NEWSLETTER

# 顔認識に関する GDPR 及び EU AI Act 上の論点

ヨーロッパ & データ保護ニューズレター　　2025 年 8 月 22 日号

執筆者:
石川 智也
n.ishikawa@nishimura.com
服部 啓
k.hattori@nishimura.com
佐々木 将也
ma.sasaki@nishimura.com

昨今、AI の飛躍的な進歩を基礎として顔認識システムの社会実装が進んでいるが、とりわけ顔識別機能を実現するための顔画像・映像の処理は GDPR 上の所謂センシティブデータの処理を伴うものであるにも拘わらず、本来 GDPR において問題となり得る論点が十分に意識されていないことが多いように思われる。また、2025 年 2 月 2 日より順次適用が開始されている EU AI Act との関係でも、顔識別データの処理を伴う AI システムは、個人の基本権に与える影響の大きさから複層的に適用可能性及び対応事項を検討する必要がある。以上を踏まえ、本稿では、顔認識に関する GDPR や EU AI Act 上問題となり得る論点について概説する。

## 1. 顔認識(facial recognition)とは

### ① 顔認識

顔認識(facial recognition)は、一般的に、顔の画像や映像を収集して抽出した人間の顔の特徴のデジタル表現(生体テンプレート)同士を比較して個人を認証又は識別するプロセス [1]を指し、顔認識には、顔認証(facial authentication)と顔識別(facial identification)という 2 つの異なる機能があるといわれている [2]。

### ② 顔認証と顔識別

顔認証(facial authentication)とは、本人の認証を目的として、事前に登録された本人の生体テンプレートを呼び出し、それと認証を受けようとする人物の生体テンプレートとを比較して本人であるかを判断することをいう。1 対 1 の比較であるため、1 対 1 認証や 1 対 1 照合などとも呼ばれている [3]。例えば、スマートフォンの所有者がパスワードを打ち込むかわりにカメラに顔を映すことによってデバイスのロックを解除する場合や、国境通過を目的として通行者の顔を撮影しパスポートに保存された顔画像と照合することにより

---

1 EDPB "Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement ver 2.0" para 8、9 参照(当該ガイドラインについて、以下「Guidelines 05/2022」という)。個人情報保護委員会から公表されている文書においても、顔認識とは、カメラにより撮影された者の中から、その者の顔特徴データと照合用データベースに登録された顔特徴データを照合してデータベースに登録されている特定の個人を見つけ出すこと(個人情報保護委員会「犯罪予防や安全確保のための顔識別機能付きカメラシステムの利用について」6 頁)と定義されており、概ね同様の意味で理解されていると考えられる。

2 Guidelines 05/2022 para 10 参照。

3 同上。

© Nishimura & Asahi 2025

本人の認証を行う場合などがこれに当たる[4]。

これに対して、顔識別(facial identification)とは、事前に登録された複数のテンプレートの中から、認証を受けようとする人物の生体テンプレートと一致するものを探し出すことをいう。本人のテンプレートを複数のテンプレートと順次照合することにより本人を特定する 1 対多の比較であるため、1 対 N 認証とも呼ばれている[5]。例えば、写真のデータベースの中から事件の被害者や被疑者の身元を特定する場合や、空港の手荷物預かり所や搭乗ゲートなどにおいてチェックインする人物の生体テンプレートをリアルタイムで計算し、システムに事前に登録されている人物の生体テンプレートと比較する場合などがこれに当たる[6]。

顔認証と顔識別については、利便性の観点からの差異(顔認証では認証する生体テンプレートを呼び出すための認証が別途必要となるのに対し、顔識別では不要である等)が指摘されることがあるが、両者の間には、データ保護法の観点からも有意な差があり得る。例えば、本人が所有するスマートフォンなどの個人用デバイスに保存された生体テンプレートに基づく顔認証を行うにすぎない場合と、モニタリングエリアに入った人物の生体テンプレートをデータベース内の多数の生体テンプレートと無作為に比較する顔識別を行う場合とでは、本人が自らの個人データの管理をどの程度主体的ないし積極的に関与できるかが大きく異なるため、本人に対するリスクの程度に大きな差異が生じ得ると考えられる[7]。

