諸外国における顔認識技術の利用と規制の動向

2021年3月23日

(株)国際社会経済研究所　調査研究部
主幹研究員　小泉 雄介
yusuke-koizumi@nec.com

１．顔認識技術の利用動向

顔認識技術の3つの用途

- 近年の顔認識技術の精度向上により、空港、小売店、ホテル、交通機関、オフィスなど様々な場面で、特定個人を識別するために顔認識技術を利用する事例が増えてきている。
- 顔特徴データを用いた顔認識サービス/システムの用途は以下の3つ。

- ①本人同意に基づき個人認証の目的で行われる顔認証サービス
  - Facial Authentication／Facial Verification（顔認証）
  - 多くは1-to-1照合
  - スマホやPCのﾛｸﾞｲﾝ、空港の顔認証ゲート、ﾃｰﾏﾊﾟｰｸの年間パス、顔認証決済、ビル入退館など
- ②容疑者の顔写真と犯罪者DB等の顔画像を捜査目的で照合する顔照合
  - Facial Matching（顔照合）
  - 1-to-many照合
  - 警察機関による利用
- ③公共空間などで（本人同意なく）不特定多数を対象に行われる自動顔認識
  - Automated Facial Recognition（AFR）／Live Facial Recognition（LFR）（自動顔認識）
  - many-to-many照合
  - 警察機関（サーベイランス）や民間企業（万引き犯顔認識、リピート顧客分析等）による利用
- ①と②の用途については法令遵守や社会的受容性の面での課題は少ないが、③の用途については課題が多く、基本的人権の保護と公共の安全の間のバランスを取ることが重要。

顔認識技術の3つの用途（分類方法）

- 顔認識サービス/システムの用途については、以下のような分類軸に沿って分類している。
  - (a)本人同意に基づく利用であるか否か。
  - (b)特定の対象者に対する利用か否か。
- (a)がYesの場合を「①本人同意に基づく利用」、(a)がNoで(b)がYesの場合を「②特定の対象者に対する利用」、(a)がNoで(b)がNoの場合を「③不特定の対象者に対する利用」として、3つの用途に分類。
  - ①本人同意に基づく利用（顔認証）
  - ②特定の対象者に対する利用（容疑者の顔写真の顔照合）
  - ③不特定の対象者に対する利用（公共空間等での自動顔認識）

(a) \ (b)	特定の対象者に対する利用	不特定の対象者に対する利用
本人同意に基づく利用	①	該当なし（※）
本人同意に基づかない利用	②	③

※顔認識の対象者から本人同意を得ている場合、その人を不特定の対象者とは言えないので、「該当なし」。

拙稿「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」（https://www.jstage.jst.go.jp/article/jssmjournal/34/2/34_3/_pdf/-char/ja）もご参照ください。

①本人同意に基づく顔認証

○空港における入国管理（英国）

- ロンドン・ヒースロー空港では、入国審査時に、e-Gateで顔認証を実施。従来は英国、EEAおよびスイス国民のみが対象だったが、2019年5月からオーストラリア、カナダ、日本、ニュージーランド、シンガポール、韓国、米国民に対象者を拡大。（ヒースロー空港のみならず、エジンバラ空港、マンチェスター空港など国内主要空港でも同様。）

○空港保安検査場での生体認証（米国）

- CLEARは、生体認証を用いた認証局ビジネスを行う米国の企業で、2017年時点で75万人の登録会員を持つ。米国の65以上の空港・スタジアムのセキュリティゲート（保安検査場）において、パスポート等を提示することなく、生体認証（指紋、虹彩、顔）での本人確認を実施している。
- 18歳以上が会員になることができ、会費は月額15ドル（年間179ドル）である。その他、デルタスカイクラブ（航空会社ラウンジ）、Hertzレンタカー、スタジアム売店での利用も可能となっている。

