見に使用される。
(b) <u>子どもや精神障害のある人の脆弱性の悪用</u> （身体的・精神的危害を引き起こすもの）	本人または他の人の身体的または精神的危害を引き起こしたり、引き起こす可能性の高い仕方でも、当該グループに属する個人の行動を実質的に歪めるために、年齢や身体的・精神的障害による特定グループの個人の脆弱性を悪用するAIシステムの市場投入、サービス提供、または使用。	音声アシスタントを組み込んだ人形が、楽しくクールなゲームを装って、未成年者に次第に危険な行動やチャレンジをするようにけしかける。
(c) <u>汎用目的のソーシャルスコアリング</u>	個人の社会的行動または既知もしくは予測された性格特性に基づき、以下のいずれかまたは両者をもたらすようなソーシャルスコアを用いて、特定の期間にわたる自然人の信頼性を評価または分類するための、公的機関による、または公的機関に代わってのAIシステムの市場投入、サービス提供、または使用。 （i）データが最初に生成または収集されたコンテキストとは関係のない社会的コンテキストにおける、特定の自然人またはそのグループ全体に対する不利益な、または望ましくない扱い。 （ii）その社会的行動またはその重大さに対して不当なまたは不釣り合いな、特定の自然人またはそのグループ全体に対する不利益な、または望ましくない扱い。	AIシステムが、親の取るに足らない、あるいは無関係な社会的「不正行為」（医者予約の無断キャンセル、離婚など）に基づいて、社会的ケアを必要としている子どもを特定する。
(d) <u>公的にアクセス可能な空間における法執行目的でのリモート生体識別システム</u> （例外あり）	公的にアクセス可能な空間における法執行の目的での「リアルタイム」リモート生体識別システムの <u>使用</u> 。ただし、そのような使用が以下の目的の1つに厳密に必要な場合を除く。 （「 <u>犯罪被害者の捜索</u> 」「 <u>テロ攻撃等の防止</u> 」「 <u>重大犯罪の容疑者の捜査等</u> 」の例外あり）	ビデオカメラによってライブで撮影された全ての顔が、テロリストを特定するためにデータベースに対してリアルタイムでチェックされる。

- 「禁止されるAI」（第5条）で以下が拡充。
 - 個人のソーシャルスコアリング評価を行うAIシステム
 - 「公的機関による」という限定を削除。
 - 公的にアクセス可能な空間における「リアルタイム」リモート生体識別システムの使用
 - 「法執行の目的で」という限定を削除。
 - 「犯罪被害者の捜索」「テロ攻撃等の防止」「重大犯罪の容疑者の捜査」といった例外を削除。
- また、以下が追加。
 - センシティブな属性に基づいて個人を分類する生体カテゴライゼーションシステム
 - ジェンダー、性自認、人種、民族的出自、移住・市民権ステータス、政治的指向、性的指向、宗教、障害等。
 - 個人の犯罪・再犯リスクを評価するAIシステム、または、個人のプロファイリングや個人の位置・過去の犯罪行動などの人格特性の評価に基づき犯罪の発生・再発を予測するAIシステム
 - インターネットや監視カメラの映像から顔画像を無差別に収集することで顔認識データベースを作成・拡張するAIシステム
 - ※ Clearview AI社のシステム等を念頭に置いていると思われる。
 - 法執行・国境管理・職場・教育機関の分野において、個人の感情を推測するAIシステム
 - 「事後の」リモート生体識別システムを介して公的にアクセス可能な空間の記録映像を分析するAIシステム
 - 重大犯罪の捜査に厳密に必要な場合は除く。

- 「禁止されるAI」（第5条）に関連する用語の定義は以下（第3条）。
 - 「生体ベースのデータ（biometric-based data）」：自然人の身体的、生理的または行動的なシグナルに関連する特別な技術的処理から得られるデータ。（新規追加）
 - 「生体識別（biometric identification）」：ある個人の生体データをデータベースに保存されている生体データと比較することにより、当該個人のアイデンティティを確立する目的で、人間の身体的、生理的、行動的および心理的特徴を自動的に認識すること（1対多の識別）。（新規追加）
 - 「生体検証（biometric verification）」：個人の生体データと以前に提供された生体データを比較することにより、自然人のアイデンティティを自動的に検証すること（認証を含む1対1の検証）。（新規追加）
 - 「[感情認識システム（emotion recognition system）](#)」：生体データおよび生体ベースのデータに基づいて、個人またはグループの感情、思考、心の状態、または意図を識別または推測することを目的としたAIシステム。（定義を拡充）
 - 「[生体カテゴライゼーション（biometric categorisation）](#)」：生体データもしくは生体ベースのデータ、またはそれらのデータから推測できるデータに基づいて自然人を特定のカテゴリーに分類すること、またはその特徴や属性（ジェンダー、性別、年齢、髪の色、目の色、タトゥー、人種的・民族的出自、健康、精神的・身体的能力、行動、行動的・人格的特徴、言語、宗教、マイノリティー集団への帰属、性的・政治的指向等）を推測すること。（定義を拡充）
 - 「[リモート生体識別システム（remote biometric identification system）](#)」：当該人物が現れるか否か、また識別できるか否かについての事前の知識をAIシステムのディプロイヤーが持つことなく、ある人物の生体データと参照データベース内に含まれる生体データとの比較によって、離れた場所にいる自然人を識別することを目的としたAIシステム。[生体検証システムは除く](#)。（定義を拡充）
 - 「公的にアクセス可能な空間（publicly accessible space）」：アクセスに一定の条件が課されうるか否かに関わらず、また潜在的な収容能力の制限に関わらず、一般市民がアクセスできる公共または私有の場所。（定義を拡充）
 - 「リアルタイム（real-time）」リモート生体識別システム：生体データの取得、比較、および識別がすべて大幅な遅延なしに行われるリモート生体識別システム。これには、即時の識別だけでなく、迂回（本規則のすり抜け）を防ぐための、限定的な遅延も含まれる。
 - 「事後の（post）」リモート生体識別システム：「リアルタイム」リモート生体識別システム以外のリモート生体識別システム。

【ご参考】 欧州委員会提案のAI規則案： ハイリスクAIシステム

(1) EU法令で規制された製品の安全コンポーネント (第6条 (1)、AnnexII)

