

欧州AI規則案の概要

2021年6月21日

(株)国際社会経済研究所

小泉 雄介

yusuke-koizumi@nec.com

欧州AI規則案の日本企業への影響

- EUの規制だが、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）やユーザー（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ー副委員長は2021年5月に、「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。
 - ※ ただし、「我が国のAIガバナンスの在り方 ver.1.0」（2021年1月公表）では、「AI システムに対する横断的な義務規定は現段階では不要であると考えられる」とされ、AIに対しては法的拘束力のないソフトローで対応する方向性が示されている。
- 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。

欧州AI規則案：これまでの経緯

日付	欧州委員会等の取組み
2018年3月9日	欧州委員会の科学新技術倫理グループ(EGE)が「AI・ロボティクス・自律システムに関する宣言」を公表。
2018年4月25日	欧州委員会はAI戦略「欧州のAI」を公表。
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。
2019年後半	上記AI倫理ガイドラインのアセスメントリストについて、350以上の組織がテストを行い、フィードバックを回答。
2020年7月17日	HLEGはフィードバックに基づき、アセスメントリストの改訂版を公表。
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。
2020年7月23日	欧州委員会はAIホワイトペーパーを補完する「Inception Impact Assessment」を公表。
2020年10月20日	欧州議会は「AI・ロボティクス・関連技術の倫理フレームワークに関する欧州委員会への勧告」を決議。
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。

【ご参考】 欧州委員会のAI倫理ガイドライン（2019年4月）

○ AIによって生じる重大な懸念として以下5つを挙げている

（1） AIによる個人識別と追跡

- AIは、公共機関や民間企業による特定個人の識別を、これまで以上に効率化する。比例原則に従ったAI技術の使用は、欧州市民の自律性を維持するために必要である。個人の識別と個人の追跡とを区別すること、また個人を標的としたサーベイランスとマスサーベイランスとを区別することは、信頼できるAIの達成にとって極めて重要。
- オンラインサービスにおけるインフォームドコンセントが示すように、消費者は考慮することなく同意を与えている。このことに鑑みれば、企業や政府は、AI技術による自動識別に対して市民が有効な同意を与えることを可能とする、完全に新しく実地的な手段を開発する倫理的な義務がある。
- AI識別技術の特筆すべき事例は、顔認識やその他のバイOMETリックデータを用いた非自発的な識別手段である。自動識別技術の適用が既存の法律等によって明確に保証されない場合には、本人同意が得られない限り、このような技術は法律・倫理の両面において大きな懸念をもたらす。

（2） 隠されたAIシステム： 自分が人間とやり取りしているのか、AIとやりとりしているのか、分からなくなること

（3） 市民の大規模なスコアリング： cf. 中国の「社会信用システム」

（4） 自律型致死兵器システム（LAWS）

（5） 潜在的な長期的懸念： 人工意識の開発、主観的体験を持ったAIシステムの開発など

【ご参考】 欧州委員会のAIホワイトペーパー（2020年2月）

○ AIのもたらすリスクとして以下を挙げている

① 基本的な人権に対するリスク：個人データとプライバシー保護、非差別を含む

- AIを用いた意思決定等を理解したり、異議申し立てを行うことの困難さ。
- AIが政府機関等によって大規模監視の目的で利用されたり、雇用主によって従業員の行動を監視する目的で利用されること。
- AIが匿名化されたデータの再識別に利用されること。
- オンライン仲介事業者（プラットフォーム）によって、ユーザ企業の情報を優先させたり、コンテンツの調整を行うために利用されること。
- 人間の意思決定と同様なバイアスがAIに存在しうること。
- 不透明さ（「ブラックボックス効果」）、複雑性、予測不可能性、部分的に自律的なふるまいなど、AI技術の特徴は、既存のEU法令の規則の遵守を証明することを困難にしたり、それらの有効な執行を妨げる恐れがある。