①本人同意に基づく顔認証

○小売店での顔認証決済（中国）

- アリペイ（やウィーチャットペイ）は、UX（顧客経験）をさらに向上させるために顔認証決済の導入に力を入れている。
- アリペイは2018年12月に顔認証決済ユニット「蜻蜓（チンティン、ヤンマの意味）」の発売を開始。アリペイ決済に対応しているPOSレジであれば、USB接続をするだけで顔認証決済が可能になる。すでにロータス（スーパー）、華南地区のセブンイレブンなどが導入している。ユニットの販売価格は、1199 元（約 1万 8000円）。1人当たりのレジ処理時間は、QRコード決済の5.6秒から、2.8秒へ短縮された。（FinTech Journalの2019年9月3日記事）

○ギャンブル依存症対策（英国）

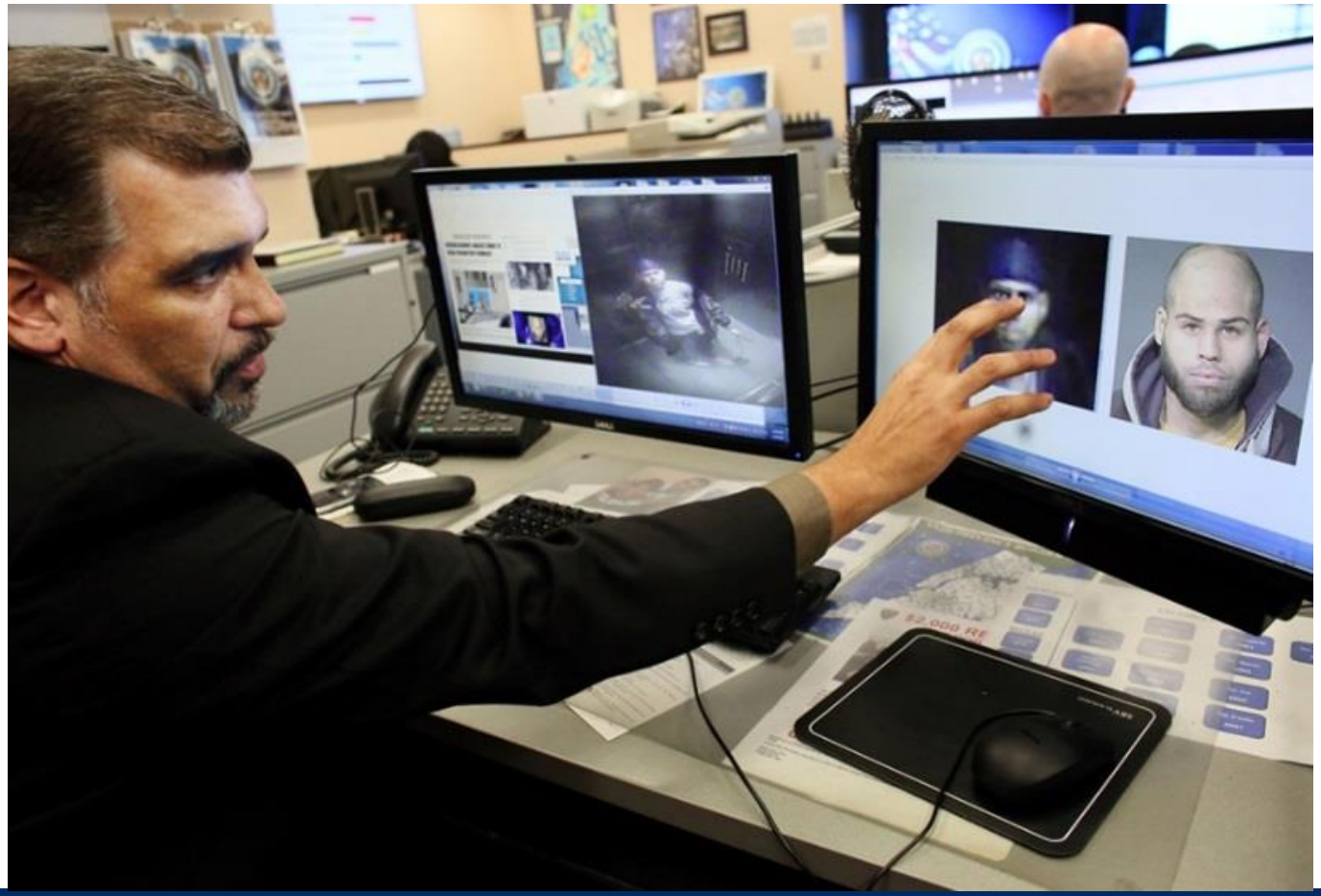
- ロンドンのカジノ（Hippodrome Casino）は、「自己除外リスト」に自ら登録した人（ギャンブル依存症患者）について、4つの入口近くに設置した監視カメラ映像により顔認識を行い、入店拒否をしている。
- 英国ではSENSE（Self-Enrolment National Self-Exclusion：全英自己除外自己登録）という制度が2015年8月に立ち上げられており、1万人以上が既に登録しているという。