- AnnexIIで挙げられた製品のうち、第三者適合性評価の対象となるもの。
- AnnexII セクションA 新たな法的フレームワーク (NLF) に基づくEU調和法令のリスト

機械に関する指令2006/42/EC	玩具の安全性に関する指令2009/48/EC
レジャークラフトとパーソナルウォータークラフトに関する指令2013/53/EU	昇降機および安全コンポーネントに関連する加盟国の法律の調和に関する指令2014/33/EU
潜在的な爆発性雰囲気での使用を目的とした機器および保護システムに関連する加盟国の法律の調和に関する指令2014/34/EU	無線機器の域内市場での利用可能化および指令1999/5/ECの廃止に関連する加盟国の法律の調和に関する指令2014/53/EU
圧力機器の域内市場での利用可能化に関連する加盟国の法律の調和に関する指令2014/68/EU	ケーブルウェイの設置に関する規則 (EU) 2016/424
個人用保護具に関する規則 (EU) 2016/425	ガス燃料を燃焼する機器に関する規則 (EU) 2016/426
医療機器に関する規則 (EU) 2017/745	体外診断用医療機器に関する規則 (EU) 2017/746

- AnnexII セクションB その他のEU調和法令 (オールドアプローチ法令) → 第84条 (評価と見直し) のみ適用

民間航空のセキュリティの分野における共通ルールに関する規則 (EC) No 300/2008	二輪車等の認可と市場監視に関する規則 (EU) No 168/2013
農林業用車両の認可と市場監視に関する規則 (EU) No 167/2013	船用機器に関する指令2014/90/EU
鉄道システムの相互運用性に関する指令 (EU) 2016/797	自動車とトレーラーの認可と市場監視に関する規則 (EU) 2018/858
自動車の型式認可要件に関する規則 (EU) 2019/2144	民間航空分野における共通ルールと欧州連合航空安全庁の設置に関する規則 (EU) 2018/1139

(2) 以下の分野におけるスタンドアロンAIシステム (第6条 (2)、AnnexIII)

1. 自然人の生体識別およびカテゴライゼーション
2. 重要なインフラの管理と運用
3. 教育と職業訓練
4. 雇用、従業員管理、自営業者へのアクセス
5. 重要な民間サービス、公共サービス、公的給付へのアクセスおよび受給
6. 法執行
7. 移住、亡命、国境管理
8. 司法手続および民主的手続の管理

1. 自然人の生体識別およびカテゴライゼーション

(a) 自然人に対する「リアルタイム」および「事後」のリモート生体識別に使用されることを目的としたAIシステム。

2. 重要なインフラの管理と運用（Management and operation of critical infrastructure）

(a) 道路交通の管理と運用、水・ガス・暖房・電気の供給の管理と運用における安全コンポーネントとして使用することを目的としたAIシステム。

3. 教育と職業訓練

(a) 教育機関および職業訓練機関へのアクセスを決定したり自然人をアサインする目的で使用されることを目的としたAIシステム。

(b) 教育機関および職業訓練機関の学生を評価する目的、教育機関への入学に一般的に必要な試験の参加者を評価する目的で使用されることを目的としたAIシステム。

4. 雇用、従業員管理、自営業者へのアクセス

(a) 自然人の採用または選定、特に求人広告、応募者のスクリーニングまたはフィルタリング、面接または試験の過程での候補者の評価に使用することを目的としたAIシステム。

(b) 昇進や仕事関連の契約関係の終了に関する意思決定、業務の割り当て、そのような契約関係における個人のパフォーマンスと行動のモニタリングや評価に使用することを目的としたAIシステム。

5. 重要な民間サービス、公共サービス、公的給付へのアクセスおよび受給

(a) 公的機関によって、または公的機関に代わって、自然人が公的支援の給付およびサービスを受ける資格を評価し、またそのような給付およびサービスを許可、削減、取り消し、または再請求するために使用することを目的としたAIシステム。

(b) 個人の信用度を評価したり、個人の信用スコアを作成するために使用することを目的としたAIシステム。ただし、小規模プロバイダーが自ら使用するためにサービス開始したAIシステムを除く。

(c) 消防士や医療救護を含め、緊急時の初期対応サービスを派遣、または派遣の優先順位を決定するために使用されることを目的としたAIシステム。

6. 法執行

- (a) 自然人が**犯罪または再犯罪を行うリスクや刑事犯罪の被害者となるリスク**を評価するために、法執行機関が個人のリスク評価を行うために使用することを目的としたAIシステム。
- (b) 法執行機関が**ポリグラフや同様のツール**として使用したり、**自然人の感情状態を検出**することを目的としたAIシステム。
- (c) 法執行機関が第52条（3）で言及されているような**ディープフェイクを検出**するために使用することを目的としたAIシステム。
- (d) 刑事犯罪の捜査または起訴の過程で**証拠の信頼性を評価**するために法執行機関が使用することを目的としたAIシステム。
- (e) 指令（EU）2016/680の第3条（4）で言及されているような**自然人のプロファイリングに基づいて実際または潜在的な刑事犯罪の発生または再発を予測**するために、または**自然人やグループの人格特性・性格や過去の犯罪行動を評価**するために、法執行機関が使用することを目的としたAIシステム
- (f) 法執行機関が、**刑事犯罪の検出、捜査または起訴の過程**で、指令（EU）2016/680の第3条（4）で言及されているような**自然人のプロファイリング**に使用することを目的としたAIシステム。
- (g) 法執行機関が様々なデータソースまたは様々なデータ形式で利用可能な、複雑な関連および非関連の大規模データセットを検索して、**データ内の未知のパターンを特定したり、隠れた相関関係を発見できるような、自然人に関する犯罪分析**に使用することを目的としたAIシステム。

7. 移住、亡命、国境管理

- (a) 所轄の公的機関が**ポリグラフや同様のツール**として使用したり、**自然人の感情状態を検出**したりすることを目的としたAIシステム。
- (b) 所轄の公的機関が、加盟国の領土に**入国**することを意図する、または入国した自然人によってもたらされる**セキュリティリスク、不法移民のリスク、健康リスク**を含むリスクを評価するために使用することを目的としたAIシステム。
- (c) 所轄の公的機関が、**自然人の渡航文書（旅券）と関連文書の真正性を検証**すること、また、セキュリティ機能をチェックすることで非真正の文書を検出することを目的としたAIシステム。
- (d) 所轄の公的機関が、**亡命、ビザ、居住許可の申請**を、また関連する苦情を、それらのステータスを申請する自然人の資格の観点から審査することの**支援**を目的としたAIシステム。

