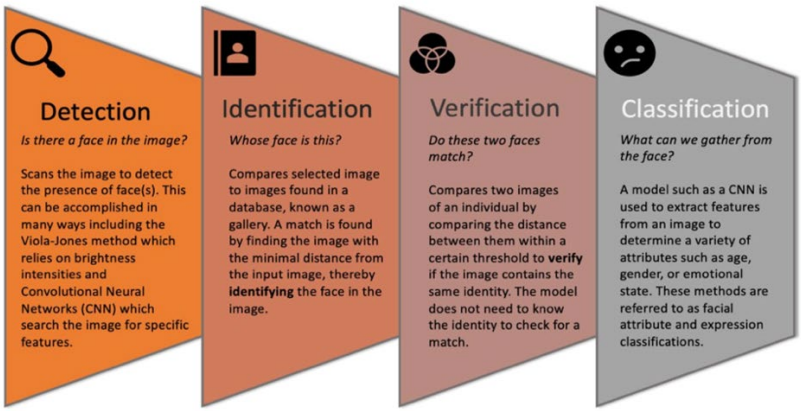
顔識別・顔認証技術に関する調査報告書の公表にあたって

本報告書は、顔識別・顔認証技術に関する、2017 年ころから現在までの国内外の状況を整理したものです。同技術の目覚ましい発展は国内外において共通していますが、同技術の法的制御に向けた本格的な取り組みが見られる国外の状況に比して、国内では、法的枠組みの実現に向けた取り組みはおろか、いまだ同技術の危険性や影響の大きさを十分に踏まえた議論がなされていない状況にあります。

例えば、一口に顔識別・顔認証技術といっても、国際的にはその利用の態様や文脈によって、Detection（「検知」）、Identification（「識別」）、Verification（「検証」）、Classification（「分類・データベース化」）の４つに区別されています。その全体像は、EU 議会のリサーチ機関(European Parliamentary Research Service)が公表した顔識別技術に関するレポート（Regulating facial recognition in the EU）においても引用された、Alan Turing Institute の下図にわかりやすく整理されています。



(Buolamwini, et al., 2020)

「検知」とは、画像ファイルの中に人の顔を探して特定する作業です。「識別」とは、「検知された画像とデータベース内の多数の画像を比較して」、検知された画像が誰の顔であるかを確認する作業です。これに対し「検証」は、識別対象の画像が「特定の閾値を超える」程度に認証対象の画像と合致するかを確認する作業です。「識別」は多数の画像から発見する作業であるのに対し、「検証」は登録済みの顔画像と合致するかを 1 対１対応で確認する作業です。「分類・データベース化」は、認証した顔画像から年齢、性別、感情などを「分析」したり、また撮影された場所や時間を紐づけて「データベース化」する作業です。

狭義の顔識別・顔認証技術は「検知」から「検証」までを指すことが多いとされていますが、多くの場合情報を取得した組織・機関ではClassification（「分析・データベース化」）まで行われています。そして、分類の目的や傾向によっては、「分析・データベース化」自体が、差別の再生産に繋がる懸念や、本人の望まない行動予測に用いられるリスクをもたらします。さらには、利用目的や分析目的が項目の分類方法などにフィードバックされ、それが差別的傾向や行動予測を強化するというサイクルが生じると、システム自体が社会に新たな差別を生み出したり、個々人の行動を予測するにとどまらず本人の気づかぬ緩やかな強制をもたらす可能性すらあります。

顔識別・顔認証に関する事例や研究報告に関しては、これら４つのどの段階の技術が利用され、問題とされているのか常に意識する必要があります。しかし国内の、とりわけ民間における議論では、これら４つの区別すら整理されずに、その利便性のみが強調される傾向にあります。顔識別・顔認証技術に関して法的枠組みを導入するためには、こういった国際的に前提とされる用語や議論を前提とする必要があります。

本報告書では、このような観点から、国内における同技術の利用状況と法的議論と、国外における同技術に関する法的規律、裁判例、提言書等を対比することで、日本でも同技術に関するより活発な法的議論が展開されることを狙いとしています。本報告書が、顔識別・顔認証技術に対する法的枠組みを検討する際の、議論の足がかりとなることを願っています。

2024年5月　監視とプライバシープロジェクト　一同

顔識別・顔認証技術に関する調査報告書

はじめに

2019 年 4 月、香港政府は、被疑者の引き渡し協定を締結していない国・地域にも引き渡しをできるよう、「逃亡犯条例」の改正案を提出した。中国政府に批判的な活動をすれば中国に引き渡されるとの懸念が強まり、大規模な抗議活動に発展した。香港政府はデモ活動を取り締まるため、街頭の監視カメラを活用してデモ参加者の認証・識別を進めていった。デモ参加者は当局に顔画像を把握されないよう、マスクをしてデモをするようになった。8 月 30 日には、抗議運動のリーダーである黄之鋒氏と周庭氏が逮捕された。10 月 4 日、香港で「覆面禁止法」が制定され、翌日施行された。デモ活動などに参加する際、マスクやゴーグルなどで顔を覆うことを禁止するものだった。

覆面禁止法は顔識別・顔認証技術の威力や、その民主的な価値を象徴する法律である。全体主義は、匿名で政治に参加する権利を奪おうとする。民主的な社会の維持にとって、匿名性は必要条件である。かつては仮に街中に監視カメラを張り巡らせたとしても、その膨大な撮影データから人の顔を検知したり、それが誰の顔かを分析することには途方もない時間と労力が必要だった。収集したデータを保存するための容量も桁外れだった。テクノロジーの進歩と AI の発展によりこれらの時間と労力は取るに足らなくなった。

近年では、官民問わずまた国の内外で、様々な文脈で顔識別・顔認証技術が利用されている。それに呼応するように、国内外のさまざまな機関が、安易な顔識別・顔認証技術の開発・利用に警鐘を鳴らしている。本報告書は、これらを整理し、日本の現状における課題をまとめるものである。

以下においては、まず国内の主要な政府機関や民間団体の報告書等を整理する。続けて海外の動向を紹介する。そのうえで、日本の現状の課題等を検討する。

第１　国内における官民の利用状況

国内において顔識別・認証技術の利用が物議を醸した事例の嚆矢は、2013 年 11 月に発表された、顔認証を利用した実証実験である。大阪駅などに設置されたカメラにより、利用者を「検知」してその動線を把握することにより、避難誘導などへ

の活用の可能性を検証することを目的としていた。当時はAIが未発達で、議論の中心は公的施設における顔識別・顔認証情報を含む個人情報の取得の是非にとどまっていたが、そこから数年が経ち、後述する2021年9月のJR東日本の事例を一つの象徴として、様々な事例がメディアを賑わすようになった。ただ、報道は、顔識別・顔認証技術のメリットや到来する便利な未来社会に力点が置かれることが多く、リスクや懸念点については旧来型のプライバシーの議論や個人情報保護法の文脈を指摘するにとどまる。また、各省庁でも行政目的を達成するために同技術の利用を始めていることが公表されているが、国外でなされるような抜本的な問題点を巡る議論があまり意識されていないものが散見される。

1　民間企業の利用

報道されたものだけでも、民間企業における利用は膨大で、多種多様である。本報告書では、その利用設計に潜む問題がメディアで指摘されたいくつかの事例を紹介する。いずれの企業においても、報道後に設計を変更したり、誤解を招く表記だったと弁明したりしているが、透明性を確保する法的規律を欠くためもあって、対応は自主的なものにとどまり、その詳細な実態は不明であることが多い。