①本人同意に基づく顔認証：学校における出欠管理（スウェーデン）

- スウェーデンの学校での顔認識実証実験に対する制裁金
- スウェーデンのデータ保護監督機関（DPA）は2019年8月22日、学校において生徒の出欠をモニターする目的で顔認識技術を用いたとして、ある自治体に20万スウェーデン・クローナ（約2万ユーロ、約218万円）の制裁金を科した 。
- スウェーデン北部のある学校は、生徒が学校に出席していることを追跡し続ける目的で顔認証を用いる実証実験を実施した。この実証実験は限られた時間に1つのクラスで実施された。
- スウェーデンDPAは、この実証実験がGDPRのいくつかの条項に違反しており、当該自治体に約2万ユーロの制裁金を科すことを決めた。スウェーデンの公共機関に科しうる制裁金の最大額は1000万スウェーデン・クローナ（約100万ユーロ）である。本件はGDPRの下でスウェーデンDPAが初めて科した制裁金事例である。
- この学校はセンシティブな生体データを違法に処理しており、十分な個人データ影響評価やスウェーデンDPAとの事前協議の検討を行っていなかった。
- この学校はこれらの生体データを同意に基づいて処理していたが、スウェーデンDPAはデータ主体（生徒）と管理者（学校）との間の（権力の）明確な不均衡に鑑みて、この同意が有効な適法性の基盤ではないとみなしている。
- （出典：https://edpb.europa.eu/news/national-news/2019/facial-recognition-school-renders-swedens-first-gdpr-fine_en）

②容疑者写真の顔照合： ニューヨーク市警察（米国）

- ニューヨーク市警察（NYPD）の顔識別ユニット（Facial Identification Section）
  - 犯罪捜査を行なう刑事から容疑者の写真を受け取り、顔照合ソフトウェアにかけ、さらに同ユニットの担当者が目視およびバックグラウンドチェックで候補者を絞り込む。
  - 2015年までに1700人の容疑者を特定、900人を逮捕。誤照合は5人のみ。



（写真の出典：http://discovermagazine.com/2015/dec/12-face-time）

②容疑者写真の顔照合： Clearview AI（米国）

- 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している。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・銀行などが利用しているという。
- 英国情報コミッショナーオフィス（ICO）とオーストラリア情報コミッショナー事務局（OAIC）は2020年7月に合同でClearview AIに対する調査を開始した。カナダのプライバシーコミッショナー事務所（OPC）も調査を開始し、7月に王立カナダ騎馬警察（RCMP）などカナダの全ての法執行機関が同社との契約を停止している。
- TwitterやGoogle、YouTube、Venmo、LinkedInなどの企業は相次いでClearview AIにデータの使用停止を求める通告書を送っている。民間企業による本人同意のない生体識別子の取得を禁じる生体情報プライバシー法（BIPA）のあるイリノイ州では、2020年1月に地方裁判所で同社が州民から訴訟を起こされている 。5月には米国の人権団体ACLU等からもイリノイ州のBIPAに違反したとして同州で訴訟を起こされている。ただし、同社は2020年8月に米国のICE（移民・関税執行局）と新たな契約を結んだという。
- EDPB（欧州データ保護会議）も、EU加盟国の政府機関による利用は問題があるとしている。
- （ニュースソース）
  - https://japan.cnet.com/article/35148187/ ・https://forbesjapan.com/articles/detail/35768
  - https://gigazine.net/news/20200707-clearview-ai-end-in-canada/
  - https://gigazine.net/news/20200207-clearview-ai-google-youtube-venmo-linkedin/
  - https://japan.cnet.com/article/35148516/ ・https://www.aclu.org/press-releases/aclu-sues-clearview-ai
  - https://jp.techcrunch.com/2020/08/15/2020-08-14-clearview-ai-ice-hsi-contract-2020/
  - https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_letter_out_2020-0052_facialrecognition.pdf