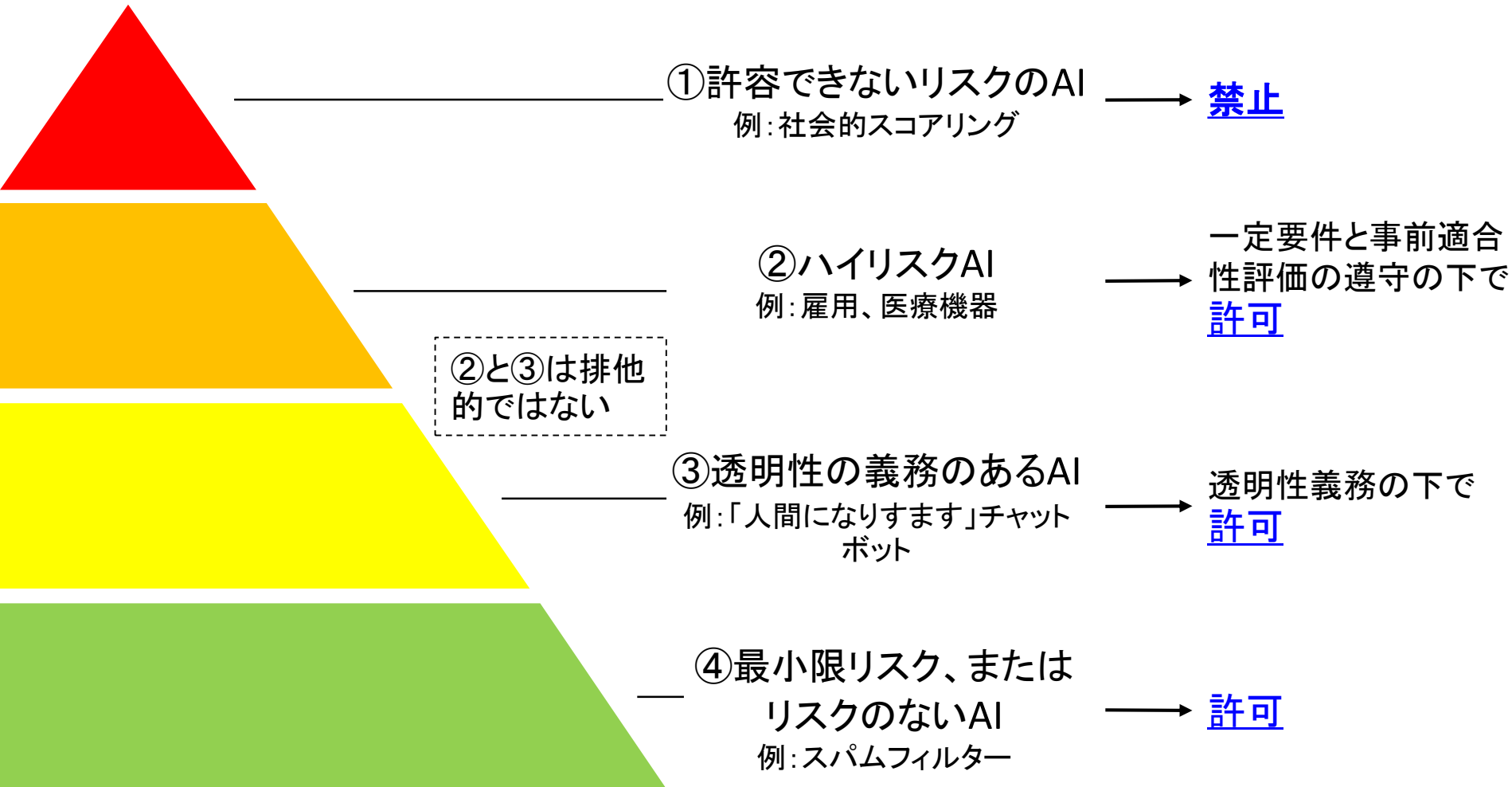
② 製品安全性と製造物責任に関連したリスク

- AI技術は、製品やサービスに埋め込まれた際に、利用者に新たな安全性のリスクを提示する恐れがある。例えば物体認識技術における欠陥の結果、自動運転車が道路上の対象物を間違えて認識し、傷害や物的損害を伴う事故を引き起こしうる。
- 製造物責任指令の下では製造者は欠陥製品に起因する損害に対して責任を負うが、自動運転車のようなAIベースのシステムでは、当該製品に欠陥があること、そして発生した損害との間に因果的なつながりがあることを証明することが難しい。

欧州AI規則案： リスクベースアプローチ

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 (2021年4月21日公表)