（1）JR東日本の犯罪捜査等への利用

2021年9月21日、読売新聞のスクープにより、JR東日本が同年7月から、顔識別・顔認証技術を用いて、駅構内の利用者を「検知」、「識別」、「認証」していることが明らかとなった。同社は、過去に駅構内などで重大犯罪を犯した出所者・仮出所者や指名手配中の被疑者、さらには不審行動をとった人の顔情報をデータベースに登録し、主要110駅などに設置された8350台のカメラで「検知」した顔情報を自動「検証」し、警察への通報や手荷物検査に繋げていたと報じられたのである。しかも、このシステムの稼働に当たり、同社が個人情報保護委員会に事前照会をし、「保護と利用のバランスを図っており、今回の防犯という目的に限った利用であればバランスを欠くケースではない」（朝日新聞Web（2021年9月21日20時00分））旨の回答を得ていたとされる。

いくつかのメディアがプライバシーの問題などを指摘し、JR東日本は一部の運用を取りやめる旨を公表した。日本弁護士会連合会などは全面的な中止を求める声明などを策定し、また個人情報保護委員会は、同社の事例をきっかけとして有識者検討会を組成して後述のガイドラインを公表するに至った。

（２）渋谷書店万引対策共同プロジェクト

万引被害の対策として、渋谷の啓文堂書店、大盛堂書店及び MARUZEN&ジュンク堂書店が共同で展開するプロジェクトである。万引き犯人の映像を三者間で共有することで、相互に自店の顔認証システムに登録し、来店時にアラートを出す仕組みを設けている。システム導入後万引被害が半減したと報じられている。

プロジェクトの基本綱領が公開され、また外部の有識者から構成される運用検証委員会を設置している。

（３）渋谷１００台プロジェクト

「40 代／男性、同席者有り（30 代／女性）、ブランド A を着用／所持、休日 12 時より渋谷に銀座線で到着、ヒカリエでランチ、 明治通りを通り、宮下パークへ低速で移動（ショッピング目的を想定）、月 3 回目（前回：休日◯曜日）・今年 10 回目の渋谷、ヒカリエ来店数◯回、前回店舗 A・B にて購入を実施……」。

これは、2023 年 7 月から「渋谷 100 台プロジェクト」を運営する、Intelligence Design 社が同年 9 月 5 日まで同プロジェクトのウエブサイト[1]で公表していたスライド資料の一部の記載である。同プロジェクトは、「渋谷駅周辺の広域に 100 台の AI カメラを設置」し、「人流データを複合的に可視化、分析することにより、マーケティングや防犯における新たな視座の獲得や、データ利用価値を模索する」ことを目的としている。

報道によりプライバシー侵害性や個人情報保護法違反が指摘されたことを受け、「誤解を招く可能性のある記載であった」として、スライド自体は削除された。「個人情報を含む映像データの保存」はせず、「人流に関する属性情報およびこれに基づく統計情報」のみを取得するため、個人情報保護法には反しないとのプレスリリースが公表されている[2]。

主要商店街のほか、コミュニティバス内などにも AI カメラを設置しているとウェブサイトに掲載されているが、具体的な取得情報や利用態様、監督制度の有無などについては、公表されていない。

２　国の省庁の利用状況等

各省庁のウェブサイトでは、以下のとおり、顔識別・顔認証技術を実際に利用しあるいはその利用を検討していたり（警察庁、税関、法務省（出入国管理庁）等）、

[1] https://idea.i-d.ai/shibuya-project/

[2] 「HP 記載内容の修正について 2023.09.05」 https://idea.i-d.ai/news/news-post/370/

その利用に関してガイドブックを公表する（経産省、総務省、国交省、文科省等）などしている。

もっとも、顔認識・顔識別技術がここ数年で著しく発達していることを踏まえると、実際には、各省庁においてウェブサイトの公表を超えたさらなる利用がなされている可能性がある。顔認識・顔識別技術が、利用方法や態様によっては、個人のプライバシー権等の重要な権利を侵害するおそれがあることに鑑みれば、その利用方法や態様については、立法その他適切な方法によって包括的に規制され、かつ、国民に対して情報公開がなされる必要があると思われる。

（1）文科省：「学校における先端技術活用ガイドブック（第２版）」

文科省では、学校等において先端技術を利用した実証実験などを行う際のガイドラインとして、2020 年度（令和 2 年度）に「学校における先端技術活用ガイドブック（第１版）」を、また翌年には同第 2 版を公表した。

ガイドブック内には、実証実験の一例として、教室内に 5 台のカメラを設置し、AI 搭載のセンシング技術を活用した出欠確認・検温の自動化などを行ったことが報告されている。また、箕面市の実例として、教室にマイクとカメラを設置し、教師と児童生徒の発話・無音の比率や、児童生徒の挙手行動、教師の板書行動、児童生徒の目線、机間巡視の軌跡を記録し、教師の研修・指導に活用していることが報告されている。

なお、教室における AI 搭載の顔識別・顔認証技術の利用に関して、取得データの保管期限、アクセス権者、分析過程における匿名化の可否など、児童・生徒のプライバシーなどに配慮した記載は見当たらなかった。

（2）国交省：「空港での顔認証技術を活用した One ID サービスにおける個人データの取扱いに関するガイドブック」

空港における旅客手続きの円滑化に資する取り組みの一つとして、成田空港・羽田空港において、顔認証技術を用いた搭乗手続きである「One ID サービス」が実施されている。顔画像情報という生体情報を活用するため、事業者は個人データの取扱いについて特に厳格に管理することが求められることから、国土交通省航空局では、2019 年（令和元年）10 月に有識者や関係機関で構成される「One ID 導入に向けた個人データの取扱検討会」を設置し、2020 年（令和 2 年）にガイドブックとして取扱指針を取りまとめて公表している。

ガイドブックによれば、当該技術は、従来、人の目で行われていた本人確認を顔認証による個人識別技術を活用して行うことにより、各手続きで搭乗券やパスポートを提示することが不要となり、“顔パス”で通過できることから、ストレスフ

リーな旅行環境の実現に向けた空港内の搭乗手続きの円滑化を目的として導入するものとされる。

利用目的を搭乗手続きに係る利用に限定すること、顔認証の利用は希望する旅客のみとし、従来通りの手続きも存置すること、個人データは取得後２４時間以内に消去し、定期的な監査を実施することなどを求めているとのことである。

（３）警察庁：「三次元顔画像識別システム」（『警察白書　平成２７年』中の「科学技術の活用」）

三次元顔画像識別システムとは、防犯カメラ等で撮影された人物の顔画像と、別に取得した被疑者の三次元顔画像とを照合し、個人を識別するものである。

資料によれば、一般に、防犯カメラ等で被疑者の顔が撮影される角度は様々で、防犯カメラ等の画像と被疑者写真等を単純に比較するだけでは個人の識別が困難な場合が多いが、このシステムでは、被疑者の三次元顔画像を防犯カメラ等の画像と同じ角度及び大きさに調整し、両画像を重ね合わせることにより、より高い精度で個人を識別することが可能となるとされている。

（４）経産省・総務省：「カメラ画像利活用ガイドブック」

経済産業省・総務省は、IoT 推進コンソーシアム・データ流通促進ワーキンググループの下に設置した、カメラ画像利活用サブワーキンググループにおいて、利活用ニーズの高いカメラ画像を安全安心に利活用するために、事業者が配慮すべき事項等を検討し『カメラ画像利活用ガイドブック ver1.0』を 2017 年（平成 29 年）1 月に公表し、またユースケースを追加検討し改訂した ver2.0 を 2018 年（平成 30 年）3 月に公表した。さらに 2021 年（令和 3 年）から 2022 年（令和 4 年）にかけて、国内外の動向を踏まえ、改正個人情報保護法との関係から対応すべき点や、プライバシー保護について注意喚起すべき点などを追加検討し、ver3.0 として 2022 年 3 月に公表した。