【ご参考】 米国顔認識ベンダーClearview AIに対するEDPB意見

- 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。
（https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_letter_out_2020-0052_facialrecognition.pdf）
- 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。

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

- 「EDPBは、EU警察・刑事司法データ保護指令（EU）2016/680に基づいて、EU内の法執行機関が同指令第8条と第10条の厳格な条件に従ってのみ自然人を一意に識別する目的で生体データを処理できることに留意する。第8条によれば、そのような処理は、指令が適用される目的の下で、EU法または加盟国法に基づく業務の遂行に必要な範囲でのみ実行できる。また、それはEU基本権憲章や欧州人権条約を遵守するものでなければならない。第10条ではそのような処理は、とりわけ、厳密に必要であり、データ主体の権利と自由に対する適切な保護措置に服することが必要とされている。これらの厳格な条件に従って、EU内の法執行機関は、特定の状況下で、写真から得られた生体テンプレート（特徴データ）を含む生体データを処理し、公的機関の管理下にあり、EU法または加盟国法の下で構築されたデータベース内の生体テンプレートと照合を行うことが許される。
- しかし、法執行機関がClearview AIから提供されるようなサービスを利用することは、警察または犯罪捜査の一環として、個人データをEU域外の民間企業と共有することや、そのような民間企業の大規模で恣意的に構築されたオンラインアクセス可能な顔画像のデータベースに対して生体データの照合を行うことを意味するという点で、根本的に異なるものである。
- EDPBは、EU法または加盟国法がClearview AIから提供されるようなサービスを利用するための法的根拠を提供するかどうかについて疑問を持っている。したがって、現状のままで、将来の調査または保留中の調査を害することなく、EU内の法執行機関によるそのような利用の適法性を確証することはできない。」

【ご参考】 米国顔認識ベンダーClearview AIに対するEDPB意見

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と比例性の要件を満たさない

- 「次にEDPBは、大量の個人データを何らの制限もなく、あるいはデータ間の正確な結合を行わずに、無差別に収集して構築されたデータベースに依存するような法執行コンテキストでの個人データの処理とその目的は、指令における厳密な必要性の要件を満たさない可能性が高いと考える。この比例性の原則の遵守に関して、EUレベルの私生活を尊重する基本権の保護は、欧州司法裁判所の判例に従い、厳密に必要な場合に限って個人データ保護の例外と制限を適用すべきであることを求めるものである。」

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

- 「最後にEDPBは、EU内の法執行機関が、Clearview AIなどのEU域外の拠点で活動を行うデータ管理者によって利用可能とされたアプリケーションを利用することは、EUから米国（同社の拠点がある国）への個人データの移転（例えば顔認識サービスを利用してアイデンティティが確認される人物の個人データの移転）を構成しうることに留意する。EDPBは特に、当該個人データの移転は、EU-USプライバシーシールド十分性決定の規定や、EU-USアンブレラ協定の対象とならないことに留意する。そのような移転が適法であるためには、EU内の法執行機関から第三国の民間企業への移転を具体的に規定する、EU警察・刑事司法データ保護指令第39条に定められた厳格な条件と要件を遵守しなければならないだろう。」