8. 司法手続および民主的手続の管理

- 15 (a) 司法当局が事実と法律を調査および解釈し、**法律を具体的な一連の事実に適用**することの支援を目的としたAIシステム。

- 「ハイリスクAIシステム」（スタンドアロン）の候補としてAnnexIIIに列挙されたAIシステムは、「それが自然人の健康・安全・基本的権利や環境に害を及ぼす重大なリスクを引き起こす場合にのみハイリスクとみなされる」ことに修正（第6条2項）。
- 「ハイリスクAIシステム」（スタンドアロン）（AnnexIII）に以下が追加。
 - 感情認識システムを含む、生体データまたは生体ベースのデータに基づいて個人の特性について推論するために使用されるAIシステム
 - 個人に適切な教育レベルを評価するために使用されるAIシステム
 - 学生のテスト中の禁止行為をモニターするために使用されるAIシステム
 - 医療保険および生命保険の資格を決定するために使用されるAIシステム
 - 所轄の公的機関によって、国境管理活動の文脈で個人を識別等する目的で使用されるAI システム
 - 所轄の公的機関によって、移民の移動や国境越えに関連する傾向の予測のために使用されるAIシステム。
 - 選挙や国民投票の結果や投票行動に影響を与えるために使用されるAIシステム
 - DSA（デジタルサービス法）で指定されたソーシャルメディアプラットフォームによって、サービス受信者にユーザー生成コンテンツをレコメンドするシステムで使用されるAI システム
- ハイリスクAIシステムのディプロイヤーに「基本的人権影響評価」の義務が追加（第29a条）。

【ご参考】 欧州委員会提案のAI規則案： ハイリスクAIシステムの要件

○ハイリスクAIシステムの要件（第8条～第15条）

<u>リスク管理</u>プロセスを確立し、実施する （AIシステムの<u>意図された目的</u>の観点から）	高品質な<u>学習データ</u>、<u>検証データ</u>、<u>テストデータ</u>を使用する （関連性があり、代表的で、エラーがなく、完全なデータ）
	<u>技術文書</u>を作成し、<u>ログ機能</u>を設計する （トレーサビリティと監査可能性）
	適切な<u>透明性</u>を保証し、ユーザーに<u>情報提供</u>する （AIシステムの使用方法に関して）
	<u>人間による監督</u>を保証する （AIシステムに組み込まれた措置および／またはユーザーが実施する措置）
	<u>堅牢性</u>、<u>正確性</u>、<u>サイバーセキュリティ</u>を保証する

出典：欧州委員会資料を和訳

【ご参考】 欧州委員会提案のAI規則案： ハイリスクAIシステムのオペレーターの義務

○ハイリスクAIシステムのオペレーターの義務（第16条～第29条）

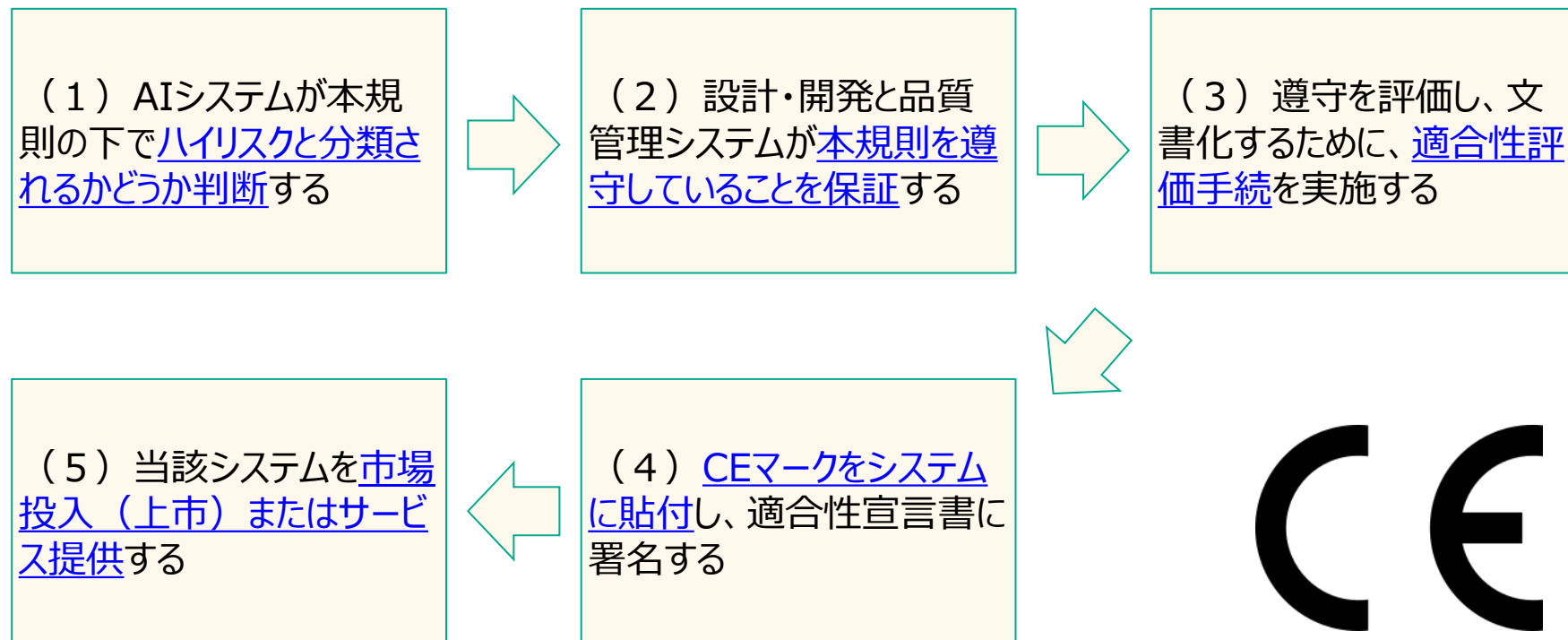
プロバイダーの義務	▶ 組織内で品質管理システムを確立し、実施する ▶ 技術文書を作成し、更新する ▶ ユーザーがハイリスクAIシステムの運用をモニターできるようにログを保管する ▶ 適合性評価を実施し、実質的な変更がある場合は当該システムの再評価を行う ▶ EUデータベースにAIシステムを登録する ▶ CEマークを貼付し、適合性宣言書に署名する ▶ 市場流通後モニタリングを実施する ▶ 市場監視機関と協力する
ユーザーの義務	▶ 使用説明書に従ってAIシステムを運用する ▶ AIシステムを使用する際に人間による監督を保証する ▶ 可能なリスクに対して運用をモニターする ▶ 重大なインシデントまたは誤動作についてプロバイダーまたは販売者に情報提供する ▶ 既存の法的義務を遵守する（GDPR等）

