EUの「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案」の概要

2022年7月

国際社会経済研究所　小泉 雄介

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案

- EDPB（欧州データ保護会議）は2022年5月12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Ver1.0（パブコメ版）」を採択した。6月27日までパブリックコンサルテーションに付された。
  - “Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement Version 1.0”
  - https://edpb.europa.eu/system/files/2022-05/edpb-guidelines_202205_frtlawenforcement_en_1.pdf
- 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。

法執行顔認識ガイドライン案の目次

顔認識の用途の分類（2.1節、2.2節）

- 同ガイドライン案では、顔認識（Facial Recognition）の用途は以下2つに分類されている。

（１）認証（Authentication）

- ある個人が、当人が主張する人間であることを確認することを目的とする。
- 事前に記録された顔画像またはテンプレート（顔特徴量データ）を、ゲートなどで撮影された個人の顔のテンプレートと比較し、同一人物であるかどうかを確認する。1対1検証（verification）とも呼ばれる。

（２）識別（Identification）

- 特定のエリアで撮影された映像等の中から、特定個人を見つけることを目的とする。
- 撮影された各人物の顔に対してテンプレート（顔特徴量データ）を生成し、それが既存のデータベース上で既知の人物と一致するかどうかを確認する。1対多の識別とも呼ばれる。

※さらに（a）「リアルタイム（ライブ）」識別と（b）「事後」識別の概念も出てくる。

- （１）顔認証の例（※法執行分野に限らない）
  - スマートフォンのログイン認証
  - 建物への入退館管理
  - デジタルID作成時の身元確認
  - 出入国ゲートでの顔認証
- （２）顔識別の例（※法執行分野に限らない）
  - 容疑者や被害者の画像とデータベースとの顔照合
  - 公共空間でのリアルタイムのリモート生体識別
  - 銀行ATMでの顧客識別
  - 公共空間における個人の移動経路の追跡
  - SNSでの友人写真のタグ付け
  - 空港での旅客の追跡

適用される法的枠組み（3節）

- 法執行分野での顔認識技術（FRT）の使用には、以下の法的枠組みが適用される。
  - EU基本権憲章
  - 法執行指令（LED）
  - 加盟国法（国内法）

- EU基本権憲章（3.1節）
  - FRTの使用は、EU基本権憲章の特に第7条（私的生活および家族生活の尊重）と第8条（個人データの保護）に影響を与える可能性。
  - また、第1条（人間の尊厳）、第10条（思想、良心および信教の自由）、第11条（表現および情報の自由）、第12条（集会および結社の自由）にも影響を与える可能性。
  - あらゆる状況において、生体データの処理は、それ自体が基本的権利への深刻な干渉となる。
  - 同憲章第52条1項に従い、基本的権利および自由の行使に対するいかなる制限（干渉）も、「法律によって規定」され、それらの「権利および自由の本質を尊重」しなければならない。
  - また同項に従い、「比例性の原則」に服しつつ、制限は、それらが「必要」であり、かつEUによって認識されている「一般的利益の目的または他者の権利と自由を保護」する必要性に真に合致する場合にのみ、行うことができる。

適用される法的枠組み（3節）

- **法執行指令（LED）：生体データの定義、個人データ処理の適法性（3.2節）**
  - **LED第3条13項で「生体データ」を定義。（GDPRと同じ定義）**

※ LED第3条（定義）13項

「生体データ」とは、自然人の身体的、生理的又は行動的な特性に関連する特別な技術的取扱いから得られる個人データであって、顔画像や指紋データのように、当該自然人を一意に識別できるようにするもの、又は、その識別を確認するものを意味する。

  - **LED第8条は、法執行機関による（一般的な）個人データ処理が適法であるためには、（LED第1条1項に記載された）「法執行目的に必要」であることに加えて、（EU法または）「処理の目標、処理される個人データ、処理の目的を指定する国内法で規制」されなければならないことを明確化。**

※ LED第8条（処理の適法性）

1. 加盟国は、第1条1項に定められた目的のために所管官庁によって行われる職務の遂行に処理が必要であり、EU法または加盟国法に基づく場合にのみ、処理が適法であると定めるものとする。