③自動顔認識： 警察による自動顔認識の実証実験（英国）

- ロンドン警視庁は、「ノッティングヒルカーニバル」や「ウェストミンスター地区」など、公共イベントや混雑した場所において、LFRの実証実験を2016年～19年に10回実施。
- 他にも、レスターシャー警察（音楽コンサート）、南ウェールズ警察（サッカーの試合）などが実証実験を実施。

写真の出典：ロンドン警視庁ホームページ

③自動顔認識： 警察による自動顔認識の実証実験（英国）

時期	実施主体	実施イベント	顔照合データベースの内容
2015年6月	レスターシャー警察	屋外音楽イベント（ロックフェスティバル）	レスターシャー警察の拘留者DB、およびユーロポールから得た国際犯の顔写真DB
2016年8月	ロンドン警視庁	ノッティングヒル・カーニバル	カーニバルへの参加を禁じられた人や、犯罪を行うためにカーニバルに参加する可能性があるとして警察が指定した人（組織犯罪者等）
2017年6月	南ウェールズ警察	欧州サッカー連盟チャンピオンズリーグの決勝戦（南ウェールズのカーディフ）	組織犯罪者・違法チケット販売者・フーリガンなどのDB（スタジアムのみならずカーディフ市内全域で顔照合）
2018年	グレーターマンチェスター警察	グレーターマンチェスターのショッピングセンター →監督機関によって中止	30人の容疑者や行方不明者の顔写真データ

③自動顔認識： 警察による自動顔認識の実証実験（英国）

時期	実施主体	実施場所	実験結果
2018年7月	ロンドン警視庁	Westfieldショッピングセンター	データベース件数：306 アラート発生数：1 逮捕者数：0
2018年12月	ロンドン警視庁	Westminster	データベース件数：2226 アラート発生数：5 逮捕者数：2
2019年1月	ロンドン警視庁	Romford High Street	データベース件数：2500 アラート発生数：10 逮捕者数：2
2019年2月	南ウェールズ警察	カーディフのCity Centre	データベース件数：830 アラート発生数：12 逮捕者数：3

③自動顔認識： 警察による自動顔認識の実運用（英国）

- ロンドン警視庁は、ロンドン市内各地での10回に渡る実証実験や、実証実験に対する評価、自動顔認識ガイダンス文書の作成等を行った後、2020年2月からロンドン市内（オックスフォードサーカス、ストラトフォード等）で自動顔認識システムの実運用を開始している。
- 実運用に当たっての措置
  - LFRのデプロイに先立ち、どこで実施するのか、オンラインで人々に告知する。
  - 全てのデプロイメントの結果について、ウェブサイトで公表する。
  - 情報リーフレットを人々に配布する。
  - 当該エリア内および周辺にポスターや掲示板を設置して、人々が顔認識技術の利用について認識できるようにする。
  - 何が行われておりLFRがどのように動作するかについて、警察官が人々に説明できるようにする。
- LFR利用の根拠となる法令
  - Common law（コモンロー、慣習法）
  - Data Protection Act 2018（2018年データ保護法）
  - Protection of Freedoms Act 2012（2012年自由保護法）
  - ・Human Rights Act 1998
  - ・Equality Act 2010（2010年平等法）
  - ・Freedom of Information Act 2000
- ロンドン警察倫理パネル（LPEP）はLFR技術に関する報告書 （2019年5月）で、法執行機関によってLFRが「倫理的に」利用されるために必要とされる以下の5つの条件を設定している。
  1. LFRにベネフィットがあることを証明することのニーズ
  2. 実証実験のデータを公表することで信頼を構築すること
  3. 必要性と比例性
  4. オペレーターや警察官に対するトレーニング
  5. 独立的な監視を伴う堅固な自主規制
- ロンドン警視庁は2020年1月23日に同報告書に対する回答書を公表し、これら5つの条件に対応できている旨を説明している。