出典：欧州委員会資料を和訳

【ご参考】欧州委員会提案のAI規則案： ハイリスクAIシステムのCE適合性マーク

○ハイリスクAIシステムのCE適合性マーク（第49条）

- CE適合性マークは、ある製品が当該製品を規制するEU法令の要件を遵守していることを示す。ハイリスクAIシステムにCEマークを貼付するために、プロバイダーは次の手順を実施する。



出典：欧州委員会資料を和訳



CEマーク

- 欧州議会修正案では、基盤モデル（foundation model）に関する項目が追加された。
- 基盤モデルの実装形態の1つが一般目的AI（general purpose AI: 汎用AI）システム。
- 基盤モデルや一般目的AIは、ハイリスクAIシステム等に組み込まれることで、AI規則案の規制対象となりうる。
- また、基盤モデルのプロバイダーには、以下の義務が課されることとなった（第28b条2項）。
 - (a) 健康・安全・基本的権利・環境・民主主義・法の支配に対する合理的に予見可能なリスクの特定・削減・軽減が、開発前および開発全体を通じて行われていることを、独立した専門家の関与や、開発後に残存する軽減不可能なリスクの文書化等の適切な方法で実証すること。
 - (b) 基盤モデルに対する適切なデータガバナンス措置、特にデータソースの適切性・潜在的なバイアス・適切な軽減策の措置を講じたデータセットのみを処理したり組み込むこと。
 - (c) ライフサイクル全体を通じて適切なレベルのパフォーマンス・予測可能性・解釈可能性・正確性・安全性・サイバーセキュリティを達成するために、概念化・設計・開発段階における、独立した専門家の関与によるモデル評価、文書化された分析、広範なテストなどの適切な方法によって評価すること。
 - (d) エネルギー使用量・資源使用量・廃棄物を削減し、エネルギー効率とシステムの全体的な効率を向上させるための標準を利用して基盤モデルを設計および開発すること。
 - (e) 下流プロバイダーが本規則の義務を遵守できるように、広範な技術文書と分かりやすい使用説明書を作成すること。
 - (f) 本条の遵守を保証し、文書化するための品質管理システムを確立すること。
 - (g) 基盤モデルを第60条で言及されたEUデータベースに登録すること。
 - 上記の義務は、基盤モデルがハイリスクAIシステム等に組み込まれているか否かに関わらず発生。

- さらに、生成AIで使用する基盤モデルのプロバイダーには、上記に加えて以下の義務が課される（第28b条4項）。
 - a) 「透明性の義務のあるAI」として、第52条1項の透明性の義務を遵守すること。
 - b) 一般に認知されている最新技術に沿って、基本的権利（表現の自由を含む）を損なうことなく、EU法に違反するコンテンツの生成に対する十分な保護措置を保証するような仕方で基盤モデルをトレーニングし、該当する場合には設計および開発すること。
 - c) 著作権に関するEU法または国内法を損なうことなく、著作権法で保護されている学習データの使用に関する十分に詳細な概要を文書化し、公開すること。

【ご参考】 欧州委員会提案のAI規則案： ハイリスクでないAIシステム

○特定のAIシステムに対する透明性の義務（第52条）

- AIシステムと相互作用をしている人々に、それが明白でない限り、その旨を[通知](#)する。（チャットボットなど）
- 感情認識システムや生体カテゴライゼーションシステムの対象となる人々に、その旨を通知する。
- 本物・真実であると誤って見えてしまう画像・音声・ビデオコンテンツ（ディープフェイク）に[ラベル](#)を付ける。（表現の自由などの基本的権利の行使や、公共の利益の理由からディープフェイクが必要な場合は除く）

○最小限リスク、またはリスクのないAIシステム：自主的な行動規範（第69条）

- 義務ではなく任意。
- 欧州委員会と欧州人工知能会議は、低リスクAIシステムへの（ハイリスクAI向け）要件の自主的適用の促進を目的とした行動規範の作成を促進する。

- 欧州議会修正案では、[AIシステムに対する一般原則](#)が新規追加された（第4a条）。
- 「[本規則の対象となるすべてのオペレーター](#)は、倫理的で信頼できるAIに対する一貫した人間中心の欧州アプローチを促進する高レベルの枠組みを確立する以下の一般原則に従って、[AIシステムや基盤モデルの開発と使用](#)に最善の努力を払うものとする。」
 - a) 「[人間の主体性と監督](#)」：AIシステムは、人々に奉仕し、人間の尊厳と個人の自律性を尊重し、人間によって適切にコントロールおよび監督できる仕方で機能するツールとして開発・使用されるものとする。
 - b) 「[技術的な堅牢性と安全性](#)」：AIシステムは、意図しない・予期しない害悪を最小限に抑え、意図しない問題が発生した場合でも堅牢であり、悪意のある第三者による不正使用を可能にするためにAIの使用やパフォーマンスを変更しようとする試みに対して耐性がある仕方で開発・使用されるものとする。
 - c) 「[プライバシーとデータガバナンス](#)」：AIシステムは、既存のプライバシーとデータ保護ルールに従って開発・使用され、品質と完全性の点で高い基準を満たすデータを処理するものとする。
 - d) 「[透明性](#)」：AIシステムは、適切なトレーサビリティと説明可能性を可能にする仕方で開発・使用され、人間がAIシステムと通信や対話していることを認識させ、ユーザーに当該システムの能力と制限について、また影響を受ける人々に彼らの権利について適切に情報提供するものとする。
 - e) 「[多様性、非差別、公平性](#)」：AIシステムは、多様な関係者を包含し、平等なアクセス・ジェンダー平等・文化的多様性を促進する仕方で開発・使用され、EU法や国内法が禁止する差別的影響や不当なバイアスを回避するものとする。
 - f) 「[社会および環境の福祉](#)」：AIシステムは、持続可能で環境に優しい仕方で、またすべての人類に利益をもたらす仕方で開発・使用され、個人・社会・民主主義への長期的な影響をモニターおよび評価するものとする。
- ⇒上記の6原則は、[欧州委員会HLEGの「信頼できるAIのための倫理ガイドライン（Ethics Guidelines for Trustworthy AI）」（2019年4月）](#)で提示された「[信頼できるAIの6要件](#)」に対応している。