2. 本指令の範囲内の処理を規制する加盟国法は、少なくとも処理の目標、処理される個人データ、および処理の目的を指定するものとする。

※ LED第1条（対象事項及び目的）1項

本指令は、公共の安全への脅威からの保護およびその防止を含め、所管官庁によって犯罪行為の防止、捜査、検知若しくは訴追又は刑罰の執行の目的で行われる個人データの処理と関連する自然人の保護に関するルール及び個人データの自由な移動に関するルールを定める。

適用される法的枠組み（3節）

- **法執行指令（LED）：生体データ処理が許可されるケース（3.2.1節）**
  - **LED第10条に従い、生体データなどの特別なカテゴリのデータの処理は、「厳密に必要」な場合にのみ許可され、「データ主体の権利と自由に対する適切な保護措置」が適用されなければならない。**
  - **それに加えて、「EU法または加盟国法によって承認されている」場合、「データ主体や他の自然人の生命に関する利益を保護する」場合、または当該処理が「データ主体によって明白に公開のものとされたデータ」に関する場合にのみ許可されなければならない。**

※　LED第10条（特別なカテゴリーの個人データの処理）

人種的若しくは民族的な出自、政治的な意見、宗教上若しくは思想上の信条、又は、労働組合への加入を明らかにする個人データの処理、並びに、遺伝子データ、自然人を一意に識別することを目的とする生体データ、健康に関するデータ、又は、自然人の性生活若しくは性的指向に関するデータの処理は、データ主体の権利と自由に対する適切な保護措置を条件として、厳密に必要な場合、かつ以下の場合にのみ許可されるものとする。

（a）EU法または加盟国法によって承認されている場合。

（b）データ主体または他の自然人の生命に関する利益を保護するため。または、

（c）当該処理が、データ主体によって明白に公開のものとされたデータに関する場合。

- **写真がデータ主体によって明白に公開されているという事実は、特定の技術的手段によってその写真から加工できる生体データまでが明白に公開されていると見なされることを意味するものではない。生体データがデータ主体によって明白に公開されていると見なされるためには、データ主体は、生体テンプレート（顔特徴量データ）をオープンソースを通じて自由にアクセス可能で公開していなければならない。第三者が生体データを開示した場合、当該データがデータ主体によって明白に公開されているとは見なされない。（→Clearview AI社の運用はNG）**

適用される法的枠組み（3節）

- 法執行指令（LED）：データ主体の権利（3.2.4節）
  - 法執行機関が顔認識技術（FRT）を使用する場合には、簡潔で、わかりやすく、簡単にアクセスできる形式でデータ主体に権利と情報を知らせなければならない。
  - 捜査や処理の目的に関係のないビデオ映像は、生体データの処理を実施する前に、常に削除または匿名化（例えば元データに回復できない非可逆的な不鮮明化）をするべきである。それは、LED第4条1項（e）の最小化原則およびLED第13条2項の情報提供の義務を履行できないリスクを回避するためである。
  - データ主体が自分の権利を行使する上でどのような情報が重要であるかを評価し、必要な情報が提供されていることを保証するのは、管理者の責任である。データ主体の権利の効果的な行使は、管理者が情報提供の義務を果たすことに依存している。
  - LED第13条1項と2項に従い、FRTを使用する場合は、以下の情報をデータ主体に提供する必要がある。この情報は、管理者のWebサイトや、印刷された形式（リーフレット等）、データ主体が容易にアクセスできるその他のソースで提供される。
    - データ保護オフィサーを含む、管理者のアイデンティティと連絡先の詳細。
    - 処理の目的と、FRTを介して処理していること。
    - 監督機関に苦情を申し立てる権利および監督機関の連絡先の詳細。
    - 個人データへのアクセス、修正または消去、および個人データの処理の制限を要求する権利。
    - 処理の法的根拠。
    - データ主体の知らないうちに個人データが収集される場合に関する情報。
    - 個人データが保存される期間、またはそれが不可能な場合は、その期間を決定するために使用される基準。
    - 該当する場合、個人データの受領者のカテゴリ（第三国または国際機関を含む）。