ガイドブックによれば、事業者に対し、カメラ画像及びカメラ画像から生成される各種データの利用目的等を定め、プライバシー保護の取り組みを促すことを目的としているとされている。

（５）厚労省：医療保険の資格確認におけるカードリーダー

顔画像利用の実例として、医療保険の資格の有無をオンラインで確認するために、マイナンバーカードの顔写真データを IC チップから読み取り、その「顔写

真データ」と窓口で撮影した「本人の顔写真」と照合して、本人確認を行うことができるカードリーダーの活用などが報告されている。

（６）財務省：「年齢識別装置を装備したたばこ自動販売機」

たばこの自動販売機に、顔認証方式の年齢識別機能を備えたものを購入したと報告されている。取得した顔画像の利用、管理、保存などに関する記載は見当たらなかった。

（７）関税局：税関検査場電子申告ゲート

関税局では、増加し続ける入国旅客の円滑な入国と待ち時間の短縮、税関検査場の混雑の緩和を図るために、税関検査場電子申告ゲートを導入したと報告されている。同ゲートの利用により、電子申告端末に二次元コードと IC 旅券（パスポート）を読み取らせることで、電子的に税関申告を行うことができるとされる。

（８）法務省（出入国管理庁）：外国人出国手続における顔認証ゲートの活用

出入国在留管理庁では、2019 年（令和元年）7 月 24 日の羽田空港を皮切りに、成田空港、関西空港、福岡空港、中部空港、新千歳空港及び那覇空港において、順次顔認証ゲートの外国人出国手続における運用を開始している。

顔認証ゲートは、ＩＣ旅券のＩＣチップ内の顔の画像と、顔認証ゲートのカメラで撮影した顔の画像を照合して本人確認を行う。照合により本人確認が完了し問題がなければ、ゲートを通過することができ、顔認証ゲートを利用した場合には、入国審査官から旅券に証印（スタンプ）を受ける必要がない。

顔認証ゲートで撮影された顔写真は、本人確認のための照合にのみ用いられ、保存されることはないとされている。

（９）金融庁：「FinTech 実証実験ハブ」

従来の ID・PW 方式に替えて、顧客のスマートフォン等の取引端末に係る位置情報と顧客の生体情報（顔認証）を、インターネットバンキングにおけるログイン・取引認証に用いるとともに、その位置情報を顧客の登録情報の最新化等に活用することを検討しているとされる。参加企業は、みずほ銀行、グーグル・クラウド・

ジャパン、野村総合研究所、大日本印刷、ほか協力銀行多数とされる。利用にあたってのプライバシー等への配慮等の記載は見当たらなかった。

（１０）小括

以上のとおり、各省庁における行政サービスにおいては、すでに顔識別・顔認証技術が活用され、またさらなる活用が見込まれている。一部の省庁ではプライバシーに配慮した記載が認められたが、文科省の実証実験のように、利用者や対象者のプライバシーと衝突する可能性が少なくないサービスでも、資料内にプライバシーへ配慮した記載が見当たらないものが認められた。

第２　国内における包括的なガイドライン等

後述の国外における議論状況と比較すると、日本においては法的規制等に関する包括的な議論状況が充実したものとは言い難い。本報告書では代表的なものとして、個人情報保護委員会の説明文書（マニュアル）と日本弁護士会連合会の意見書を紹介する。

１　個人情報保護委員会のマニュアル

個人情報保護委員会は、個人情報保護法により新設された機関で、個人情報の適正な取扱いの確保を活動目的としている。個人情報保護委員会は、2023 年 3 月、「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」と題する説明文書（以下「個人情報保護委員会マニュアル」という。）を公表した。近年、事業者などにおいて顔識別カメラの利用が広がっている一方、利用態様等によっては受忍限度を超えプライバシー侵害となりうることから、適切な対応を促すために有識者検討会における検討を踏まえて作成された文書である。

個人情報保護委員会マニュアルは、顔識別機能付カメラシステムのメリットとして、顔特徴量を用いることにより、従来型防犯カメラによる目視よりも容易に検知対象者を検知し、発見することができ、追跡の効率性が非常に高く、特定の個人を長期かつ広範にわたり追跡して監視につながるおそれがあると指摘する。商用ではなく犯罪予防や安全確保（行方不明者等の捜索等）のために顔識別機能付カメラシステムを利用するに際して、個人情報保護法の遵守や肖像権・プライバシー保護の観点から留意すべき点や望ましい対応についての説明がなされており、チェックリストを末尾に添付するなど、民間の事業者が顔識別機能付きカメラシステムを導入する際のマニュアルとして利用できるよう工夫されている。

最高裁判例も挙げながら、個人情報保護法違反にならない場合であっても不法行為が成立する場合があることを注意喚起したり、AI の学習内容によって顔識別機能付きカメラシステムの被検知者が、性別の違いや肌の色の違いにより特定の属性の者に対して偏る等の不当な差別的取扱いが違法行為となることを指摘する。

他方で、顔識別・顔認証技術の危険性を踏まえた包括的な法規制の提言などはなされていない。万引き犯とテロや重大犯罪とを区別することなく犯罪予防として位置付けていたり、撮影された画像を照合用データベースに登録した場合の保存期間について上限の設定もないなど、不十分な現行法の規律により生じる問題点等は指摘しておらず、現行の法令や判例法理の枠組みに基づく留意点の説明にとどまる内容となっている。

2　日本弁護士連合会の意見書

日本弁護士連合会（日弁連）は、2021 年、「行政及び民間等で利用される顔認証システムに対する法的規制に関する意見書」（以下「日弁連意見書」という。）を公表した。

日弁連意見書は、顔認証システムの懸念点として、特定の監視対象者の顔認証データベースをあらかじめ作成している限り AI を用いて収集された顔画像データを自動的に検索・照合することが可能であること、顔認証データが検索・照合の対象となってしまうと、個人が過去から将来にわたって網羅的な監視対象とされ、その移動履歴が詳細に特定され得ることから、指紋よりもはるかに緻密に個人特定を可能とする生体情報であり、DNA 型情報に準じる高度のセンシティブ性があることを挙げるなど、より顔識別・顔認証技術の核心を踏まえた分析をしている。

これらの懸念を踏まえ、日弁連意見書では顔認証システムの利用等を規律する個別法の制定を求めており、その内容として以下の項目が必要であると整理している。

① 明示の同意のない顔認証データベース等の作成及び顔認証システムの利用の原則禁止
② 例外的に行政機関や民間事業者等が顔認証データベース等を作成した顔認証システムを利用することができる場合の厳格な条件
　a　登録対象者は、テロリストなど、極めて限定的なものであること
　b　達成しようとする行政目的が、入国管理の際のテロリスト等のチェックなど、極めて重要な行政目的であること
　c　本人の同一性確認のために、顔認証システムの利用が手段として不可欠であること

d　照合の対象となる顔認証データの元である顔画像データは、行政目的達成のために不可欠な場所で取得されたものに限定し、当該場所以外で収集された顔画像データを使用しないこと

e　顔認証データベースの作成及び顔認証システムの設置・利用について、法律が具体的かつ明確に許容していること

f　民間業者が利用する場合における対象の限定や犯罪発生の相当高度の蓋然性など

③ 個人情報保護委員会による実効的な監督

④ 顔認証システムに関する基本情報の公表

⑤ 誤登録されている可能性のある対象者の権利保護

などを盛り込んだ法律（個別法）の制定を求めている。

日弁連意見書は、日本において包括的な法規制を提言するほぼ唯一の意見書であり、その提言内容も危険性を踏まえた具体的かつ現実的なものである。

第３　国外の動向

日本の動向と対比すると、国外においては顔識別・顔認証技術のリスクを強調する報告書等が多い傾向にある。本報告書では、国際機関の報告書や各国の司法機関の判決、研究機関のレポートなどを紹介する。