## 2. 顔認識と GDPR

### (1) 個人データ処理の適法性根拠

GDPR 上、個人データの処理には適法性根拠を備える必要がある(GDPR6 条 1 項)が、一定の種類の個人データは、特別な種類の個人データ(special categories of personal data。いわゆるセンシティブデータ)に該当し、通常の個人データに比べて処理の要件が加重されている(GDPR9 条)。この特別な種類の個人データには、自然人を一意に識別することを目的とする生体データ(biometric data for the purpose of uniquely identifying a natural person。GDPR9 条 1 項)も含まれる。顔写真や顔の映像が直ちに GDPR9 条が適用されるセンシティブデータとしての生体データに該当するわけではないものの[8]、顔認証と顔識別については、いずれも、個人を識別された又は識別可能とする技術的な処理を伴うものとして、特別な種類の個人データの処理に該当すると考えられる[9]。したがって、GDPR の適用のある個人データについて顔認識を行う際には、データ主体の明確な同意を取得することが必要になると考えられる(GDPR9 条 1 項)。なお、生体データの処理につきデータ主体の明示的な同意を取得することができたとしても、なお必要性や相当性に関する GDPR の処理原則に適合しているかについての検討が要求されている点には注意が必要である[10]。

さらに、特別な種類の個人データの処理に当たっては、プライバシー・バイ・デザイン/デフォルト

---

4 Guidelines 05/2022 para 19、21 参照。

5 EDPB "Opinion 11/2024 on the use of facial recognition to streamline airport passengers' flow (compatibility with Articles 5(1)(e) and(f), 25 and 32 GDPR) ver 1.1" para 22 参照。当該 Opinion について、以下「Opinion 11/2024」という。

6 Guidelines 05/2022 para 22 参照。

7 Guidelines 05/2022 para 17 参照。

8 GDPR 前文(51)参照。

9 Guidelines 05/2022 para 12、Opinion 11/2024 para 22 参照。

10 Opinion 11/2024 para 31、32 参照。

© Nishimura & Asahi 2025

(GDPR25 条 1 項)についてもより慎重な対応が求められる。例えば、ガイドライン上、GDPR9 条により同意取得が要求される場合、管理者は、原則として、生体データの処理を受け入れることをサービスへのアクセスの条件とすることは禁じられ、本人に対して制約や追加費用を課すことなく、生体データの処理を伴わない代替的なソリューションを提供する必要があるとされている [11]。また、管理者は、データ最小化原則に従い、生体テンプレートを作成するために抽出されるデータに不要な情報が含まれていないことを保証する必要があり [12]、さらに、生体テンプレートへの不正アクセス防止のため、暗号化を含む保護措置を実施する必要があるとされている [13]。

なお、EDPB が、2024 年 5 月、空港で旅客の流れを合理化するための顔認識機能の利用に関するオピニオンを公表している。下記の 4 つのシナリオについて、記録保存の期間制限(GDPR5 条 1 項(e))、完全性及び機密性(GDPR5 条 1 項(f))、プライバシー・バイ・デザイン/デフォルト(GDPR25 条)、安全管理措置(GDPR32 条)の適合性を論じたものとして参考になる。

- シナリオ①：チェックポイントを通過する際に旅客を認証(1 対 1 認証)するために登録された生体テンプレートを、旅客の手元のデバイス等に保存する手法→同一の目的を同程度の効率性をもって達成できるより侵襲性の低い代替策がないことを示すことができれば、適合
- シナリオ②：空港内で、登録された生体テンプレートを、暗号化された状態で、秘密鍵とともに、乗客の手元のみに集中保管する手法→適合
- シナリオ③：登録された生体テンプレートを、空港運営者の管理の下、暗号化された形式で空港内に集中保管する手法→不適合
- シナリオ④：登録された生体テンプレートを暗号化された形でクラウドに集中保管する手法→不適合

### (2) データ保護影響評価

GDPR 上、管理者は、自らが行おうとしている個人データの処理が個人の権利及び自由に高いリスクをもたらす蓋然性がある場合、事前に、当該処理についてデータ保護影響評価(Data Protection Impact Assessment)と呼ばれるリスク評価を実施しなければならない(GDPR35 条)。