③自動顔認識： 警察による自動顔認識の利用計画（ドイツ）

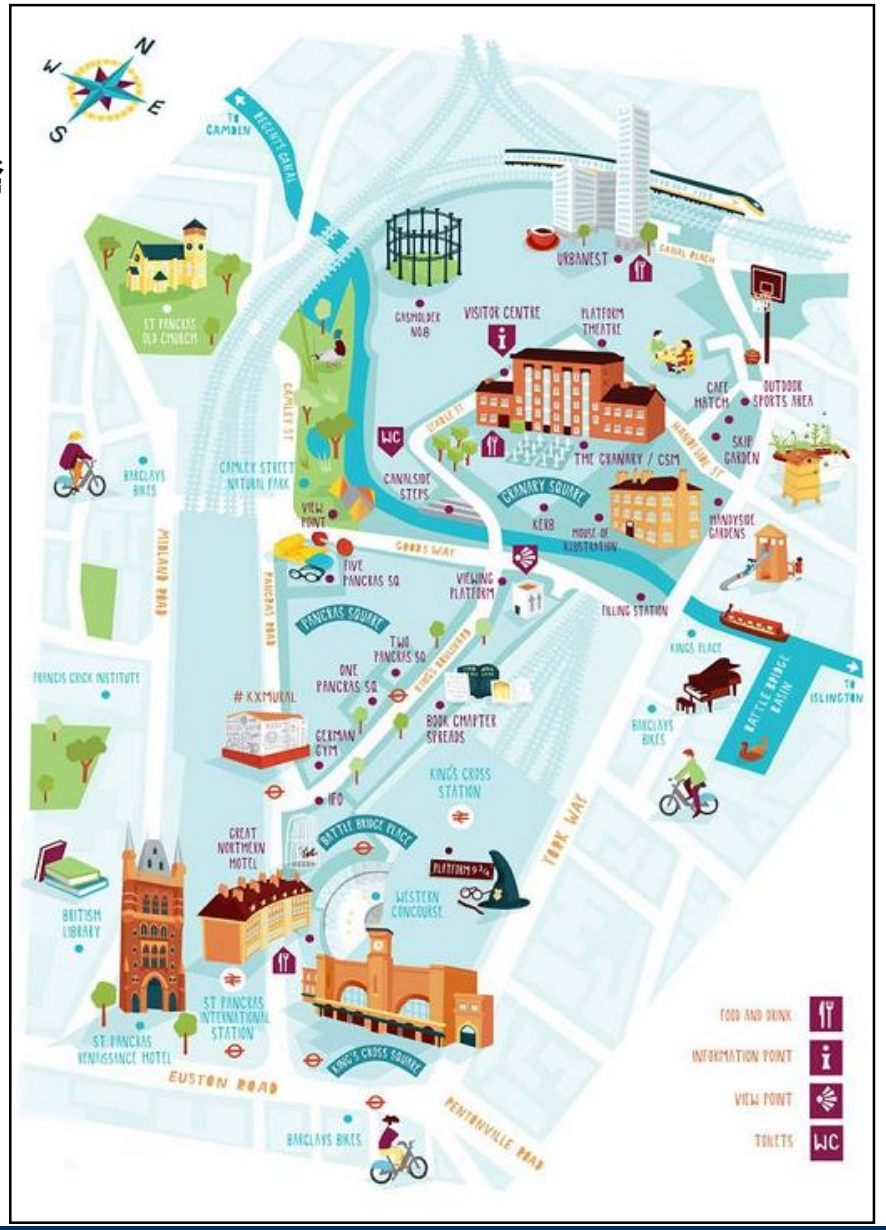
- ドイツのゼーホーファー内務大臣は国内134の鉄道駅と14の空港での自動顔認識の利用を計画中。。
- 内務省は公式に当該措置を公表していないが、政府のスポークスマンは、EURACTIVから尋ねられ、警察に「改善された技術的可能性、また可能かつ合理的な場合は拡大された責任」を提供するために連邦警察法の改正が計画されていると述べた。
- 社会民主党（SPD）のリーダーであるSaskia Esken氏は同年1月4日に「私の意見では、顔認識を伴うビデオ監視は自由の権利に対する過度の干渉である。偽陽性のアラームは、監視よりもセキュリティに大きな損害を与える。罪のない人々が標的にされる。私は、社会のデジタル化を民主化したい」とTwitterで警告している。
- ゼーホーファー内務大臣は2018年のベルリンのズードクロイツ駅でのテストの後、顔認識システムが「警察の仕事をさらに効率的にし、市民の安全を向上させる」という見方を示した。