１　国連人権高等弁務官事務所（OHCHR）の年次報告書

国連人権高等弁務官事務所（OHCHR）は、近年の年次報告書において、デジタル時代におけるプライバシーその他の人権に関する重要な問題提起を行っている。2020 年には「新しい技術が抗議活動を含む集会における人権の促進及び擁護に及ぼす影響」に関する報告書を[3]、2021 年には国や企業による AI の広範な利用がプライバシー権及び関連する権利に与える影響を分析した「デジタル時代におけるプライバシーの権利」と題する報告書を[4]、2022 年にはスパイウェアと監視に関する問題を分析した「デジタル時代におけるプライバシーの権利」と題する報告書[5]をそれぞれ公表しており、これらのなかで顔認識・顔認証の問題に触れている。

[3] A/HRC/44/24（2020 年 6 月 24 日）Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including protests

[4] A/HRC/48/31（2021 年 9 月 13 日）The right to privacy in the digital age

[5] A/HRC/51/17（2022 年 8 月 4 日）The right to privacy in the digital age

2020 年の報告書では、顔識別・顔認証技術について、“偽陽性”の認定による人違いの危険、人種や民族、性別などに着目した差別的な運用、集会の自由で伝統的に保護されてきた公共空間における匿名参加の自由を崩壊させかねない、といった重大なリスクを指摘したうえで、他の新たな技術とともに、参加者の監視や取締りに利用されることで平和的な集会の自由の行使を含む人権を侵害することに繋がりうるために、平和的な集会の自由及びこれに関連する権利が政府により侵害されないよう、人権規範や基準と整合する規制枠組みの確立が求められると述べている（V. New technologies and the surveilling of protesters（7p 以下）参照)。

2021 年の報告書では、デジタル時代のプライバシー全般の問題点を指摘する中で、顔識別・顔認証技術がプライバシーに与える影響について、2020 年報告書の内容を紹介したうえで、とりわけ重視されるべき点として、法執行機関などが「公共の場所における個人を体系的に同定し、追跡する能力を劇的に高めることで、人々が監視されずに日常生活を送る力を弱体化させ、かつ表現の自由、平和的集会及び結社の自由、並びに移動の自由に対する直接的な悪影響をもたらすこと」を強く懸念している（B. Concerns about artificial intelligence systems in key sectors （7p 以下）参照)。

2022 年の報告書では、監視カメラの利用が世界的に拡大しており、特に顔認識や不審な動作を認識する画像解析能力を備える高度なカメラが増えていること、こうした顔認識技術とその他の生体情報認識技術の進化が、公共の場所にいる個人や集会の参加者を識別する能力を飛躍的に向上させたことなどを指摘したうえで、公共の場所において無差別に本人の同意なく画像を収集・分析・保持することは、プライバシー権に対する干渉となるほか、公共の場所における監視が、特定の集団や個人の監視活動といった個人やコミュニティに直接影響を与える措置につながることがあり、AI の利用と相まって、マイノリティに対し不釣り合いな影響を及ぼしており、また表現の自由や平和的集会の権利の行使を委縮させる効果を持つとする（C. Human rights impacts（11p 以下）参照)。

以上を踏まえて OHCHR は、各国に対して以下の点を推奨している(IV. Conclusions and recommendations （15p 以下）参照)。

(a) 一般市民の監視を含むプライバシー権に対するいかなる干渉も、法的根拠、正当な目的、必要性、比例性、及び非差別の原則を含む国際人権法に準拠すること

(b) 監視システムの設計、開発、購入、展開及び運用時に、包括的な人権影響評価を含む人権デューデリジェンスを制度的に実施すること

(c) 新しい監視システムや権限を評価する際には、それらが置かれた法的及び技術的な環境全体を考慮すること。また、将来の政治的変化によるリスクを含む、濫用、機能拡大及び目的変更のリスクも検討すべきこと
(d) 公共・民間部門に適用される、国際人権法に準拠したデータプライバシー法（プライバシー権を効果的に保護するための保障、監視及び救済手段を含む）を制定し、独立した中立的な機関により効果的に施行すること
(e) 監視技術の使用について、一般市民及び影響を受ける個人やコミュニティに適切に情報を提供し、その効果と人権への影響を評価するための関連データを公表するなど、透明性を向上させるための措置を速やかに取ること
(f) 監視技術の使用に関する公共の議論を促進し、監視技術の取得、移転、販売、開発、展開、及び使用に関する意思決定（公共政策の検討及び実施を含む）にすべての利害関係者の有意義な参加を確保すること
(g) 人権を保護するための十分な保障が整うまで、公共の場で個人の識別や分類に使用できる生体認証システムなどの監視システムの国内及び国際的な販売及び使用を停止すること。かかる保障は、これまで勧告された方針に準拠し、国内及び輸出管理措置を含むべきこと
(h) 監視システムの使用に関連する人権侵害の被害者が効果的な救済手段にアクセスできるようにすること

2 EUにおける動向

（1）概要

EUの主要な法源として、はじめにEUの憲法と立法に簡単に触れておく。複数の国家で構成されるEUにおいて、憲法に相当する法源としてEU基本条約[6]とEU基本権憲章（the Charter of Fundamental Rights of the European Union）がある。その下位法規に当たるEU立法の主要なものとしては、規則（regulation）、指令（direction）及び決定（decision）の３種類がある。規則はEUの全加盟国に直接適用される。これに対し指令は、加盟国に対し、達成しなければならない目標を規定するにとどまり、直接適用はなされない。各国は指令の定める目標を実現するべく国内法を制定する作業が求められる。決定は、個別具体的な案件に関してその名宛人（EU加盟国や個別企業）を拘束するものとなる。

[6] EU基本条約としては、EU条約（the Treaty on European Union）とEU機能条約（the Treaty on the Functioning of the European Union）がある。

顔識別・顔認証に関して重要なEU立法としては、GDPR及び法執行機関指令（捜査機関データ保護指令）並びにAI規則がある。その他法的拘束力等はないものの重要の影響力を有するものとしては、EDPB[7]が策定したガイドラインがある。

（２）GDPRにおける顔識別・顔認証規律について

GDPR（General Data Protection Regulation、一般データ保護規則）は、2018年５月に施行されたEUにおける個人情報保護の基本法である[8]。GDPRでは、顔識別・顔認証を生体データと位置づけ、特別な種類の個人データとして規制を及ぼしている。

すなわち、GDPR4条（定義）の(14)号は、「『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」[9]と定義し、同９条１項では、「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取扱い、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取扱いは、禁止される」と規定している。

顔画像の利用は原則禁止されるが、たとえば、データ主体が特定された目的のための取り扱いに明確な同意を与えた場合（同条２項a）や、EU法又は国内法に基づき、重要な公共の利益のために比例的に用いる場合で、データ主体の権利や安全性を確保するための措置を講じたとき(同g)などでは、生体データ（顔識別・顔認証）の利用も認められる。