そこで、どのような場合に「高いリスクをもたらす蓋然性がある」かが問題となるが、GDPR 上、いわゆるセンシティブデータの大規模な処理を行う場合にはデータ保護影響評価が必要であると明記されていること(GDPR35 条 3 項(b))、及び、現行のガイドライン [14]等の記載を参照する限り、顔認識を含む個人データの処理については、データ保護影響評価の実施が求められる場面が多いと考えられる [15]。

---

11 EDPB "Guidelines 3/2019 on processing of personal data through video devices version 2.0" para 77 参照。当該ガイドラインについて、以下「Guidelines 3/2019」という。

12 Guidelines 3/2019 para 87 参照。

13 Guidelines 3/2019 para 88 参照。

14 Article 29 Data Protection Working Party "Guidelines on Data Protection Impact Assessment (DPIA) (wp248rev.01)"

15 Guidelines 3/2019 para 137、Guidelines 05/2022 para 97、Opinion 11/2024 para 47 参照。なお、GDPR35 条 4 項に基づき、EU 各加盟国の当局は、データ保護影響評価が必要となる処理のリストを公表しているため、実際の事業展開に当たっては、関連する法域の当局の公表情報にも注意する必要がある。

© Nishimura & Asahi 2025

## 3. 顔認識と EU AI Act

EU AI Act(以下「AIA」という)上、顔認識という概念自体は定義されていないものの、顔認識に関連する概念として、生体認証(biometric verification)と生体識別(biometric identification)がある(AIA3 条 36 号、35 号)。生体認証と生体識別との区別は、それぞれ、顔認識における顔認証と顔識別の区別に概ね対応しており、前者が特定の自然人の生体データと事前に提供された生体データとを 1 対 1 で比較し自動的に認証するものであるのに対し、後者は、個人の生体データをデータベース内の生体データと 1 対多で比較することにより、自然人を自動的に認識するものである。

また、生体識別については、本人の積極的な関与なしに識別を行うことを企図した AI システムとして遠隔生体識別システム(remote biometric identification system)が定義されている(AIA3 条 41 号)。さらに、遠隔生体識別システムのうち、生体データの取得、比較及び識別が大幅なタイムラグなく行われるものがリアルタイム遠隔生体識別システム(real-time remote biometric identification system)、それ以外がポスト遠隔生体識別システム(post remote biometric identification system)と定義されており(AIA3 条 42 号、43 号)、下記のとおり、両者は異なる規律に服することがあるため、注意が必要である。

### (1) 禁止された AI プラクティスに該当する場合

AIA 上、EU 域内における禁止された AI プラクティスは一切禁止されており、具体的には、以下の行為がこれに該当する(AIA5 条)。

| | 禁止された AI プラクティスの類型 |
|---|---|
| (a) | ・ 人の意識を超えた**サブリミナル技術又は意図的に操作的・欺瞞的な技術を用いる AI システムの上市、運用開始又は使用**であって、**十分な情報に基づいた意思決定能力を著しく損なう**ことによって、個人又は集団の行動を実質的に歪め、それにより、当該個人、他者又は集団に重大な損害を与える又は与える可能性が高い方法で、個人又は集団がそうでなければ**行わなかったであろう決定を行わせる目的又は効果**のあるもの |
| (b) | ・ **年齢、障害又は特定の社会的・経済的状況**に起因する**自然人又は特定の集団の脆弱性を悪用**する AI システムの**上市、運用開始又は使用**であって、個人又は集団に属する**人の行動を**、当該個人又は他者に重大な損害を与える又は与える可能性が高い方法で、**実質的に歪める目的又は効果**のあるもの |
| (c) | ・ 社会的行動や既知、推論又は予測される**個人的・人格的特徴に基づき**、一定期間にわたって**自然人又は集団の評価又は分類を行う**ための AI システムの**上市、運用開始又は使用**であって、特定の自然人又は集団に対して、**ソーシャルスコア**が以下の**いずれかの不利益取扱い**をもたらすもの<br>(i) データが当初生成又は収集された文脈と**無関係な社会的文脈での不利益取扱い**<br>(ii) その**社会的行動又は重大性に対して不当又は不均衡な不利益取扱い** |
| (d) | ・ 自然人が**犯罪を犯すリスクを評価又は予測するために**、自然人の**プロファイリング又は人格的特徴・特性の評価のみに基づき**、**自然人のリスク評価**を行う AI システムの**上市**、この特定の目的のための**運用開始又は使用**<br>・ この禁止は、犯罪活動に直接関連する客観的かつ検証可能な事実に既に基づいている、犯罪活動への人の関与に関する人の評価を支援するために使用される AI システムには適用されない |