ユースケース（AnnexⅢ 実践的事例集）

シナリオ１．出入国ゲートでの顔認証　○

- 国境通過点を通過するEU市民等のパスポート等に保存されているバイオメトリック画像を認証し、当人がパスポート等の正当な所有者であることを証明することにより、自動国境通過を可能にする出入国管理システム。
- 適用される法的枠組み
  - 規則（EC）2252/2004：加盟国が発行するパスポートその他の渡航文書には、当該文書に埋め込まれた電子チップに保存されたバイオメトリック顔画像が含まれなければならないと規定。
  - 規則（EU）2017/2225：「eゲート」、「自動出入国管理システム」、「セルフサービスシステム」の定義と、国境チェックを実行するための生体データの処理の可能性が導入された。
- 必要性と比例性
  - バイオメトリック画像を使用した自動出入国管理におけるEU市民のアイデンティティ検証は、EU国境警備に直接関係しており、EUによって認識された一般的利益の目的に役立つ。また自動ゲートは、旅客処理を高速化し、人為的ミスのリスクを軽減するのに役立つ。
  - さらに、本シナリオでの干渉の範囲や強度は、他の形式の顔認識と比較してはるかに限定的である。
- 結論
  - 自動国境管理の文脈でのEU市民のアイデンティティ検証は、適切な保護措置が講じられている限り、特に目的制限・データ品質・透明性・高いセキュリティレベルの原則が適用されている限り、必要かつ比例的な措置である。

ユースケース（AnnexⅢ 実践的事例集）

シナリオ２．児童誘拐の被害者の顔識別　○

- 権限を与えられた警察官が、誘拐された可能性のある児童の生体データを、児童誘拐被害者データベースと照合する。この顔照合は、厳格な条件下で、捜査が開始されアラートが発出された行方不明児童の特徴に一致する可能性のある個人を識別するという目的のみで、実施可能。
- 適用される法的枠組み
  - 本シナリオでは、当該国の国内法において、児童誘拐被害者データベースを構築し、処理の目的と、データベースに入力・アクセス・使用するためのクライテリアを定めた、専用の法的枠組みが規定されている。
  - その国内法はまた、保持期間、完全性と機密性の原則、データ主体や保護者への情報提供の方法、データ主体の権利の行使の方法、権利行使の制限の可能性等を規定。また法案作成前に、当該国のDPAに事前相談。
- 必要性と比例性
  - 本シナリオでは、児童の顔照合は、より侵入的でない手段が他になく、厳密に必要な場合に限り、例えば旅行中の児童の身分証明書の真正性に疑問がある場合や犯罪捜査が行われている行方不明児童の特徴との一致の可能性を示す証拠を確認した後に限り、最後の手段として、権限のある警察官のみが実行できる。
  - また児童誘拐被害者データベースの構築は、一般的な公益の重要な目的および他者の権利と自由の保護に役立つ。
- 結論
  - 本シナリオの処理の必要性と比例性、そのような個人データ処理を実行する上での児童の最善の利益を考慮し、データ主体の権利の行使を特に保証にするために十分な保障が実施されているならば、このようなアプリケーションはEU法とコンパチブルである可能性が高いと見なされるかもしれない。

ユースケース（AnnexⅢ 実践的事例集）

シナリオ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、暴動を行った人を識別するシステム×

- デモ行為の最中に暴動が起こり、警察はCCTV映像や目撃者を用いた捜査により複数の容疑者を特定する。警察は続いて、暴動現場や周辺エリアでCCTVや個人スマホに録画された映像をデータベース化し、容疑者の写真と照合する。
- 適用される法的枠組み
  - 本シナリオでは、当該国の国内法は、LED第10条の一般条項（厳密に必要であり、当人の権利と自由のための適切な保護措置がある場合に許可）を規定しているのみ。このような単にLED条項をコピペしただけの法的根拠は、法執行機関が公共空間のCCTV映像を使用して生体データを作成したり、それを警察データベースや他のCCTV・プライベート録画などと比較する権限を与えられる条件や状況を個人に十分に説明するという観点からは、十分に明確でない。
- 必要性と比例性
  - 本シナリオでは、重大犯罪の疑いがない人々の映像や、暴動と地理的・時間的に離れた人々の映像もデータベース化され、容疑者写真との顔照合にかけられる。このように警察が作成するデータベースは比例性の要件を満たす映像に限定されないため、顔照合される映像の数が無制限なものとなる。これは、データ最小化の原則と矛盾する。
  - また、デモ行為の周辺エリアで収集された映像はデモ参加者の「政治的意見」を明らかにしている可能性が高い。さらに、デモへの参加によって警察データベースに登録されたことを個人が知った場合、集会の権利の行使に深刻な萎縮効果をもたらす恐れがある。
- 結論
  - 本シナリオは法的根拠となりうる個別の規定が存在しない。仮に、十分な法的根拠となる個別の規定があったとしても、必要性と比例性の要件が満たされないため、EU基本権憲章の下でのデータ主体の私的生活の尊重と個人データの保護に対する比例的でない干渉が発生してしまう。