(<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELLAR%3Ae0649735-a372-11eb-9585-01aa75ed71a1>)



出典：欧州委員会資料を和訳、加筆

欧州AI規則案： AIの定義

- 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

欧州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。

欧州AI規則案： ① 許容できないリスクの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は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は、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。 (後略)	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。

欧州AI規則案： ②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

欧州AI規則案： ②ハイリスクAIシステム（スタンドアロン）

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。

欧州AI規則案： ②ハイリスクAIシステム（スタンドアロン）

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

- (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。

欧州AI規則案： ②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</u> <u>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

欧州AI規則案： ②ハイリスクAIシステムの要件

○データおよびデータガバナンス（第10条）

- 学習データ（等）のガバナンスにあたっては、潜在的なバイアスを吟味する。
 - 想定される例： 雇用AIシステム用の学習データに、従来の採用者のデータのみを用いると、従来の採用者層（例えば白人男性）に有利なバイアスが働く恐れがある。
- 学習データ（等）は、関連性があり、代表的で、エラーがなく、完全なものとする。
 - 想定される例： 空港の出入国管理での顔認証システム用の学習データには、日本人のみならず、諸外国・人種の人々の顔データも用いる。
- 学習データ（等）は、ハイリスクAIシステムの使用が意図されている特定の地理的、行動的、または機能的な条件に固有の特性または要素を、考慮に入れる。
 - 想定される例： 自動運転システム用の学習データには、当該国の交通ルールや道路状況等に基づいたものを用いる。

欧州AI規則案： ②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）

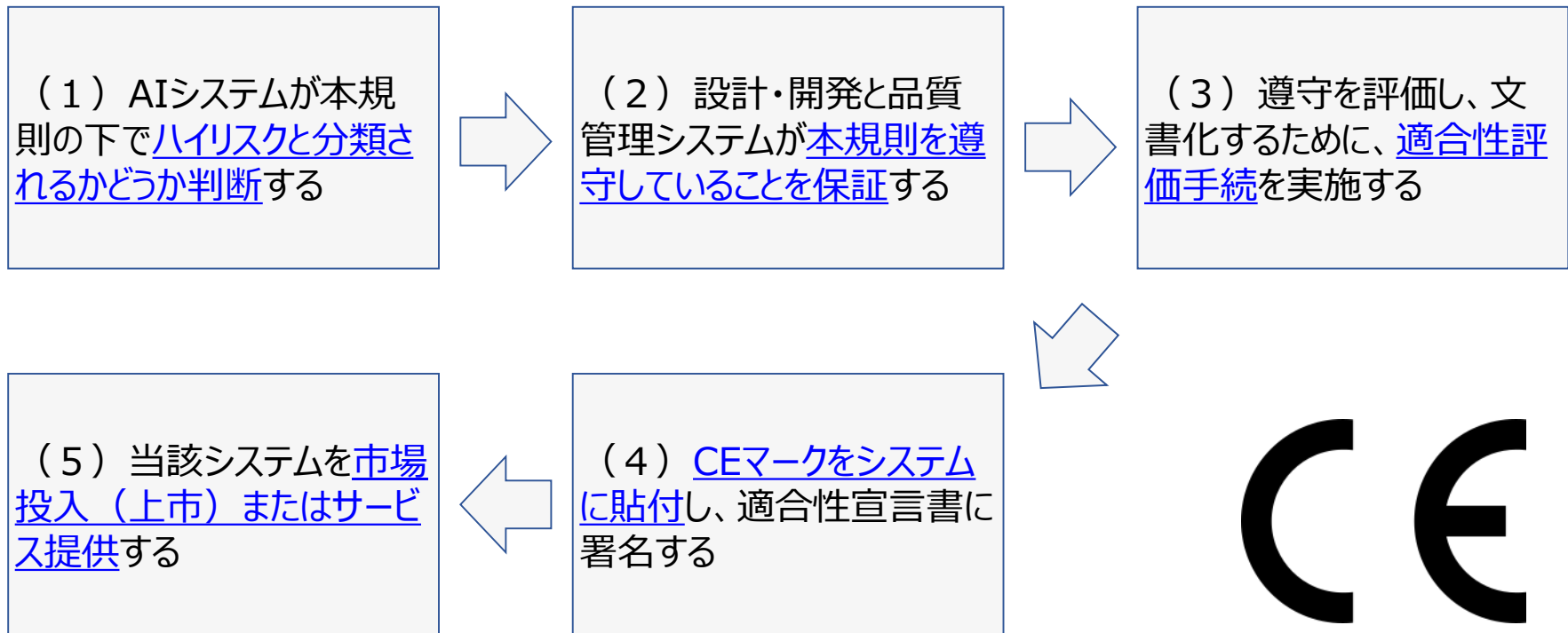
プロバイダーの義務	▶ 組織内で品質管理システムを確立し、実施する ▶ 技術文書を作成し、更新する ▶ ユーザーがハイリスクAIシステムの運用をモニターできるようにログを保管する ▶ 適合性評価を実施し、実質的な変更がある場合は当該システムの再評価を行う ▶ EUデータベースにAIシステムを登録する ▶ CEマークを貼付し、適合性宣言書に署名する ▶ 市場流通後モニタリングを実施する ▶ 市場監視機関と協力する
ユーザーの義務	▶ 使用説明書に従ってAIシステムを運用する ▶ AIシステムを使用する際に人間による監督を保証する ▶ 可能なリスクに対して運用をモニターする ▶ 重大なインシデント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