© Nishimura & Asahi 2025

| | |
|---|---|
| (e) | ・ **インターネット又は CCTV 映像**から**無作為にスクレイピングした顔画像**を用いて、**顔認識データベース**を作成、又は拡張する AI システムの**上市**、この特定の目的のための**運用開始又は使用** |
| (f) | ・ **職場・教育機関**において**自然人の感情を推測するため**の AI システムの**上市**、この特定の目的のための**運用開始又は使用**<br>・ 但し、医療上又は安全上の理由によるものを除く |
| (g) | ・ **人種、政治的意見、労働組合への加入状況、宗教的・哲学的信条、性生活・性的指向を推測又は推論するため**に、**生体データに基づいて**個々の**自然人を分類する生体分類システム**の**上市**、この特定の目的のための**運用開始又は使用**<br>・ この禁止は、合法的に取得された画像等の生体データセットの生体データに基づくラベリング若しくはフィルタリング、又は法執行分野における生体データの分類には適用されない |
| (h) | ・ **法執行の目的で**、**公共のアクセス可能な空間**において、**リアルタイム遠隔生体識別システムを使用**すること<br>・ 但し、以下のいずれかの目的のために厳密に必要である場合は除く<br>(i) 拉致、人身売買又は性的搾取の被害者の捜索及び行方不明者の捜索<br>(ii) 自然人の生命若しくは身体の安全に対する具体的、実質的かつ差し迫った脅威、又は真正かつ現存する若しくは予見可能なテロ攻撃の脅威の防止<br>(iii) Annex II に定める犯罪であって、当該加盟国において拘禁刑又は拘禁命令により最長で少なくとも 4 年以上の処罰が可能な犯罪について、犯罪捜査、訴追又は刑事罰の執行を行う目的で、犯罪を犯したと疑われる者の所在地を特定し、又は身元を識別すること |

以上の禁止された AI プラクティスのうち、顔認識に直接関連し得るものとしては、以下が挙げられる。

① インターネット上又は CCTV 映像から無作為に顔画像を収集して顔認識データベースを作成又は拡張する AI システムの上市、この特定の目的のための運用開始又は使用(AIA5 条 1 項(e))
② 職場又は教育機関において自然人の感情を推測するための AI システムの上市、この特定の目的のための運用開始又は使用(AIA5 条 1 項(f))
③ 人種、政治的意見、労働組合への加入状況、宗教的・哲学的信条、性生活・性的指向を推測又は推論するために、生体データに基づいて個々の自然人を分類する生体分類システムの上市、この特定の目的のための運用開始又は使用(AIA5 条 1 項(g))
④ 一般にアクセス可能な空間におけるリアルタイム遠隔生体識別システムの法執行目的での使用(AIA5 条 1 項(h))

例えば、上記①との関係では、道路や空港等の公共空間で動作する監視カメラから特定の個人や属性の集団にターゲットを絞ることなく顔画像を収集するような場合も適用スコープとして想定されており [16]、これらの方法で収集した顔画像をもとに顔認識データベースを作成することができる AI システムを、EU 域内で上市したり使用したりすれば、AIA5 条 1 項(e)に抵触する。また、上記②との関係では、職場における AI の

[16] European Commission ANNEX to the Communication to the Commission Approval of the content of the draft Communication from the Commission - Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act) (以下「Commission Guidelines on prohibited artificial intelligence」という) para 228、232 参照。

© Nishimura & Asahi 2025

利活用が日々推進されているが、顔画像から従業員等[17]の感情を推測する AI システムの上市や使用等は EU 域内において禁止されている(AIA5 条 1 項(f))点にも特に留意が必要であるように思われる。例えば、コールセンターでウェブカメラを使用して従業員の感情をトラッキングしたり、スーパーマーケットでカメラを使用してスタッフの感情を推測したりするような行為は禁止される AI プラクティスに該当すると考えられており[18]、顔画像から感情を推測する機能を有する AI システムを提供又は実装するに当たっては、EU 域内で禁止された AI プラクティスを実施することにならないか、特に慎重に検討を進める必要があると考えられる。