ユースケース（AnnexⅢ 実践的事例集）

シナリオ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 ○

- 警察官が犯行現場等の場所から収集されたビデオ映像から容疑者の画像を手動で選択し、その画像をフォレンジック部門に送信する。フォレンジック部門はこれらの画像を、これまで警察によってデータベース（容疑者や元受刑者で構成されるデータベース）に収集された個人の写真と顔照合する。
- 適用される法的枠組み
  - 本シナリオでは、当該国の国内法において、重大犯罪を犯した容疑者を識別する目的を達成するために厳密に必要な場合に、データベースでの画像照合を通じて、フォレンジック分析を行う際に生体データを利用することできると規定されている。
  - 国内法は、処理される可能性のあるデータ、個人データの完全性と機密性を維持するための手続き、その廃棄の手続きを規定しているため、悪用のリスクに対して十分な保障を提供している。
- 必要性と比例性
  - 本シナリオで顔認識技術（FRT）を使用することは、目視での照合よりも明らかに時間効率が高くなる。事前に容疑者の画像を手動で選択することで、現場の全てのビデオ映像をデータベースに対して照合する場合と比較して干渉を少なくし、それによって、重大犯罪と闘うという目的の対象となる人物のみを区別してターゲット化することとなる。
  - FRTや個人データへのアクセス権を持つ職員を制限することは、プライバシーとデータ保護の権利への影響を軽減し、不要となった顔特徴量データは廃棄される。照合結果を目視で確認することで、偽陽性のリスクを減らしている。
- 結論
  - 本シナリオでは、FRTの使用条件、生体データにアクセスできる人の数、目視での確認など、データ保護の権利への干渉を制限するための措置が国内法で規定され、講じられている。FRTは警察のフォレンジック部門の捜査業務効率を大幅に向上させるものであり、厳密に必要な場合に限って処理を許可する法律に基づいているため、個人の権利の適法的な干渉と見なされるかもしれない。

ユースケース（AnnexⅢ 実践的事例集）

シナリオ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） ×

- リモート生体識別とは、公共空間において、離れた所から、連続的もしくは継続的に、生体識別子（顔画像、歩容、虹彩など）をデータベースに保存されたデータと照合することにより、個人のアイデンティティを確立することである。警察は捜査の一環として、事前に関心ある対象者のウォッチリストを作成する。対象者がショッピングモールや広場といった特定エリアにいることを示唆するインテリジェンスに基づいて、警察はリモート生体識別をいつ、どこで、どのくらいの期間、展開するかを決定する。照合結果がポジティブであった場合、現地の警察官が、その個人に介入するか、接近するか、最終的に逮捕するかを決定する。
- 必要性と比例性
  - 本シナリオでは、当該エリアのすべての通行人をモニタリングするため、公共空間で匿名であるという住民の合理的な期待に深刻な影響を及ぼす。公共空間での匿名性は、市民団体への参加、集会への訪問、あらゆる社会的・文化的背景を持つ人々との出会い、政治的プロテストへの参加、様々な場所への訪問など、民主的プロセスの多くの側面の前提条件である。公共空間における匿名性の感覚を損なうことは、市民の行動に深刻な萎縮効果をもたらす恐れがある。
  - 特定エリアを歩いただけで、法執行機関による生体データの収集につながり、警察データベースとも照合されてしまう。これは全通行人が強制的に指紋を採取されることに等しく、このようなデータ処理は明らかに目的に照らして比例的ではない。
  - 各エリアを通り過ぎるすべての人が影響を受けるため、影響を受けるデータ主体の数は非常に多い（ターゲット化されていない）。さらに本シナリオは生体データの大量自動処理に当たり、警察データベースに対する生体データの大量照合にも当たる。
  - 警察によるリモート生体識別は、すべての通行人を潜在的な容疑者として扱う。しかし、法の支配に基づく国では、違法行為が証明されるまで、市民は正しい人間であると推定される。LED第6条に従うと、法執行機関が或る個人を容疑者として扱う場合、当人に対して「犯罪を犯した、または犯そうとしていると信じる重大な理由」を持たなければならない。
- 結論
  - 競合する私的利益と公共の利益のバランスをとることができず、EU基本権憲章第7条・8条の権利への比例的でない干渉である。