欧州AI規則案： ②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。



CEマーク

出典：欧州委員会資料を和訳

欧州AI規則案：②ハイリスクAIシステムのライフサイクルと関連義務

○ハイリスクAIシステムのライフサイクルと関連義務

関連義務	説明
要件に沿った設計	AIシステムが <u>意図された目的で一貫して機能</u> することと、本規則で規定された <u>要件を遵守</u> していることを保証する。
適合性評価	<u>事前に</u> 適合性評価を実施する。
市場流通後モニタリング	プロバイダーは、AIシステムの信頼性・パフォーマンス・安全に関する <u>データ</u> をライフタイムに渡って <u>積極的かつ体系的に収集・文書化・分析</u> し、AIシステムが <u>本規則を遵守していることを継続的に評価</u> する。
インシデント報告	<u>基本的権利の侵害につながる重大なインシデントと誤動作を報告する</u> （所轄機関による調査の基礎として）
新たな適合性評価	プロバイダーや第三者による「 <u>実質的な変更</u> 」がある場合は <u>新たな適合性評価</u> を実施する。 （実質的な変更とは、AIシステムの意図された目的の変更、または本規則の遵守に影響を与える変更を意味する。） 変更が、 <u>継続的に学習し続けるAIシステム</u> に対してプロバイダーが示す「 <u>事前定義範囲</u> 」を超える場合を含む。