### (2) ハイリスク AI システムに該当する場合

禁止された AI プラクティスに該当しないとしても、人の生体データと参照されるデータベース内にある生体データを遠隔で比較することにより、本人の関与なく、自然人を識別するための AI システムである遠隔生体識別システムは、原則として[19]ハイリスク AI に該当する(AIA6 条 2 項、Annex III 1.(a))。そのため、顔画像を機械的に処理して作成した顔認識データベースを利用して識別を行う機能を有する AI システムを実装するサービスは、ハイリスク AI システムに該当しないか慎重に検討する必要がある。

また、感情認識のために使用されることを目的とする AI システムや、機微又は保護された特性の推論に基づいて生体分類のために使用されることを目的とする AI システムは、ハイリスク AI システムに該当する(AIA6 条 2 項、Annex III 1.(b)(c))。そのため、顔認識機能により収集した顔画像を分析して感情を識別・推論したり、性別等の一定のカテゴリーに分類したりする AI システムは、ハイリスク AI システムに該当しないか慎重に精査する必要があると考えられる。

なお、感情認識や生体分類を目的とする AI システムの Deployer は、原則として、それに晒された個人に対して AI システムが稼働していることを通知する透明性義務を負う点にも留意する必要がある(AIA50 条 3 項)。ハイリスク AI システムに関する義務と透明性義務は二者択一ではなく、両者が同時に適用されることがある。

### (3) ハイリスク AI システムの Provider、Deployer として講ずべき措置

AIA 上、Provider は AI システムを開発し又は開発させ、自己の名義若しくは商標の下で EU に上市若しくはサービス供給する者と定義され(AIA3 条 3 号)、他方で、Deployer は権限に基づいて AI システムを使用する者を意味する(AIA3 条 4 号)。具体的には、AI システムを開発するベンダー等が Provider となり、その AI システムを事業に用いる事業者が Deployer となるため、多くの事業者は Deployer の立場で AIA に関わることになる。ハイリスク AI システムの Provider 及び Deployer の主な対応事項は下記のとおりである。

---

17 従業員、契約社員、トレイニー、ボランティア等の法的地位を問わず、採用候補者も含む(Commission Guidelines on prohibited artificial intelligence para 254)。

18 Commission Guidelines on prohibited artificial intelligence para 254 参照。

19 なお、本人確認のみを目的とする、生体認証(1 対 1 認証)に使用される AI システムは、ハイリスク AI システムに該当しない(AIA6 条 2 項、Annex III 1.(a))。

© Nishimura & Asahi 2025

① Provider

| 類型 | 項目 |
|---|---|
| システム要件 | リスクマネジメントシステムの実施 |
| | データガバナンス |
| | 技術文書の作成 |
| | ログの自動記録 |
| | 透明性の確保(Deployer への情報提供) |
| | 人間による監視 |
| | 正確性、堅牢性、サイバーセキュリティ |
| 市販後モニタリング | 市販後のシステム要件遵守に係る継続的なモニタリングの実施 |
| 品質管理 | 品質マネジメントシステム(ポリシー、手順書及び指示書の形で文書化) |
| 文書・記録保管 | 技術文書・品質マネジメントシステムに係る文書等、自動生成ログの保管 |
| | 監督当局の求めに応じたシステム要件適合性の証明文書、自動生成ログの提出 |
| 不適合時の対応 | 是正措置(リコール、廃棄等)・Deployer への通知 |
| 製品表示 | AI システム又はパッケージ/附属文書上に名称、商標、連絡先住所の記載 |
| 製品安全性 | 域外に拠点を有する Provider の認定代理人の指名 |
| | 適合性評価・適合性宣言書の作成 |
| | CE マークの貼付 |
| | AI データベースへの登録 |
| | アクセシビリティ法令への準拠の確認 |

② Deployer

| 類型 | 項目 |
|---|---|
| システム要件関連 | 使用説明書に従った技術的組織的措置 |
| | 自然人によるモニタリング |
| | 入力データが適切であることの保証 |
| | 自動的に生成されたログの保管 |
| | 使用説明書に基づく運用のモニタリング |
| 是正措置・情報提供 | 不適合発生時における当局・関係者への通知・使用停止 |
| 透明性の確保 | (職場で導入する場合)労働者代表者・影響を受ける労働者への事前通知 |
| | AI システムの使用の対象になる旨の自然人への事前通知 |
| 自然人のリスクの影響評価 | データ保護影響評価における Provider から提供を受けた情報の考慮 |
| | 基本権影響評価 |