これらの例外のうち、たとえば(a)の「明確な同意」に関連して、EDPBのガイドラインでは、顔認識技術を用いて建物へのアクセスを管理しているケースについて、「明確に説明を受けた上での同意を事前に与えている場合にのみ、(顔認識技術を用いた）アクセス方法を利用できる。しかし、事前に同意を与えていない者のデータが取り込まれることのないことを確保するためには、例えばボタンを押すなどの方法によるなど、データ主体自身が顔認識機能を作動させるようにするべき

---

[7] 欧州データ保護会議（The European Data Protection Board）。GDPRや法執行機関指令が加盟各国で統一的に運用されるようにするとともに、加盟各国の個人情報保護監督機関相互の協力を促進する欧州の独立機関。

[8] EU基本権憲章８条(1)項とEU機能条約16条(1)項は、それぞれ個人データの保護について規定している。つまり、EUの憲法レベルで個人データの保護が規定されており、GDPRは、その前文(1)項で、これらEU憲法の条項に触れている（後述する法執行機関指令の前文も同様）。

[9] 和訳は個人情報保護委員会による。GDPRにつき以下同じ。

である。取扱いの適法性を確保するために、管理者は、バッジや鍵など、生体認証の取扱いなく建物にアクセスするための代替手段を常に提供しなければならない」と記載している[10]。

（３）法執行機関指令（捜査機関データ保護指令）における規律

GDPR2 条 2 項(d)号は、「公共の安全への脅威からの保護及びその脅威の防止を含め、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ために行われる」個人データの取り扱いには GDPR は適用されないと規定している。代わりに捜査機関等による個人データの取り扱いに適用されるのが、EU 立法のうち「指令」の形式で定められた「法執行機関指令」である[11]。

法執行機関指令は、GDPR のように規則（EU 議会における施行と同時に、加盟国政府や企業、個人に直接効力が及ぶ）ではなく、ディレクティブ（指令）なので、加盟国による国内法の制定によって効力を有することになる。

法執行機関指令 3 条（定義）の（13）号は、GDPR と同様、「『バイオメトリックデータ』[12]とは、物理的、生理的、又は行動の特徴に関して特別な技術を用いて処理することによって生じるもので、顔画像又は指紋のデータのように、当該自然人の一意的な特定を可能にし、あるいは確定する個人データをいう」と定義している[13]。また、同指令第 10 条（特別なカテゴリーの個人データの処理）は、その柱書で、「人種的若しくは民族的出自、政治的意見、宗教的若しくは哲学的信条又は労働組合加入を明らかにする個人データの処理並びに遺伝的データ、自然人の一意的な特定を目的とするバイオメトリックデータ、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、厳密に必要とされ、データ主

---

[10] EDPB における 2020 年 1 月 29 日採択「ビデオ装置を介した個人データの取扱いに関するガイドライン 3/2019 バージョン 2.0」77 項記載の例

[11] 正式名称は、「犯罪の予防、捜査、取り調べ若しくは起訴、又は刑罰の執行を目的として、所轄官庁により実施される個人データの処理に関する自然人の保護、並びに当該データの自由な移転に関する EU 指令」DIRECTIVE (EU) 2016/680 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA

[12] 生体データ。後記脚注 11 の JCLU 仮訳では「バイオメタリックデータ」と訳しているため、ここでは「バイオメトリックデータ」とした。

[13] JCLU では法執行機関指令（捜査機関データ保護指令）を全訳（仮訳）している（http://jclu.org/issues/privacy で公表）。ここではその仮訳を用いている。法執行機関指令につき以下同じ。

体の権利と自由のための適切な安全措置が施され、かつ、以下の場合にのみ許可される」と規定する。ここに規定する「以下の場合」として、次の(a)，(b)及び(c)が規定されている。

(a) ＥＵ又は加盟国の法によって認可されている場合
(b) データ主体又は他の自然人の必要不可欠な利益を保護する場合
(c) データ主体によって公表されたことが明白なデータに関する処理である場合

上記(a)により、加盟国の法律で定めれば顔識別・顔認証も可能になる。もっとも、法執行機関指令の下では、間接アクセスやログ検証の仕組みなどが設けられており、独立した監督機関による厳格な監督が及ぶ点に特徴がある。間接アクセスとは、データ主体本人のアクセス権が制限されている一定の場合[14]に、本人に代わって、監督機関によって行使される仕組みである（法執行機関指令 17 条)。ログ検証の仕組みは、自動処理システムにおける個人データの収集、変更その他の利用について、処理操作の理由及び日時等が確定でき、かつ可能な限り個人データの参照者や個人データの受領者を特定できるようにログを残すことを求め、そのうえで、監督機関から要請があった場合には、このログを開示しなければならないとする仕組みである（法執行機関指令 25 条)。

（４）欧州 AI 規則における規律

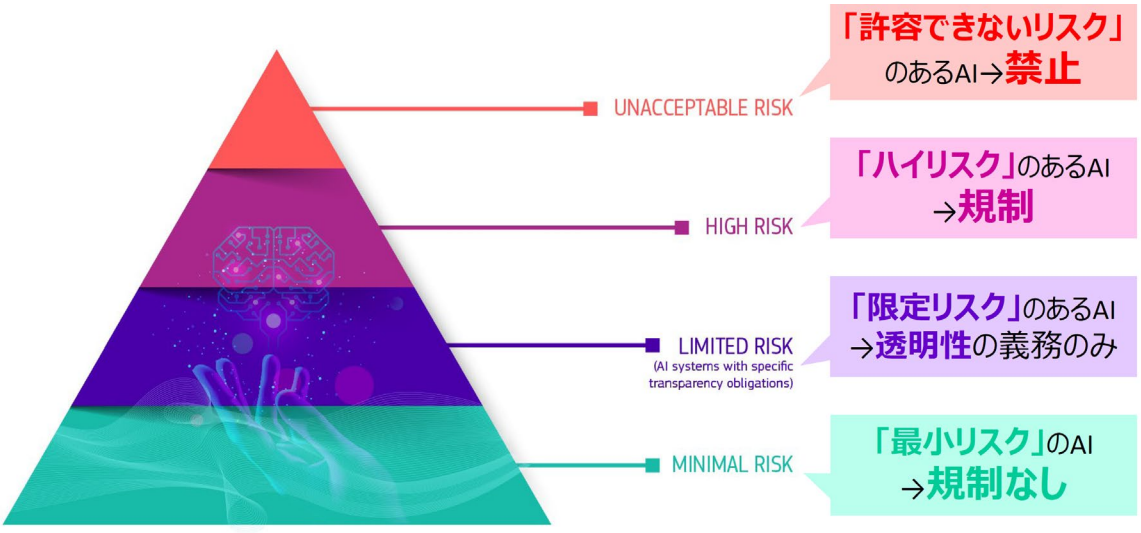
2023 年 12 月 9 日、欧州理事会は、2021 年 4 月に策定していた「人工知能に関する整合的規則（人工知能法）の制定及び関連法令の改正に関する欧州議会及び理事会による規則案」（以下「欧州 AI 規則案」という）に関して、欧州議会との暫定的な合意に至ったと公表した（以下「暫定合意案」という。）[15]。その後、欧州議会は、2024 年 3 月 13 日に暫定合意案を承認した。

---

[14] 公務上又は法律上の照会、捜査又は手続の妨害を回避する目的、刑法犯の防止、拘禁、捜査若しくは起訴又は刑法上の罰金の執行を害することを回避する目的、公共の安全を保護する目的、国家の安全を保護する目的、他者の権利及び自由を保護する目的から、データ主体本人によるアクセス権が制限される場合（法執行機関指令 13 条３項、15 条３項、16 条４項）