出典：欧州委員会資料を和訳

欧州AI規則案： ③④ハイリスクでないAIシステム

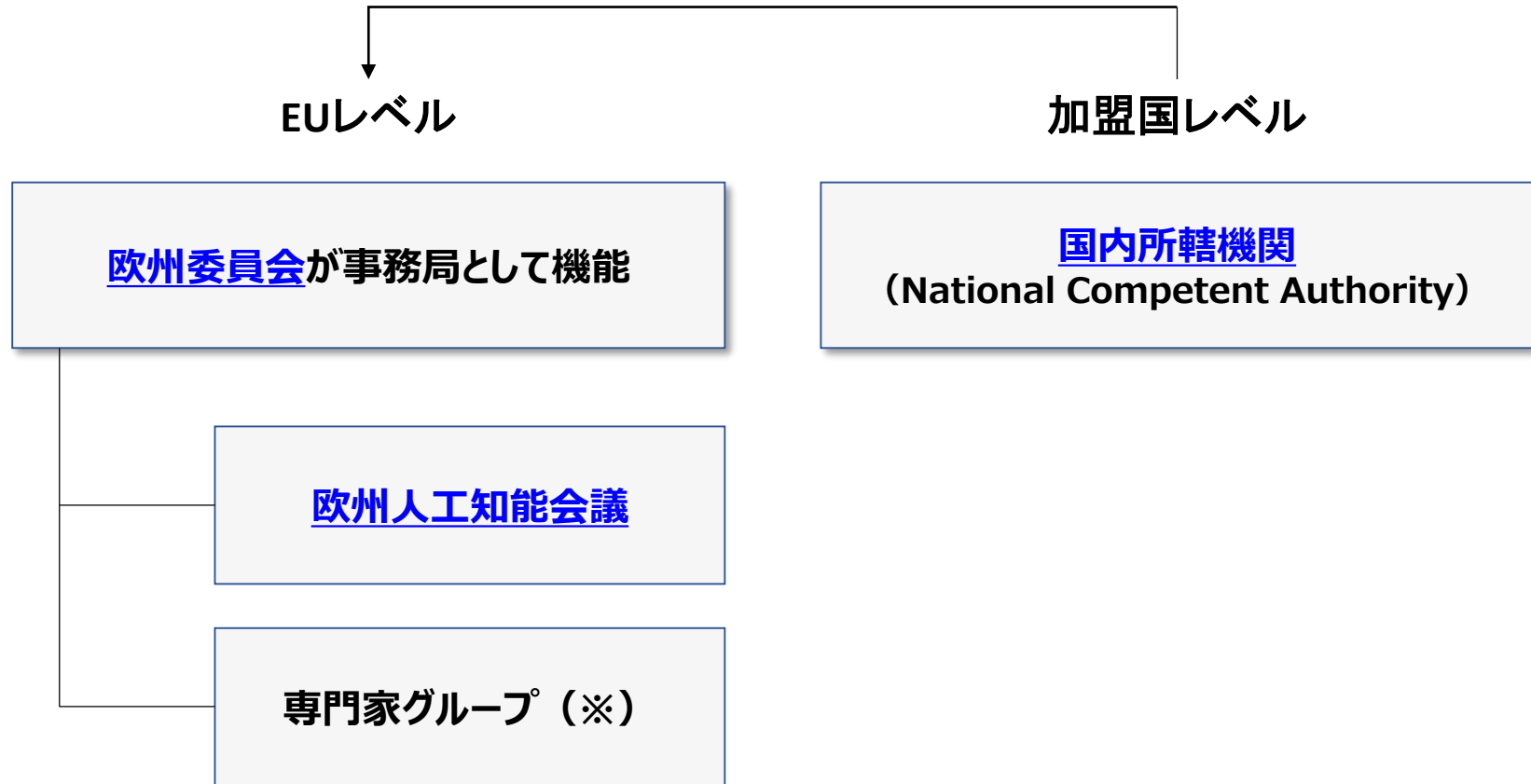
③特定のAIシステムに対する透明性の義務（第52条）

- 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）

④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AI規則案： ガバナンス構造



※欧州AI規則案では規定されていないが、欧州委員会は施行プロセスで専門家グループを導入予定

出典: 欧州委員会資料を和訳

欧州AI規則案： 罰則

・ 罰則（第71条）

違反事由	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。 - 第10条で規定された要件（<u>データおよびデータガバナンス</u>）を遵守しない場合。	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
<u>本規則の要件または義務</u> を遵守しない場合。 （第5条および第10条を除く）	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。	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

欧州AI規則案：顔認識関連のAIシステム

分類	顔認識関連のAIシステム
①許容できないリスクの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。

【ご参考】欧州AI規則案：顔認識関連規定

① 許容できないリスクのAIシステム：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 関連

○条文

第3条 定義

(36)「リモート生体識別システム (remote biometric identification system)」とは、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システムのユーザーが持つことなく、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システムを意味する。

(37)「リアルタイム (real-time)」リモート生体識別システムとは、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を意味する。これには、即時の識別だけでなく、迂回（訳注：本規則のすり抜け）を防ぐために、限定的な短い遅延も含まれる。

(38)「事後の (post)」リモート生体識別システムとは、「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を意味する。

(39)「公的にアクセス可能な空間 (publicly accessible space)」とは、アクセスに一定の条件が課されうるか否かに関わらず、一般市民がアクセスできる場所を意味する。

第5条 禁止される人工知能の慣行 (Prohibited Artificial Intelligence Practices)

1. 以下の人工知能の慣行は禁止されるものとする。

(d) 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。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、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。

(ii) 自然人の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、またはテロ攻撃の防止。

(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。

2. 第1項(d)で言及されている目的のいずれかの法執行を目的とした、公的にアクセス可能な空間での「リアルタイム」リモート生体識別システムの使用は、以下の要素を考慮に入れるものとする。