- 第10条（データとデータガバナンス）で規定されたプロバイダーの義務に関して、「プロバイダーがデータにアクセスできず、データがディプロイヤーによって独占的に保持されているためにプロバイダーが本条に定められた義務を遵守できない場合、契約に基づいて、ディプロイヤーが本条の違反の責任を負ってもよい」（第10条6a項）という条項を追加。
- ディプロイヤー等がプロバイダーとみなされるケースを追加（第28条1項）。
 - 「第28条 プロバイダー、販売者、輸入者、ディプロイヤー、その他の第三者のAIバリューチェーンに沿った責任
 - 1. 販売者、輸入者、ディプロイヤー、またはその他の第三者は、本規則の目的上、以下のいずれかの状況下ではハイリスクAIシステムのプロバイダーとみなされ、第16条の下でのプロバイダーの義務に従うものとする。
 - （a）市場投入したり、サービス提供したハイリスクAIシステムに、自らの名前または商標を付ける場合。
 - （b）すでに市場投入またはサービス提供されているハイリスクAIシステムに実質的な変更を加え、変更後もハイリスクAIシステムである場合。
 - （ba）すでに市場投入またはサービス提供されているAIシステムであって、ハイリスクと分類されていないもの（一般目的AIを含む）に、ハイリスクAIシステムになるように実質的な変更を加える場合。
 - 2. 第1項の（a）から（ba）で言及されている状況が発生した場合、最初に当該AIシステムを市場投入またはサービス提供したプロバイダーは、本規則の目的上、もはやその特定AIシステムのプロバイダーとはみなされなくなるものとする。（後略）」
- 欧州委員会が、「ハイリスクAIシステムのプロバイダーと、ハイリスクAIシステムで使用または組み込まれるツール・サービス・コンポーネント・プロセス（基盤モデルを含む）を提供する第三者との間の拘束力のないモデル契約条件を開発し、推奨する」旨を追加（第28条2a項）。

- 「AIリテラシー」に関する条項を追加（第4b条）
 - EUと加盟国は、プロバイダー・ディプロイヤー・影響を受ける人々の様々なニーズを考慮し、分野を超えて十分なレベルのAIリテラシーを開発するための措置を促進する。
 - AIシステムのプロバイダーとディプロイヤーは、職員等の技術的知識・経験・教育・訓練やAIシステムが使用される文脈を考慮して、AIシステムの運用と使用を担当する職員等の十分なレベルのAIリテラシーを保証するための措置を講じる。
- 「AIシステムによる影響を受ける人々の権利」を追加（第68a条～68c条）。
 - 国内監督機関に異議を申立てる権利
 - 国内監督機関を相手方とする効果的な司法救済の権利
 - 個人に対する意思決定について説明を受ける権利

- 第71条（罰則）で、禁止AIに対する制裁金額の上限額は上がったが、それ以外の制裁金額は下がっている。

違反事由	欧州議会修正案の制裁金額	（参考）欧州委員会案の制裁金額
第5条で規定された <u>AI慣行の禁止</u> を遵守しない場合。	4000万ユーロ以下の制裁金、または違反者が企業の場合は、直前の会計年度における世界全体における売上総額の7%以下の金額、もしくはいずれか高額の方の制裁金	3000万ユーロ以下の制裁金、または違反者が企業の場合は、直前の会計年度における世界全体における売上総額の6%以下の金額、もしくはいずれか高額の方の制裁金
第10条（ <u>データおよびデータガバナンス</u> ）・第13条（ <u>透明性と情報提供</u> ）で規定された要件を遵守しない場合。	2000万ユーロ以下の制裁金、または違反者が企業の場合は、直前の会計年度における世界全体における売上総額の4%以下の金額、もしくはいずれか高額の方の制裁金	3000万ユーロ以下の制裁金、または違反者が企業の場合は、直前の会計年度における世界全体における売上総額の6%以下の金額、もしくはいずれか高額の方の制裁金（第13条違反は2000万ユーロ以下または4%以下）
<u>本規則の要件または義務</u> を遵守しない場合。（第5条・第10条・第13条を除く）	1000万ユーロ以下の制裁金、または違反者が企業の場合は、直前の会計年度における世界全体における売上総額の2%以下の金額、もしくはいずれか高額の方の制裁金	2000万ユーロ以下の制裁金、または違反者が企業の場合は、直前の会計年度における世界全体における売上総額の4%以下の金額、もしくはいずれか高額の方の制裁金
要求への回答において公認認証機関および国内所轄機関に <u>不正確、不完全、または誤解を招く情報を提供</u> した場合。	500万ユーロ以下の制裁金、または違反者が企業の場合は、直前の会計年度における世界全体における売上総額の1%以下の金額、もしくはいずれか高額の方の制裁金	1000万ユーロ以下の制裁金、または違反者が企業の場合は、直前の会計年度における世界全体における売上総額の2%以下の金額、もしくはいずれか高額の方の制裁金