[15] 暫定合意案の全文は以下に掲載されている。
https://data.consilium.europa.eu/doc/document/ST-5662-2024-INIT/en/pdf

欧州 AI 規制案においては、リスクに応じて規制内容を変えるリスクベースアプローチが採用されている。「許容できないリスク」のある AI、「ハイリスク」のある AI、「限定リスク」のある AI、及び「最小リスク」の AI の 4 つにカテゴリー分類し、各 AI システムの危険性に対応した規制が定められている。上記のリスクベースアプローチについて図を用いて整理すると、以下のとおりである（三部裕幸弁護士が総務省に提出した説明資料（「EU の AI 規制法案の概要」）[16]の 4 頁から引用。）



（図の出典）https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

「許容できないリスク」のある AI システムについては原則として使用等が制限され、人の安全や権利に影響を及ぼすおそれが高い「ハイリスク」AI システムについては、一定の要件に該当するもののみ使用等が許可される。「限定リスク」のある AI システムについては、透明性の義務（欧州 AI 規則案 52 条 1 項）を順守することを条件に利用等が許可される。「最小リスク」しかない、又はリスクのない AI システムについては、特に制限はない。

顔識別技術を用いた AI システムについては、第 1 に、法執行を目的とした公のアクセス可能な空間における「リアルタイム」で一般市民の生体情報（顔データーを含む）を収集・識別する遠隔生体識別システム（欧州 AI 規則案 5 条 1 項（d））及びインターネット上の映像等から顔画像を無差別に収集し、顔認識データベースを作成・拡張する AI システム（暫定合意案）に関しては、「許容できないリスク」のある AI として、原則禁止される。これらは、①誘拐・人身売買・性的搾取・行方不明者の捜索、②「真正かつ現在の」又は「真正かつ予見可能な」テロ攻撃等の防止、及び③特定の重大な犯罪（少なくとも 4 年の拘禁刑）の被疑者に対する捜査といった限定的な法執行目的の場合に限り、厳密な必要性を要件として、例外的に使用が認められる（暫定合意案）。

[16] https://www.soumu.go.jp/main_content/000842190.pdf

第２に、生体情報を収集して自然人を識別する、「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」はハイリスクＡＩとされ、同じく原則禁止される。AI規則案8条乃至115条に記載された各要件を満たす必要があるほか、システムを管理し、利用するオペレーターは同16条乃至29条の義務を遵守しなければならないとされている。

（５）EDPB顔識別に関するガイドライン

EDPBは、2023年4月26日、「法執行分野における顔識別技術の利用に関するガイドライン」（「EDPB顔識別ガイドライン」）の第2版を採択した。同ガイドラインでは、顔認証システムは法執行機関指令（Law Enforcement Directive） を厳密に遵守すべきことを強調しており、ＥＵ基本権憲章[17]に規定されているように、必要性及び比例原則にしたがって使用されるべきであるとする。同ガイドラインは6つの事例をあげて、顔認証システムの事例が認められる場合と認められない場合を説明している。

たとえば、子どもの誘拐事件で被害者を特定するための利用は認められる場合があるが（ガイドライン・シナリオ２）、暴動が起こったデモにおいて、暴動参加者を識別するためにデモ参加者や周辺の映像をデータベース化するシステムは認められない（同３）。また、事前に捜査機関の関心がある捜査対象者のリストを作成しておき、対象者がショッピングモールなど公共空間に現れたとの情報を得た場合に、現場で遠隔地から顔認証を用いて通行人等との照合を行うことも認められない（同５）。

シナリオ5の結論を出す過程において、EDPB顔識別ガイドラインは、「公共の場所における匿名性」の重要性に言及している。公共の場所における匿名性は、市民集会への参加、市民集会などの場においてすべての社会的・文化的背景をもった人々と交流するなどの民主的な過程の前提となり、情報やアイディアを集め、交換するために不可欠である。公共の場所における匿名性の保護を弱体化することは、市民に重大な萎縮効果を与える。同ガイドラインは、このような指摘をしたうえで、シナリオ５において顔認識システムの利用は認められないという結論に至っている。

（６）顔識別・顔認証技術に関する裁判例

2023年7月4日、EU人権裁判所（ECtHR）は、Glukhin対ロシア事件において、EDPB顔識別ガイドライン等を参照しながら、顔識別技術が「高度に侵襲的な技術

[17] EU基本権憲章52条(1)項

である」とし、適切な法規制、必要性の検討、権利侵害との均衡などが取れていない場合には私生活の保護を定めた EU 人権規約 8 条と表現の自由を保障した同 10 条に抵触しうるとした上で、路上における平和的なデモを監視カメラで監視するロシア政府の対応には規約違反があると判示した。

3　欧州主要国及びアメリカ合衆国における動向

欧州主要国（フランス、ドイツ、英国）においては、EU 法の規律を踏まえ、様々な顔識別・顔認証に関する規律を定めている。アメリカ合衆国においては、サンフランシスコが顔識別・顔認証技術の利用を原則禁止とする条例を定めて注目を集めた。

（1）フランス

ア　データ保護法

個人情報保護に関する基本法として「情報処理、情報ファイル及び自由に関する 1978 年 1 月 6 日法律第 78-17 号」（1978 年制定　「データ保護法」）が制定されている[18]。データ保護法は、GDPR 及び EU データ保護指令制定を受けて重要な改正がなされている。

データ保護法は、GDPR 第 9 条 1 項と同様に、生体データの処理を原則として禁止し（同法 6 条 1 項）、GDPR 第 9 条第 2 項で例外として認める場合（データ主体の明確な同意がある場合など）にのみ処理を認めている（データ保護法 6 条 2 項）。

また、データ保護法には、刑事犯罪の予防と捜査、探知と訴追、または公共の安全および犯罪に対する脅威からの保護を含む刑事罰の執行を目的として行われる個人データの処理についての特別の規定がある。「生体データ」の取扱いについては、データ主体の権利および自由に対する適切な保護措置の下に、(a)絶対的に必要な場合で、(b)法律上または規制上の規定によって許可されている場合で、(c)－1 自然人の生命的利益を保護することを意図している場合、または(c)－2 データ主体によって明らかに公表されているデータに関する場合、に処理が認められている（88 条）。

イ　データ保護機関

データ保護機関として「フランス共和国データ保護機関」（CNIL: Commission Nationalede l'Informatique et des Libertés）が設けられている。CNIL は、2019

[18] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés,
https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000886460/

年 11 月 15 日付報告書「Reconnaissance faciale ： pour un débat à la hauteur des enjeux」(CNIL 報告書) において、顔認証技術の取扱いについて述べている [19]。

CNIL 報告書は、「顔認識の機能」として、(a)人物の認証 (authentification)と(b)人物の識別 (identification) を挙げている。

また、「顔認証技術のリスク」として、(a)取り扱うデータが他の個人データ以上に機微 (センシティブ) なデータで特別な保護が必要であるとし、(b)ユーザーの知らないところで利用可能であり、(c)公共空間での匿名性を損なう監視の可能性があり、(d)誤って識別されることにより非常に重大な結果をもたらす可能性があり、機器の設置や開発などの経済的コストがかかる技術であると指摘している。

そして、「顔認証技術の導入」にあたって３つの要件 ((a)実験的であっても許されないレッドラインを設定し、(b)人権尊重をアプローチの中心とし、(c)真に実験的なアプローチを採用すること) を挙げている。

ウ　刑事手続規則

刑事手続規則 (Code de procédure pénale) は、警察が、犯罪の被疑者、被害者、死因、重傷、失踪の原因について調査されている人物の写真を犯罪記録データベース (TAJ : Traitment des Antécédents Judiciaires) に保管し、顔認識装置を使用することを認めている。