（出典：EURACTIV 2020年1月10日記事）

③自動顔認識： 民間による自動顔認識の実証実験（英国）

- キングスクロス再開発地
  - ロンドンのキングスクロス駅前の東京ドーム6個分の広さ（27万平方メートル）の再開発地。
  - 敷地内に240台のカメラがあり、不動産会社が保有。CCTV室で集中管理。

- 自動顔認識の実証実験
  - 自動顔認識のトライアルを実施（2016年～18年）。
    - 警察から犯罪者や行方不明者の顔写真を含む人物データを受領。
  - 欧州の公共空間で初めての「常時」リアルタイム顔認識とのこと。



図の出典：www.kingscross.co.uk

２．顔認識技術に対する懸念

顔認識技術に対する懸念

- ①本人同意に基づき個人認証の目的で行われる顔認証サービス
  → 懸念・批判は少ない （本人が同意した上でのデータ利用であるため）
  - ただし、以下はNG （EUや英国）。
    - 脆弱な立場の個人（生徒、従業員等）への同意強制
    - 空港ゲートなどで顔認証に同意していない旅客の映り込み

  → 顔認証以外の選択肢の提供が必要

- ②容疑者の顔写真と犯罪者DB等の顔画像を捜査目的で照合する顔照合
  → 懸念・批判は少ない （犯罪と無関係の一般市民の権利を侵害しないため）
  - ただし、以下の批判は有り。
    - 照合するDBの内容の正確性
      （英国警察の拘留者DBには釈放者の写真も残存、Cleanview AI）
    - DBの目的外利用
      （米国FBIが各州の運転免許DBを参照、Cleanview AI）
    - 顔照合ソフトウェアの品質 （人種・性別的バイアス）

- ③公共空間などで（本人同意なく）不特定多数を対象に行われる自動顔認識
  → 懸念・批判が大きい

顔認識技術に対する懸念：　①本人同意に基づく顔認証

- 空港ゲートでの顔認証や店舗での決済時の顔認証、イベント会場入場時の顔認証などは、顔特徴データを取得・利用される本人が同意した上でのデータ利用であるため、これに対するプライバシー等の立場からの懸念や批判は少ない（※）。利用者に顔認証以外の選択肢も提供されている限り、もし顔のデータを取得されることが嫌であれば顔認証を利用しなければよいことから、社会的受容性の面で①の用途に特段の問題ないと考えられる。
- 日米欧の個人情報保護法令上も基本的には問題ない。ただしEUや英国においては、スウェーデンの制裁金事例に見られるように、データ管理者が脆弱な立場の個人（生徒、従業員等）に同意を強制することのないように顔認証以外の方法を提供したり、またGDPR（欧州一般データ保護規則）のビデオ機器個人データ処理ガイドラインで規定されているように、空港ゲートなどで顔認証を利用したくない（顔認証に同意していない）旅客が写り込まないように顔認証以外のゲートを用意するといった対応が、EUの法令上、データ管理者に求められる。

- ※：2019年11月に当社で実施した英国の情報コミッショナーオフィス（ICO）へのヒアリングによれば、①の用途は③など本人同意のない用途に比べリスクが低いが、「生体データの保持期間」「顔認識ソフトウェアの精度」「本人同意撤回時の代替手段」などは課題になるという。

顔認識技術に対する懸念：　②容疑者写真の顔照合

- 既に米国や英国、ドイツ等の警察において10年弱の利用実績がある。あくまで犯行現場等で取得された「容疑者」の顔写真に対する顔照合であり、犯罪と無関係の一般市民の権利を侵害するものではない。また前述のニューヨーク市警察の事例など、顔照合に当たっては担当者による目視確認やバックグラウンドチェックが併せて行われており、これらの結果、容疑者の顔写真とDB上の人物とが一致したとしても、直ちに当該人物が逮捕される訳ではなく捜査のきっかけになるにすぎない。
- この用途にも、いくつかの懸念は寄せられているが、いずれも「容疑者写真の顔照合」そのものに対する本質的な懸念ではなく、「照合するデータベースの内容の正確性」や「データベースの目的外利用」、「顔認識ソフトウェアの精度・品質」といった副次的な事項に対する懸念となっている。