分類	顔認識関連のAIシステム（欧州委員会案）
①許容できないリスクのAIシステム （禁止AIシステム）	第5条 禁止される人工知能の慣行 1.以下の人工知能の慣行は禁止されるものとする。 （d）<u>公的にアクセス可能な空間における法執行の目的での「リアルタイム」リモート生体識別システムの使用</u>。ただし、そのような使用が以下の目的の1つに厳密に必要な場合を除く。 （i）行方不明の子どもを含む、<u>特定の潜在的な犯罪被害者に対するターゲット化された搜索</u>。 （ii）自然人の<u>生命または身体的安全に対する特定の、実質的かつ差し迫った脅威の防止</u>、または<u>テロ攻撃の防止</u>。 （iii）理事会枠組み決定2002/584/JHAの第2条（2）で言及され、当該加盟国において国内法によって少なくとも<u>3年間の拘禁刑または拘禁命令により罰することができる刑事犯罪の加害者または容疑者の検出、位置の特定、識別、または起訴</u>。
②ハイリスクAIシステム	Annex III 第6条2項で言及されているハイリスクAIシステム 1.自然人の生体識別およびカテゴリーライゼーション （a）自然人に対する<u>「リアルタイム」および「事後」のリモート生体識別</u>に使用されることを目的としたAIシステム。 6.法執行（Law enforcement） （b）法執行機関がポリグラフや同様のツールとして使用したり、自然人の感情状態を検出することを目的としたAIシステム。 7.移住、亡命、国境管理（Migration, asylum and border control management） （a）所轄の公的機関がポリグラフや同様のツールとして使用したり、自然人の感情状態を検出したりすることを目的としたAIシステム。
③透明性の義務のあるAIシステム	第52条 特定のAIシステムに対する透明性の義務 2.<u>感情認識システムまたは生体カテゴリーライゼーションシステムのユーザー</u>は、それに晒されている自然人に、システムの運用について情報提供するものとする。この義務は、刑事犯罪を検出・防止・捜査・起訴するために法律で許可された生体カテゴリーライゼーションに使用されるAIシステムには適用されないものとする。

○欧州議会修正案での追加

- 「公共空間でのリアルタイムリモート生体識別システム」から「法執行の目的で」という限定を削除し、3つの例外も削除
- 「センシティブな属性に基づいて個人を分類する生体カテゴリーライゼーションシステム」を追加
- 「インターネットや監視カメラの映像から顔画像を無差別に収集するAIシステム」を追加
- 「法執行・国境管理・職場・教育において個人の感情を推測するAIシステム」を追加
- 「事後のリモート生体識別システムを介して公共空間の記録映像を分析するAIシステム」を追加（例外有）

- 「感情認識システム」を追加

- 第5条で禁止されていない「感情認識システム」や「生体カテゴリーライゼーションシステム」に対して事前同意を義務化

- 欧州議会の報告書「生体認識と行動検出：公共空間における現在および将来の使用を中心とした生体認識と行動検出技術の倫理的側面の評価」（2021年8月）における[バイOMETリック技術の分類](https://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU(2021)696968)
([https://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU\(2021\)696968](https://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU(2021)696968))
- (1) [認証 \(Authentication\)](#)
 - 認証は「1対1」の比較であり、特定のアイデンティティを持っていると主張する個人の特徴量データ（テンプレート）を、データベースに保存されている当該アイデンティティの特徴量データと照合することで、その主張が正しいかどうかを確認する。
 - スマホのログイン認証、空港の顔認証ゲート、顔認証決済 等
- (2) [識別 \(Identification\)](#)
 - 識別は「1対多」の比較であり、個人から（しばしば本人の意識的協力なく、場合によっては本人の意志に反して）取得された特徴量データを、データベースに保存されている特徴量と照合することで、当該個人のアイデンティティを確立する。
 - リピーター分析、万引犯顔識別、警察によるリモート生体識別 等
- (3) [カテゴライゼーション \(Categorisation\)](#)
 - 個人を年齢、性別、民族などの（長期的な）属性でカテゴライズする。
 - 年代・性別などの属性推定 等
- (4) [検出 \(Detection\)](#)
 - 怒り、疲れ、特定の意図（ex.犯罪を行う意図）、病気など、個人の（しばしば一時的な）状態を検出する。
 - 感情認識システム 等

- EDPB（欧州データ保護会議）は2023年4月26日に、「[法執行分野における顔認識技術の使用に関するガイドライン Ver2.0](#)」を採択した。
 - “Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement Version 2.0”
 - https://edpb.europa.eu/system/files/2023-05/edpb_guidelines_202304_frtlawenforcement_v2_en.pdf
 - 同ガイドライン案（Ver1.0）は2022年5月12日に採択され、同年6月27日までパブリックコンサルテーションに付されていた。
- 同ガイドライン案は、[EUの法執行指令（LED）の下での法執行機関による顔認識技術の使用に関する指針](#)。
 - LED（法執行指令）はGDPR（一般データ保護規則）と同時期に制定された指令で、[犯罪行為の防止、捜査、検知若しくは訴追又は刑罰の執行の目的での所管官庁による個人データ処理に適用](#)される。
 - EDPBは、GDPRの下でのカメラ画像や顔認識技術の取扱いに関する指針として別途、「[ビデオ機器を通じた個人データ処理に関するガイドライン](#)」を2020年1月に公表済み（https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_en_0.pdf）。
- 顔認識（Facial Recognition）は、「認証」と「識別」の2つを指す用語として定義されている。
- [法執行分野における顔認識技術（FRT）のユースケースとして6つ](#)が挙げられ、法的側面からの「可否」を提示。
 - 1. 出入国ゲートでの顔認証 →○
 - 2. 児童誘拐の被害者の顔識別 →○
 - 3. デモ行為を行っている人々やその周辺の映像をDB化し、その中から暴動を行った人を識別するシステム →×
 - 4. 容疑者の画像と犯罪者データベースとの顔照合による識別 →○
 - 5. 公共空間でのリアルタイムのリモート生体識別（顔識別） →×
 - 6. インターネット上で収集した顔画像をDB化し、警察などのユーザーに顔識別サービスを提供 →×
- その他、「[生体カテゴライゼーションシステム](#)」と「[感情認識システム](#)」についても禁止を要求。

- 米国のClearview AIは、[FacebookやGoogle、Venmo、YouTubeなどのウェブサイトから（本人同意なく）取得された顔画像のデータベース](#)を持ち、[警察などの顧客から送信された容疑者などの顔画像をデータベースと照合し、一致した画像と出典元サイトへのリンク情報を提供するアプリケーション](#)を提供。データベースは30億枚以上の画像から構成され、米国FBIや英国国家犯罪対策庁など各国の600以上の法執行機関や、民間企業・学校・銀行などが利用。（<https://forbesjapan.com/articles/detail/35768>、<https://gigazine.net/news/20200707-clearview-ai-end-in-canada/>）
- [EDPB（欧州データ保護会議）](#)は、欧州議員からのClearview AIに関する照会に対し、2020年6月10日に回答を行っている。同回答の中で、EU加盟国の政府機関による同社アプリケーションの利用は以下3つの観点から問題があるとしている。（https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_letter_out_2020-0052_facialrecognition.pdf）
 - 1. EU法や加盟国法の下で構築されたデータベースを用いていない
 - 2. 無差別かつ不正確なデータベースの利用は厳密な必要性和比例性の要件を満たさない
 - 3. EU内の法執行機関から米国の民間企業への越境データ移転に該当する
- [各国のDPA（データ保護監督機関）による執行事例](#)
 - イタリアDPA： 同社に対してGDPR違反で2000万ユーロの制裁金（2022年3月）
 - 英国DPA（ICO）： 同社に対して英国データ保護法制違反で約750万ポンドの制裁金（2022年5月）
 - ギリシャDPA： 同社に対してGDPR違反で2000万ユーロの制裁金（2022年7月）
 - フランスDPA（CNIL）： 同社に対してGDPR違反で2000万ユーロの制裁金（2022年10月）
 - オーストリアDPA： 同社に対してGDPR違反で是正命令（2023年5月）
 - スウェーデンDPA： 同社サービスを使ったスウェーデン警察庁に対して約25万ユーロの制裁金（2021年2月）