国会の 2018 年の報告書によると、TAJ には 700 万から 800 万の顔画像が含まれている [2021]。情報の保存期間は、被疑者は 20 年間 (道交法などの特定の犯罪は 5 年に短縮され、殺人、誘拐などは 40 年に延長される)、被害者は 15 年間 (判決が確定次第、削除要求可) とされている [22]。

（２）ドイツ

ア　データ保護法

---

[19] CNIL, Reconnaissance faciale ： pour un débat à la hauteur des enjeux (15 Nov. 2019),
https://www.cnil.fr/sites/default/files/atoms/files/reconnaissance_faciale.pdf

[20] Greens/EFA,Biometric and Behavioural Mass Surveillance in EU Member States: Report for the Greens/EFA in the EuropeanParliament (Oct. 2021),
http://extranet.greens-efa-service.eu/public/media/file/1/7297

[21] 「欧州主要国における顔識別機能付カメラの利用に関する法制度に関する調査」2022 年 3 月 31 日　渥美坂井法律事務所・外国法共同事業
https://www.ppc.go.jp/files/pdf/major_european_countries_camera_report_R403.pdf

[22] https://www.service-public.fr/particuliers/vosdroits/F32727

個人情報保護に関する法律として、「ドイツ連邦データ保護法」（BDSG:undesdatenschutzgesetz）が制定されている[23]。

同法は、管理者による公共の場所でのビデオ監視は以下の場合に可能であるとしている（データ保護法4条第1項)。

(a)公的機関が業務執行をする場合

(b)立ち入り拒否を判断する権利を行使する場合

(c)具体的に設定された目的のために、正当な利益を保護する場合

のいずれかに該当し、かつ、

(d)これらに優先するデータ主体の正当な利益がない場合

公共交通機関（鉄道、船、バス）の車両や大型の公共アクセス施設では、個人の生命、健康及び自由を守ることが非常に重要な利益であるとみなされる（同項)。

加えて、データ保護法では、GDPR第9条(4)の権限委任に基づき、以下のいずれかに該当し、かつ、管理者の利益がデータ主体の利益を上回る場合に、特別なカテゴリーのデータの処理が認められている（BDSG 第22条)。生体データはこの特別なカテゴリーのデータに含まれる（同46条13項)。

(a)公的機関及び民間機関によるデータ処理が認められる場合

・データ処理が、社会保障及び社会保護の権利から派生する権利の行使、またそれに関連する義務の履行に必要な場合（BDSG 第22 条(1)1.(a))

・データ処理が、予防医学、従業員の労働能力の評価、医学的診断、医療もしくは社会的ケア又は治療の提供、医療もしくは社会的介護システム及びサービスの管理、またはデータ主体と医療専門家との契約に基づき、これらのデータが医療専門家または職業上の守秘義務を負う他の者によって、又はその監督下で処理される場合（BDSG 第22 条(1)1.(b))

・データ処理が、国境を超えた健康への重大な脅威からの保護、医療及び医薬品・医療機器の高い品質と安全性を確保など、公衆衛生分野における公益上の理由から処理が必要である場合（BDSG 第22 条(1)1.(c))

・データ処理が、重大な公共の利益のために急遽必要な際（BDSG 第22条(1)1.(d))

(b)公的機関によるデータ処理のみが認められる場合

・データ処理が、公共の安全に対する重大な脅威を防止するために必要な場合（BDSG 第22条(1)2.(a))

・データ処理が、公益の重大な損害を防止するため、もしくは公益の重大な懸念を保護するために緊急に必要である場合（BDSG 第22 条(1)2.(b))

[23] Bundesdatenschutzgesetz https://www.gesetze-im-internet.de/englisch_bdsg/

・データ処理が、緊急の防衛上の理由、または危機管理もしくは紛争予防の分野における連邦の公的機関の超政府的もしくは政府間の義務の履行または人道的措置のために必要な場合（BDSG 第 22 条(1)2.(c)）

イ　国内での状況

警察や自治体により顔認識技術が試験的に導入されている。ドイツの連邦データ保護会議（Conference of German Data Protection Authorities (Datenschutzkonferenz)（DSK)）は、民間機関（公的機関以外）によるビデオ監視に関するガイダンス（2020 年 7 月 17 日）を制定している[24]。また、DSK は生体認証解析に関するポジションペーパーを公表している[25]。

（３）英国

ア　データ保護法

英国は、EU からの離脱により GDPR の規律が直接及ぶことはないものの、「2018 年データ保護法」（DPA2018: Data Protection Act 2018[26]）が制定され、GDPR とほぼ同内容の規律が国内法化されている。

DPA2018 は、UK GDPR の適用がない法執行部門にも適用される。

イ　データ保護機関

英国のデータ保護機関は「情報コミッショナー事務局」（ICO: Information Commissioner’s Office）である。ICO は 2019 年に、公共の場での法執行機関によるライブ顔認識技術（live facial recognition technology）の使用に関する意見[27]を公表した。

同意見は、ライブ顔認識（live facial recognition）の使用には個人データを取り扱うため、「法執行目的」での管轄当局による個人データの処理は、DPA2018 の第 3 編の適用を受けるとし、技術の導入の必要性と比例性の検討、監視リストの作成、生体認証データの取扱いからデータの保持と削除に至るまで、ライブ顔認識技術の全過程に適用されるとしている。

---

[24] https://www.datenschutzkonferenz-online.de/media/oh/20200903_oh_v%C3%BC_dsk.pdf

[25] https://www.datenschutzkonferenz-online.de/media/oh/20190405_positionspapier-biometrie.pdf

[26] https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

[27] Information Commissioner’s Office, Information Commissioner’s Opinion: The use of live facial recognition technology by law enforcement in public places (31 Oct. 2019), https://ico.org.uk/media/about-theico/documents/2616184/live-frt-law-enforcement-opinion-20191031.pdf

また、ICO は、2021 年に公共の場でのライブ顔認識技術の使用に関する意見[28]を公表した。同意見は、公共の場で、特定のエリアにいる全員を対象として個人のバイオメトリックデータを自動収集するライブ顔認識の使用に関して述べたもので、法執行のための使用は対象としていない。同意見は、管理者は UK GDPR および DPA2018 を遵守しなければならないとし、公共の場でライブ顔認識を展開する際の共通の法的要件として、以下を挙げている。

・合法性・公平・透明性、目的の制限、データの最小化、正確性、記録保全の制限、完全性・機密性、説明責任というデータ保護の原則の遵守（UK GDPR 第 5 条）
・適切な法的根拠の選択（UK GDPR 第 6 条）
・特別なカテゴリーのデータや犯罪データを処理する適切な条件の遵守（UK GDPR 第 9 条及び第 10 条）
・データ主体の権利（通知を受ける権利、アクセス・訂正・削除権、処理制限権、異議権、自動意思決定およびプロファイリングに関する権利）を行使できるようにすること（UK GDPR 第 12 条～22 条）
・設計によるデータ保護・デフォルトとしてのデータ保護を確保するための適切な技術的措置および組織的措置の実装（UK GDPR 第 25 条）
・データ保護影響評価（DPIA）の実施（UK GDPR 第 35 条）