(a) 使用の可能性を生じさせる状況の性質。特に当該システムの使用がない場合に引き起こされる危害の重大性、可能性および規模。

(b) 関係するすべての個人の権利と自由に対する当該システムの使用の結果。特にそれらの結果の重大性、可能性および規模。

【ご参考】欧州AI規則案：顔認識関連規定

第5条 禁止される人工知能の慣行（続き）

2.(続き)

さらに、第1項(d)で言及されている目的のいずれかの法執行を目的とした、公的にアクセス可能な空間での「リアルタイム」リモート生体識別システムの使用は、特に時間的・地理的・個人的な制限に関して、その使用に関連した必要かつ比例的な保護措置と条件を遵守するものとする。

3.第1項(d)および第2項に関して、公的にアクセス可能な空間での「リアルタイム」リモート生体識別システムの法執行を目的とした個々の使用は、使用が行われる加盟国の司法当局または独立行政当局によって与えられる事前の承認に服するものとする。そのような承認は、合理的な要求に応じて、また第4項で言及されている国内法の詳細なルールに従って発行される。ただし、緊急の正当な理由がある状況では、当該システムの使用は承認なしに開始することができ、承認は使用中または使用後に要求することができる。

所轄の司法当局または行政当局は、提示された客観的な証拠または明確な兆候に基づいて、当の「リアルタイム」リモート生体識別システムの使用が、要求で特定された第1項(d)の目的の1つを達成するために必要であり比例的であることが認められる場合にのみ承認を与えるものとする。要求(への承認)を決定する際に、所轄の司法当局または行政当局は、第2項で言及されている要素を考慮に入れるものとする。

4.加盟国は、第1項(d)、第2項および第3項に記載された制限内および条件下で、公的にアクセス可能な空間での法執行の目的での「リアルタイム」リモート生体識別システムの使用を完全または部分的に承認する可能性を提供することを決定できる。当該加盟国は、国内法において、第3項で言及されている承認の要求、発行、行使、それに関連する監督に必要な詳細ルールを定めるものとする。また、それらのルールは、第1項(d)にリストされているどの目的について、同号(iii)で言及されているどの刑事犯罪なのかを含めて、所轄当局がそれらのシステムの法執行の目的での使用を承認できるのかを特定するものとする。

○前文

(8)(前略)

「リアルタイム」システムの場合、生体データのキャプチャ、比較、および識別は、すべて瞬時に、ほぼ瞬時に、またはいずれにしても大幅な遅延なしに行われる。この点で、わずかな遅延を提供することにより、当のAIシステムの「リアルタイム」使用に関する本規則のルールを回避する余地はないはずである。「リアルタイム」システムでは、カメラや同様の機能を備えた他のデバイスによって生成された、ビデオ映像などの「ライブ」または「ほぼライブ」の素材を使用する。対照的に、「事後」システムの場合、生体データはすでにキャプチャされており、比較と識別は大幅な遅延の後にのみ行われる。これには、当該システムを使用する前に、関係する自然人に関して、CCTVやプライベートデバイスによって生成された写真やビデオ映像などの素材が含まれる。

【ご参考】欧州AI規則案：顔認識関連規定

(18)法執行の目的で公的にアクセス可能な空間で自然人を「リアルタイム」でリモート生物識別するためのAIシステムの使用は、人口の多くの部分の私的生活に影響を与え、常時監視されている感覚を生じさせ、集会の自由やその他の基本的権利の行使を抑止する(萎縮させる)可能性がある範囲で、関係する個人の権利と自由に特に侵害するものと考えられている。さらに、影響の即時性と、「リアルタイム」で動作するそのようなシステムの使用に関して、更なるチェックや修正の機会が限られていることは、法執行活動に関係する人々の権利と自由に対するリスクを高める。

(19)したがって、法執行の目的でこれらのシステムを使用することは禁止されるべきである。ただし、実質的な公共の利益を達成するために使用が厳密に必要であり、その重要性がリスクを上回る、3つの限定列举され、狭く定義された状況を除く。(後略)