## 4. 日本法・日本企業の実務への影響

日本では、AI を活用した顔認識技術の社会実装が進んでおり、個人情報保護法やプライバシー侵害との関

© Nishimura & Asahi 2025

係での論点整理も進められている(「個人情報保護法についてのガイドライン」に関する Q&A[20](個人情報保護委員会)、カメラ画像利活用ガイドブック(IoT 推進コンソーシアム・総務省・経済産業省)等)が、EU においては、現状の日本法上の整理とは大きく異なる点として [21]、顔画像を技術的に処理して得られた識別性を有する顔特徴データは、生体データとして、いわゆるセンシティブデータに該当し、原則として、データ主体の明示の同意なく処理することができない点が挙げられる。また、かかる論点への対応のみならず、顔認識による生体データの処理が個人の権利利益に与える影響に照らして、基本原則を遵守できるようなシステムアーキテクチャの構築及び体制整備、これらを踏まえたデータ保護影響評価の実施に至るまで、一貫したデータ保護に関するコンプライアンスを実装することが重要であることも付言する。

そして、生体データが AI の出力の基礎とされることで自然人の権利利益への影響が大きくなりやすいことから、AIA においても、顔認識機能を実装する AI システムは、禁止された AI プラクティスやハイリスク AI システムに該当する例が少なくない。そのため、EU 域内で顔認識機能を有する AI システムを提供する場合は、どのカテゴリーのリスクレベルに分類されるかについてのアセスメントが必須である。

また、GDPR、AIA ともに、EU 域外の事業者に対して域外適用されるが、AIA に関しては、その適用範囲が GDPR よりも広く解される可能性も相応にある(AIA2 条 1 項(c))[22]。そのため、顔認識機能を有する AI システムを EU 域内に向けて提供していない(そのため、GDPR 及び AIA の適用は受けない)という整理を行う場合には、域外適用のリスクを十分に低減できるよう慎重に検討を行う必要がある。

当事務所では、クライアントの皆様のビジネスニーズに即応すべく、弁護士等が各分野で時宜にかなったトピックを解説したニューズレターを執筆し、随時発行しております。N&A ニューズレター購読をご希望の方は N&A ニューズレター　配信申込・変更フォームよりお手続きをお願いいたします。
また、バックナンバーはこちらに掲載しておりますので、あわせてご覧ください。

本ニューズレターはリーガルアドバイスを目的とするものではなく、個別の案件については当該案件の個別の状況に応じ、日本法または現地法弁護士の適切なアドバイスを求めていただく必要があります。また、本稿に記載の見解は執筆担当者の個人的見解であり、当事務所または当事務所のクライアントの見解ではありません。

西村あさひ 広報課 newsletter@nishimura.com

20 カメラ画像の取扱いに関する見解は、カメラに関する Q&A に抜粋されている。

21 日本でも、現在検討が進められている個人情報保護法の 3 年毎見直しにおいて、生体データは通常の個人情報と比較して個人の権利利益に与える影響が大きく、保護の必要性が高いと考えられることを踏まえ、生体データの利用について、本人がより直接的に関与できる必要がある等の考え方が呈示されており(個人情報保護委員会「個人情報保護法いわゆる 3 年ごと見直しに係る検討の中間整理」)、改正の動向が注目される。

22 さらに、AIA は、医療機器、無線機器といった製品の安全性に関する法令の AI 版であるところ、実際、AIA の適用範囲を画する重要な要素となる AI システム及び汎用目的 AI モデルの「上市」(AIA2 条 1 項(a))の概念に関して、汎用目的 AI モデルの義務の範囲に関するガイドラインにおいて、製品安全性に係る法令の実装方法を解説した Blue Guide における「上市」の説明を参照すべきとされていることも注目に値する(European Commission, Guidelines on the scope of the obligations for general-purpose AI Models established by Regulation (EU) 2024/1689 (AI Act) para 54 参照)。

© Nishimura & Asahi 2025