ウ　ビデオ監視に関するガイダンス

ICO は、2022 年にビデオ監視（Video Surveillance）に関するガイダンス[29]を公表した。

同ガイダンスは、公共部門および民間部門の組織によるビデオ監視システムによる個人情報の処理を対象とするもので、監視システムとしては、従来の CCTV、自動ナンバープレート認識、身体装着型ビデオ、ドローン、顔認識技術（FRT）、車載カメラ、スマートドアベルカメラを挙げているが、それらに限定されないとしている。同ガイダンスは、秘密の監視技術、DPA2018 第 3 編の法執行機関による処理及び DPA2018 第 4 編の情報機関による処理は、対象外としている。同ガイダンスは、管理者の説明責任、UK GDPR のデータ保護原則の遵守、ビデオ監視システムの展開後の情報開示などについて述べており、ビデオ監視システムを利用する公共部門及び民間部門が取り組むべき複数のチェックリストを掲載している。

---

[28] Information Commissioner’s Office, Information Commissioner’s Opinion: The use of live facial recognition technology in public places (18 June 2021),
https://ico.org.uk/media/about-the-ico/documents/2619985/ico-opinion-the-use-of-lfr-in-public-places-20210618.pdf

[29] Information Commissioner’s Office, Video Surveillance
https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/cctv-and-video-surveillance/guidance-on-video-surveillance-including-cctv/

エ　顔識別・顔認証技術に関する裁判例

Bridges v. South Wales Police 訴訟は、世界で初めて顔識別技術の違法性を争った訴訟と言われている。争いとなった顔識別技術は大規模イベントや公共施設などに設置され、１秒あたり 50 人の顔を識別して記録し、警察のデータベース内における要注意人物リストとの照合をかけ、照合しないデータは即座に削除されるとされていた。

2020 年 8 月 11 日、イングランド・ウェールズの高等裁判所（Royal Court of Justice）は、要注意リストの登録や装置の設置場所などに関する警察官の裁量が広すぎることなどを理由に、顔識別技術の利用に関する法規制が EU 人権規約 8 条やデータ保護法に反すると判断した（上訴なく確定）。

（４）米国

ア　サンフランシスコを始めとする監視条例における取り扱い

サンフランシスコでは監視技術を網羅的に定義し、その利用に包括的な規制をかける監視条例を制定している。2019 年 6 月 14 日、同条例に顔識別・認証の利用を厳しく制限する規定が設けられた。

顔識別技術について、「個人の顔に基づき個人を特定又は認証することを容易にする自動化又は半自動化されたプロセスをいう」（Sec. 19 B 1）と定義した上、その利用について、一部の例外を除き原則として禁止した（Sec. 19 B 2 (d)）。また例外的に使用する場合にも、監視影響評価や監視技術指針などの手続的な規律に服する。

その後、2020 年中には 18 の自治体が法執行機関による顔識別技術の利用を制限する法規制を制定した。2023 年にはマサチューセッツ州が同様の規制を策定している。

なお、2020 年 6 月にはアメリカ議会でも顔識別技術の利用に制限をかける法案が提出されたが、現時点で制定には至っていない。

イ　民間企業のステートメント

米国の大手テクノロジー企業においても、顔識別技術の開発や利用に関する懸念が数多く表明されている。

例えばマイクロソフトは、2018 年 12 月の声明において、顔識別技術に対する法規制を求め、その中では法執行機関による公共スペースにおける継続監視は、裁判官による令状等の厳格な手続きを必要とするなど厳格な規制が必要であると述べている。

IBM は、2020 年 6 月、アメリカ議会に向けた CEO 名義の書簡において、「IBM は顔識別技術が大量監視、レイシャル・プロファイリングその他の基本的な人権・自由を侵害するために用いられることに強く反対し、容認しない。」と述べ、顔識別技術市場から撤退することを表明した。

2020 年 6 月には Amazon も、顔識別技術の開発や利用について 1 年間の凍結が望ましいと声明を出している。

（5）小括

以上のように、フランス、ドイツ、イギリス及びアメリカの各国では、顔識別・顔認証技術に他の技術とは異なる危険性があることを踏まえ、適切な制御のための法的規律を検討し、あるいは取り組みを実現させている。

おわりに

顔識別・顔認証技術を巡る国内外の動向を整理すると、日本における議論が未成熟であることが浮き彫りとなる。OHCHR が 3 つの報告書で指摘するとおり、顔識別・顔認証技術には大きく 3 つの点で社会を大きく変えるリスクが有る。第 1 に、個々人のプライバシーに対する干渉である。顔識別・顔認証技術は人々が監視されずに日常生活を送る力を弱体化させる。とりわけリアルタイム AI を用いた行動データの取得や移動経路の追跡は、個々人の私的領域を極限まで縮小させることに繋がりかねない。第 2 に、差別の問題である。顔識別・顔認証監視は、既存データベースの人種、民族、性別等の割合に依存するため、その性質上、そのコミュニティにおけるマイノリティが不釣り合いに「識別」や「検証」の対象とされる傾向にある。また AI が従来の差別的な運用を参考に開発され、成長することで、差別的な「分類」が固定化される可能性がある。第 3 に、民主主義との関係である。公共空間における匿名参加の自由は、集会の自由にとって不可欠の要素であるが、法執行機関などが「公共の場所における個人を体系的に同定し、追跡する能力を劇的に高めることで・・表現の自由、平和的集会及び結社の自由、並びに移動の自由に対する直接的な悪影響をもたらすこと」となる[30]。

国際的には、顔識別・顔認証技術が、個人のプライバシー権と衝突するのみならず、表現の自由や差別禁止、全体主義の抑止といった社会全体の重要な理念にとって大きなリスクであることは所与の前提とされている。その上で、適切な利用とのバランスでどのように効果的かつ合理的な規律を及ぼすかにつき、監督機関また

[30] 第 3 の点は、本報告書でも紹介した顔識別に関する EDPB ガイドライン、フランス共和国データ保護機関（CNIL）報告書でも指摘されている。

は民間企業が相次いで提言し、また立法機関が先端的な規律を提示する段階に達している。おおよそのスタンダードも定まりつつある。具体的には、

① 法的根拠、正当な目的、必要性、比例性、及び非差別の原則の要請
② 包括的で一般的なデータプライバシー法の制定
③ 監視システムの設計
④ 中立で独立した監督機関の設立
⑤ 導入に際しての人権デューデリジェンスの実施
⑥ 適切な情報提供、透明性の向上
⑦ ステークホルダーの議論への参加確保
⑧ 効果的な救済制度の創設と被害者のアクセス確保
⑨ これらの措置が整うまで、顔識別・顔認証技術の販売及び使用を停止すること

が最低限の規律として要請されている。

他方で日本では、いまだに網羅的な規律を定立する動きは全く見られない。リスクの評価としても指摘されるものはプライバシーとの衝突が主であり、差別や民主主義との衝突など、社会全体にとって取り返しのつかない状況を引き起こしかねないと言った懸念はほとんど聞かれない。

監督機関である個人情報保護委員会も、懸念される問題点を整理するにとどまり、規律に関する踏み込んだ提言はなされてない。民間企業や各省庁においても、先端技術を実務に利用した成果が羅列されるのみで、国際的に共有される懸念点などに関する問題意識は見られない。国内で具体的かつ網羅的な提言している機関は日弁連ガイドラインにとどまるのが現状である。

当然ながら顔識別・顔認証技術の危険性は普遍的なものである。日本においてのみ他国と比して緩やかな規制を許すことは、日本に住む人々のプライバシーを他国と比較して緩やかに利用することを許容することに繋がるし、日本の民主制度を根底から崩す危険性も生じさせてしまう。技術の進歩は目覚ましいものがあり、拱手する期間が長くなるほど、取り返しがつかない事態が生じるおそれも高くなる。

日本においても、顔識別・顔認証技術の問題点を正面から受け止め、本報告書で整理した最低限の規律を導入することが強く望まれる。

以上