(20)これらのシステムが責任ある比例的な仕方で使用されることを保証するために、これらの3つの限定列举され、狭く定義された状況のそれぞれにおいて、特定の要素を、特に使用の要求を生じさせる状況の性質と、関係する全ての個人の権利と自由のための使用の結果、および使用に備えられた保護措置と条件を考慮に入れるべきであることを確立することも重要である。さらに、法執行の目的で公的にアクセス可能な空間での「リアルタイム」リモート生体識別システムの使用は、特に脅威・被害者・加害者に関する証拠または兆候を考慮して、時間と空間の適切な制限に服するべきである。個人の参照データベースは、上記の3つの状況のそれぞれのユースケースごとに適切であるべきである。

(23)法執行の目的で、公的にアクセス可能な空間で自然人を「リアルタイム」でリモート生体識別するためのAIシステムの使用には、必然的に生体データの処理が含まれる。特定の例外を条件として、TFEU(欧州連合の機能に関する条約)第16条に基づきそのような使用を禁止する本規則のルールは、指令(EU)2016/680(警察・刑事司法データ保護指令)の第10条に含まれる生体データの処理に関するルールに関して特別法として適用するべきである。これらにより、徹底的な仕方、そのような使用と生体データの処理が規制される。(後略)

【ご参考】欧州AI規則案：顔認識関連規定

②ハイリスクAIシステム：「リアルタイム」および「事後」のリモート生体識別システム 関連

○条文

第3条 定義（再掲）

(36)「リモート生体識別システム(remote biometric identification system)」とは、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システムのユーザーが持つことなく、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システムを意味する。

(37)「リアルタイム(real-time)」リモート生体識別システムとは、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を意味する。これには、即時の識別だけでなく、迂回(訳注:本規則のすり抜け)を防ぐために、限定的な短い遅延も含まれる。

(38)「事後の(post)」リモート生体識別システムとは、「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を意味する。

第6条 ハイリスクAIシステムの分類ルール

2.第1項で言及されているハイリスクAIシステムに加えて、AnnexIIIで言及されているAIシステムもハイリスクとみなされるものとする。

○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

第6条2項に従うハイリスクAIシステムは、以下の分野のいずれかに記載されたAIシステムである。

1.自然人の生体識別およびカテゴライゼーション(Biometric identification and categorisation of natural persons)

(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。

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。

【ご参考】欧州AI規則案：顔認識関連規定

○条文

第12条 記録保管(Record-keeping)

4. [AnnexIIIの第1項\(a\)で言及されているハイリスクAIシステムの場合、ログ機能](#)は少なくとも以下を提供するものとする。
- (a) システムの各使用期間の記録(各使用の開始日時および終了日時)。
 - (b) 入力データがシステムによってチェックされた参照データベース。
 - (c) 検索によって一致が得られた入力データ。
 - (d) 第14条(5)で言及されている、結果の検証に関与する自然人の身元。

第14条 人間による監督(Human oversight)

3. 人間による監督は、以下の1つまたは全ての措置を通じて保証されるものとする。
- (a) 市場投入またはサービス提供前にプロバイダーによって特定され、技術的に実現可能な場合、プロバイダーによってハイリスクAIシステムに組み込まれる措置。
 - (b) 市場投入またはサービス提供前にプロバイダーによって特定され、ユーザーによって実装されるのが適切な措置。
5. [AnnexIIIの第1項\(a\)で言及されているハイリスクAIシステムの場合、第3項で言及されている措置は、さらに、少なくとも2人の自然人によって検証および確認](#)されない限り、当該システムから得られた識別に基づいてユーザーが行動または意思決定を行わないことを保証するものとする。

第43条 適合性評価

1. [AnnexIIIの第1項にリストされているハイリスクAIシステムの場合](#)であって、プロバイダーが本編第2節で規定されている要件の遵守を示す際に第40条で言及されている調和標準または(該当する場合)第41条で言及されている共通仕様を適用する場合、プロバイダーは以下の手順のいずれかに従うものとする。
- (a) AnnexVIで言及されている、[内部統制に基づく適合性評価手続](#)。
 - (b) AnnexVIIで言及されている、[公認認証機関が関与する、品質マネジメントシステムの評価および技術文書の評価に基づく適合性評価手続](#)。