ユースケース（AnnexⅢ 実践的事例集）

シナリオ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×

- ある民間企業は、顔画像をインターネットからスクラップしてデータベースを作成し、顔識別サービスを提供している。当該サービスはユーザー（警察等）からアップロードされた写真をデータベース内の顔画像や顔特徴量データと照合する。警察は、既存の警察データベースに登録されておらず、内部情報では識別できないような容疑者のビデオ映像について、顔識別を行うために当該サービスを使用することを決定する。

- 適用される法的枠組み
  - この民間企業は、データベースを作成するためにインターネットから画像をスクラップする等の個人データ処理について、法的根拠（適法性の根拠）を持っていなければならない。（生体データへの加工についても）
  - また、当該サービスを使用する法執行機関も、個人データ処理の法的根拠を持っていなければならない。法執行機関が生体データを処理できるようにするには、その目標、処理する個人データ、処理の目的、個人データの完全性と機密性を維持するための手続き、その廃棄のための手続きを規定する法的枠組みが必要である。
  - 当該サービスのデータベースが配置されている場所によっては、個人データや特別なカテゴリの個人データのEU域外への越境移転を伴う場合がある。この場合、LED第39条（第三国に拠点を持つ受領者への個人データ移転）が適用される。

ユースケース（AnnexⅢ 実践的事例集）

シナリオ６．（続き）

- 必要性と比例性
  - 法執行機関による当該サービスの使用は、個人データを無制限に大規模な方法で収集してデータベース化する民間企業と個人データが共有されることを意味する。また、民間企業が収集した個人データと、法執行機関が追求する目的との間には何のつながりもない。
  - 法執行機関による民間企業へのデータの共有は、民間企業によって処理されるデータに対する法執行機関のコントロールの欠如と、（データ主体が自分のデータがこのように処理されていることに気づいていないため）データ主体による権利行使が非常に困難になることを意味する。
  - 生体データの処理は厳密に必要な場合にのみ許可されるが、本シナリオがLEDに定められた要件を満たすかどうかは疑わしい。重大犯罪と闘う上での有効性という一般的な利益は、それ自体では、膨大な量のデータが無差別に収集される処理を正当化することはできない。
  - したがって、本データ処理は必要性と比例性の要件を満たしていない。
- 結論
  - LED第4条および第10条の要件を満たすような明確で正確かつ予見可能なルールが欠如していること、また、法執行機関が目的を達成するために本データ処理が厳密に必要であるという証拠が欠如していることにより、このアプリケーションの使用は必要性と比例性の要件を満たさず、EU基本権憲章の下での私生活の尊重と個人データ保護の権利に対する比例的でない干渉を意味するという結論が導かれる。

【ご参考】 GDPRとLEDにおける生体データ処理の適法性の基準

	GDPR（EU一般データ保護規則） （2016年制定）	LED（EU法執行指令） （2016年制定）
生体データの扱い	特別なカテゴリの個人データ （GDPR第9条1項）	特別なカテゴリの個人データ （LED第10条）
生体データ処理の適法性の基準 （どのような場合に生体データを処理できるか）	●以下のいずれかの場合（GDPR第9条2項） • データ主体の明示的な同意 • 雇用及び社会保障並びに社会的保護の法律の分野における管理者やデータ主体の義務の履行や権利の行使 • データ主体等の生命に関する利益の保護 • 政治、思想、宗教、労働組合の目的による団体の正当な活動 • データ主体によって明白に公開のものとされた個人データ • 訴えの提起もしくは攻撃防御、裁判所の権能行使 • 重要な公共の利益 • 予防医学もしくは産業医学の目的 • 公衆衛生の分野における公共の利益を理由とする処理 • 公共の利益における保管の目的、科学的・歴史的研究の目的、統計の目的	●以下をいずれも満たし（LED第8条） • 法執行目的に必要 • EU法、または処理の目標、処理される個人データ、処理の目的を指定する国内法で規制 ●さらに以下をいずれも満たす場合（LED第10条） • 厳密に必要 • データ主体の権利と自由に対する適切な保護措置 • かつ以下のいずれかの場合 （a）EU法または加盟国法によって承認 （b）データ主体または他の自然人の生命に関する利益を保護、または、 （c）データ主体によって明白に公開のものとされたデータ