- インテリジェントポータブル国境管理システム（Intelligent Portable Border Control System：iBorderCtrl）プロジェクト（<https://cordis.europa.eu/project/id/700626>）は、EUのHorizon 2020フレームワークの下で2013年から2019年の間に実施された、[国境管理における意思決定支援システム](#)の開発を目的とした研究プロジェクトであり、[欺瞞検出（嘘発見）システム](#)が含まれている。EUから450万ユーロ（約5億8000万円）の資金提供を受けていた。ハンガリー、ギリシャ、ラトビアのいくつかの陸路の国境検問所で6ヶ月間のパイロット試験が実施された。その後、同システムは実運用されていない。
- この欺瞞検出ツールは、[EUへの入国者が事前にウェブカメラでアバターとのインタビューを行うことを通じて、「欺瞞のバイオマーカ」、すなわち欺瞞（嘘）に関連する顔の非言語的な38個の微細な表情やジェスチャー（目の瞬き、顔の赤みの増加、頭の動きの方向など）](#) を分析。研究者たちは、欺瞞検出の正確性が73～75%と報告。
- 欧州議会の報告書「EU国境におけるAI：アプリケーションの概要と主要イシュー」（2021年7月）は、同プロジェクトがその[科学的妥当性や信頼性に関して重大な批判](#)を引き起こしたとする。科学的妥当性に関しては、米国のバレット教授等による2019年の文献レビューを引用しながら、iBorderCtrlのような[顔の表情から感情を検出することを目的としたAIシステムの科学的根拠について大きな懸念](#)が示されているとする。
- 同報告書は、現実状況でシステムを展開するときに、例えば[システムを騙すことを積極的に求めている（そして自分自身を訓練している）人間に対処する場合には、信頼性の問題が生じる](#)ことも指摘。
- 欧州議会の「刑法におけるAIと刑事事件における警察と司法機関によるAIの利用に関する報告書」（2021年7月）および決議（同年10月）でも、iBorderCtrlを[自動インタビューに基づいて旅行者をプロファイリングする「スマート嘘発見システム」](#)とみなし、EU国境にAIを展開するHorizon 2020の下で資金提供された研究プロジェクトに強い懸念が示されている。

- EU理事会はチェコ議長国の下で2022年12月6日に、AI規則案に対する合意案（general approach）を採択。主な内容は以下。
（<https://www.consilium.europa.eu/en/press/press-releases/2022/12/06/artificial-intelligence-act-council-calls-for-promoting-safe-ai-that-respects-fundamental-rights/>）
 - 「AIシステムの定義」を、機械学習アプローチや、論理および知識ベースのアプローチによって開発されたシステムに限定。
 - 「許容できないリスクのAIシステム（禁止AI）」として、ソーシャルスコアリングにAIを使用することの禁止を民間企業にも拡大。
 - 重大な基本的権利の侵害やその他の重大なリスクを引き起こす可能性が低いAIシステムまで「ハイリスクAI」とみなされないように、「ハイリスクAIシステム」の分類の上に水平レイヤーを追加。
 - 「ハイリスクAIシステムに対する要件」を明確化。
 - AIシステムが様々な目的で使用されうる状況（一般目的AI）や、一般目的AI技術が他のハイリスクAIシステムに統合されている状況を考慮して、新しい規定を追加。そのような場合、ハイリスクAIシステムに対する一定の要件が一般目的AIシステムにも適用されることを規定。ただし、これらの要件を直接適用する代わりに、実施法令が、コンサルテーションと詳細な影響評価に基づき、またこれらのシステムの特徴や関連するバリューチェーン・技術的な実現可能性・市場と技術の発展を考慮して、一般目的AIシステムに関連してこれらの要件を適用する方法を規定するものとされた。
 - AI規則の範囲を明確化（例えばAI規則の範囲から国家安全保障、防衛、軍事目的を明示的に除外）し、法執行機関に関連する規定を明確化。
 - AI規則のコンプライアンスフレームワークを簡素化。
 - 透明性を高め、ユーザーの苦情を可能とするための新しい規定を追加。
 - イノベーションを支援する措置（AI規制サンドボックス等）に関する規定を大幅に変更。

• 米国

- 大統領府OSTP（科学技術政策局）が2022年10月、「[AI権利章典の青写真](#)」（Blueprint for an AI Bill of Rights）を公表。
 - 5原則とプラクティス集で構成。
- NIST（国立標準技術研究所）が2023年1月、「[AIリスク管理フレームワーク1.0](#)」を公表。
- 商務省NTIA（国立電気通信情報局）が2023年4月13日、「[AIアカウンタビリティポリシーに関するRFC](#)」を公表。意見期間は6月12日まで。
 - AIの信頼性と安全性を確保するために、[AIの監査・評価・認証等](#)に関するどのような政策が必要か。
- バイデン政権は5月4日、[米国人の人権と安全を保護するための責任あるAIイノベーションの推進計画](#)を公表。
 - 企業はAI製品をディプロイ/公開する前に[それらが安全であることを保証する責任](#)を持つ。
 - 生成AIをScale AIが開発した[評価プラットフォームで公開評価](#)。評価軸はAI権利章典とNISTフレームワーク。
 - バイデン大統領がIT企業の責任を規定した法案策定を連邦議会に呼びかけているとの報道（日経新聞）も。