プロバイダーが本編第2節で規定されている要件を遵守していることを示す際に第40条で言及されている調和標準を適用しないか、部分的にのみ適用する場合、またはそのような調和標準が存在せず、第41条で言及されている共通仕様を利用できない場合、プロバイダーはAnnexVIIIに記載されている適合性評価手続に従うものとする。AnnexVIIで言及されている適合性評価手続の目的で、プロバイダーは公認認証機関のいずれかを選択することができる。ただし、システムが法執行機関、入国管理局、亡命(asylum)当局、またはEUの機関・組織・部局によって使用されることを意図している場合は、該当する場合、第63条(5)または(6)で言及されている市場監視機関が、公認認証機関として機能するものとする。

【ご参考】欧州AI規則案：顔認識関連規定

○前文

(24)本規則で規制される法執行の目的で公的にアクセス可能な空間での「リアルタイム」リモート生体識別システムの使用に関連する場合を除き、生体識別のためのAIシステムの使用に関連する生体データおよびその他の個人データの処理は、AIシステムが法執行以外の目的で公的にアクセス可能な空間で所轄機関によって使用される場合を含め、規則(EU) 2016/679(GDPR)の第9条(1)、規則(EU) 2018/1725の第10条(1)、指令(EU) 2016/680(警察・刑事司法データ保護指令)の第10条に基づくすべての要件を引き続き遵守すべきである。

(33)自然人のリモート生体識別を目的としたAIシステムの技術的な不正確性は、バイアスのかかった結果につながり、差別的な影響をもたらす恐れがある。これは、年齢、民族、性別、障害に関して特に関連性が高い。したがって、「リアルタイム」および「事後」のリモート生体識別システムは、ハイリスクとして分類すべきである。それらがもたらすリスクを考慮して、両方のタイプのリモート生体識別システムは、ログ機能と人間による監視に関する特定の要件に従うべきである。

③透明性の義務のあるAIシステム：感情認識システム・生体カテゴライゼーションシステム 関連

○条文

第3条 定義

(34)「感情認識システム (emotion recognition system)」とは、生体データに基づいて自然人の感情または意図を識別または推測することを目的としたAIシステムを意味する。

(35)「生体カテゴライゼーションシステム (biometric categorisation system)」とは、生体データに基づいて、性別、年齢、髪の色、目の色、入れ墨、民族的出自、性的指向などの特定のカテゴリーに自然人を分類することを目的としたAIシステムを意味する。

第52条 特定のAIシステムに対する透明性の義務

2.感情認識システムまたは生体カテゴライゼーションシステムのユーザーは、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。

説明者の略歴

○小泉 雄介

株式会社 国際社会経済研究所 主幹研究員 <https://www.i-ise.com/jp/about/researcher/koizumi.html>
yusuke-koizumi@nec.com

・ 専門領域：

- ・ 個人情報保護/プライバシー、監視社会、電子政府（国民ID/マイナンバー制度）、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）パブリックサービス推進本部に出向
- ・ 2010年7月（株）国際社会経済研究所（旧NEC総研）に復帰

・ 主な著書

- ・ 『国民ID 導入に向けた取り組み』（共著、NTT出版、2009年）
- ・ 『ブログ・SNS利用者の実像』（共著、NEC総研、2006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）

・ 主な論文・解説

- ・ 「『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）
- ・ 「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」（日本セキュリティ・マネジメント学会誌2020年9月号）
- ・ 「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」（日本セキュリティ・マネジメント学会誌2018年9月号）
- ・ 「ICT世界の潮流パートⅦ：欧米における監視カメラ・顔認識技術の規制（上・下）」（日刊工業新聞2019年10月）
- ・ 「ICT世界の潮流パートⅥ：AIにおけるプライバシー問題（上・下）」（日刊工業新聞2018年8月）
- ・ 「米国における顔認識技術とプライバシー保護」（画像ラボ2018年2月号）
- ・ 「英国における監視カメラと顔認識の動向」（画像ラボ2017年3月号）
- ・ 「プライバシー影響評価（PIA）の海外動向と日本への応用」（日本データ通信2017年3月号）
- ・ 「EUデータ保護規則案の動向と個人データ越境移転」（ITUジャーナル2015年11月号）
- ・ 「マイナンバー制度とは」（日本経済新聞2013年4月7日「今を読み解く」に掲載）
- ・ 「EUデータ保護指令の改定と日本企業への影響」（CIAJ Journal 2012年6月号） 等



国際社会経済研究所

Institute for International Socio-Economic Studies