• 英国

- DCMS（デジタル文化メディアスポーツ省）が2022年7月、[データ改革法案（データ保護・デジタル情報法案）](#)を議会に提出。
 - AIに関しては法規制ではなく白書で政策を示すとされていた。
 - 2023年3月に、EUからの十分性認定の維持等に配慮した[修正法案（No.2法案）](#)を提出。
- DCMSが2023年3月29日、[AI白書「AI規制へのイノベーション寄りアプローチ](#)（A pro-innovation approach to AI regulation）」を公表。意見期間は6月21日まで。
- ICO（情報コミッショナーオフィス）が2023年4月3日、「[生成AI：開発者とユーザーが自問する必要のある8つ質問](#)」というガイドを公表。

- 米国大統領府の[科学技術政策局（OSTP）](https://www.whitehouse.gov/ostp/ai-bill-of-rights/)は2022年10月4日、「[AI権利章典の青写真](#)」（Blueprint for an AI Bill of Rights）を公表。（<https://www.whitehouse.gov/ostp/ai-bill-of-rights/>）
 - OSTPは大統領府（ホワイトハウス）内に設置されている事務局の1つで、連邦政府内で科学技術政策の推進・調整役を担う。
 - 2021年10月にAI権利章典を策定する計画を公表し、「AIは人間を取り巻く世界を変革しているが、差別やプライバシー侵害など様々な問題も引き起こしているため、[人間が作り上げた強力な技術（AIなどのデータ駆動型技術）から人間自身を守るための権利章典が必要](#)」としていた）
- 「AI権利章典の青写真」は大きくは以下の2つから構成される。
 - AIシステムの設計・使用・ディプロイメントの指針となる「[5つの原則](#)」
 - AI権利章典の青写真を実践するためのプラクティス集「[原則からプラクティスへ](#)」
- AI権利章典の青写真（5原則とプラクティス集）は、[政府機関、民間企業を含むあらゆる組織](#)における、[以下の2つの条件を満たすシステム](#)に適用されるべきとされている。（[法的拘束力はない](#)。）
 - (1)自動化されたシステム、かつ
 - (2)米国市民の[権利](#)、[機会](#)、重要なリソースやサービスへの[アクセス](#)に意味のある影響を与える可能性があるもの
- 5つの原則
 - (i) [安全で効果のあるシステム](#)（Safe and Effective Systems）
 - (ii) [アルゴリズムによる差別からの保護](#)（Algorithmic Discrimination Protections）
 - (iii) [データプライバシー](#)（Data Privacy）
 - (iv) [通知と説明](#)（Notice and Explanation）
 - (v) [人間による代替手続き、検討、フォールバック](#)（Human Alternatives, Consideration, and Fallback）

- 「生成AI：開発者とユーザーが自問する必要がある8つ質問」 <https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2023/04/generative-ai-eight-questions-that-developers-and-users-need-to-ask/>
 - 生成AIという技術は斬新だが、[データ保護法の原則は変わらない](#)。生成AIを開発または使用する組織は、[データ保護バイデザイン・バイデフォルトアプローチ](#)を採用して、データ保護の義務を最初から検討すべき。
 - 個人データを処理する[生成AIを開発または使用する組織](#)は、以下の8つの質問を自問する必要がある。
- 1. 個人データを処理する[適法性の根拠](#)は何か？
 - 個人データを処理する場合は、「同意」や「正当な利益」など、適切な適法性の根拠を特定しなければならない。
- 2. あなたは[管理者、共同管理者、処理者](#)のいずれなのか？
 - 個人データを利用して生成AIを開発している場合、データ管理者としての義務。他社開発モデルを使用している場合も、管理者/共同管理者/処理者に該当する可能性。
- 3. [データ保護影響評価](#)（DPIA）を準備したか？
 - 個人データの処理を開始する前に、DPIAを通じてデータ保護のリスクを評価し、軽減しなければならない。データ処理とその影響の進展に伴ってDPIAを更新すべき。
- 4. [透明性](#)をどのように保証するか？
 - 原則的にデータ処理に関する情報を公開しなければならない。過大な負担がかからない場合は、この情報をデータ主体に直接伝えなければならない。
- 5. [セキュリティリスク](#)をどのように軽減するか？
 - 個人データ漏えいのリスクに加えて、モデル反転や、メンバーシップ推論、データポイズニング、その他の敵対的攻撃のリスクを考慮して、軽減すべき。
- 6. [不必要な処理](#)をどのように制限するか？
 - 明示した目的を達成するのに十分なデータのみを収集しなければならない。データは関連性があり、必要なものに限定されているべき。
- 7. [個人からの権利要求](#)にどのように対応するか？
 - アクセス、訂正、消去その他の情報権に関する個人からの要求に対応できなければならない。
- 8. [完全自動意思決定](#)を行うために生成AIを使用するか？
 - 完全自動意思決定が法的効果や同様に重要な影響を及ぼす場合（重要な医療診断等）、個人はUK GDPR第22条に基づく権利を有する。

- 小泉 雄介 （株）国際社会経済研究所 主幹研究員 yusuke-koizumi@nec.com
- 専門領域：
 - プライバシー/個人情報保護、国民ID/マイナンバー制度、海外政策動向調査、途上国市場調査
- 略歴：
 - 1998年 （株）NEC総研入社 ・ 2008年7月 日本電気（株）に出向
 - 2010年7月 （株）国際社会経済研究所（旧NEC総研）に復帰
 - 2012年～ 電子情報技術産業協会（JEITA）個人データ保護専門委員会客員
- 主な著書
 - 『国民ID 導入に向けた取り組み』（共著、NTT出版、2009年）
 - 『[現代人のプライバシー](#)』（共著、NEC総研、2005年）
 - 『経営戦略としての個人情報保護と対策』（共著、工業調査会、2002年） 等
- 主な論文
 - 「[『快適で安全』な監視社会 一個人の自由が保障されなくていいのか](#)」（岩波「世界」2019年6月号）
 - 「[感情認識の倫理的側面：データ化される個人の終着点](#)」（日本セキュリティ・マネジメント学会誌2022年度第2号）
 - 「[中央銀行デジタル通貨における個人情報保護と日本での発行モデル](#)」（同学会誌2021年度第2号）
 - 「[AI社会における「自由」と「安全」のトレードオフ：顔認識技術のケーススタディ](#)」（同学会誌2020年度第2号）
 - 「[監視社会とプライバシー：リトルブラザーの共存する世界へ](#)」（同学会誌2018年度第2号） 等

I I S E