- 例：　前述のCleanview AIでも、問題視されているのは、同社が「SNSサイト上の顔画像を本人同意なく目的外利用」している点や、法執行機関がそのような「無差別かつ不正確なデータベースを顔照合に利用」している点である。

顔認識技術に対する懸念：　③自動顔認識

- 顔認識技術に対する批判は③の用途に集中している 。主な懸念・批判は、以下の5点にまとめることができる。

（１）顔画像の取得の容易さ
- 監視カメラや顔認識技術は、他の技術に比べて容易に個人情報を取得できる。

（２）透明性の欠如
- 個人は撮影されていることに気付いたとしても、裏でデータベースと照合されているとは思わない。

（３）行動の自由の萎縮効果
- 個人は絶え間なく監視されていると感じることで、行動を抑制するようになる。

（４）顔認識技術の精度
- 自動顔認識を行う環境によっては、誤照合率（偽陽性率）が高いケースがある。

（５）顔認識技術におけるバイアス
- ソフトウェアによっては、人種・性別・年代的なバイアスが顕著なケースがある。

顔認識技術に対する懸念：　③自動顔認識

（３）行動の自由の萎縮効果　に関する懸念・批判の例

- 「政府による顔認識の利用は、民主主義の自由と人権を侵害する可能性がある。人々が自由に集まり、意見を交換することによってこそ民主主義は成立する。顔認識の活用には人々の自由にリスクをもたらしうるものもある。政府は顔認識を利用して、特定個人の長期的監視を行うことができる。」（Microsoftの最高法務責任者）
  （https://news.microsoft.com/ja-jp/2018/12/13/blog-facial-recognition-its-time-for-action/）
- 「法を遵守している市民さえも、追跡される恐れなくして、結社の自由（交際の自由）や移動の自由、言論の自由を行使することができなくなる。」（米国の哲学教授および法学教授）
  （https://www.nytimes.com/2019/10/17/opinion/facial-recognition-ban.html）
- 「公共の監視には萎縮効果がある。絶え間ない監視により、人々は行動を適応させることを強いられる。これに民主主義にとって不健康なことである。なぜなら、市民は自分の顔が顔認識データベースに保存されていることを知ったならば、政治的な参加を避けてしまうかもしれない。」（ドイツの人権団体）
  （https://www.euractiv.com/section/data-protection/news/german-ministers-plan-to-expand-automatic-facial-recognition-meets-fierce-criticism/）

顔認識技術に対する懸念：　③自動顔認識

（５）顔認識技術におけるバイアス　に関する米国NISTの報告書

- **NIST（米国国立標準技術研究所）は2019年12月19日に「Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects」という報告書を公表。**
  （https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software）
- **同報告書では189の顔認識ソフトウェアについて、それらが様々な性別・年齢・人種の人々をどの程度正確に識別するかの調査が行われた。顔識別の正確性は各々のソフトウェアが用いているアルゴリズム、それが利用されるアプリケーション、入力データに依存するが、大部分のソフトウェアは性別・年齢・人種によって異なる正確性を示した。**
- **NEC、パナソニック、Idemia、Gemalt Cogent、Microsoft等を含む。なお、Amazon、Apple、Facebook、Google（GAFAの4社）は対象外。**
  - これら4社は自社のアルゴリズムを提出しなかったという。（https://www.chicagotribune.com/consumer-reviews/sns-facial-recognition-bias-20191226-cldfnnmqbzf6lp5w622jnw7oga-story.html）
- **各ソフトウェアは下記2つのタスクについて、偽陽性（別の人物を同一と判断する）のエラーと偽陰性（同一人物を別の人物を判断する）のエラーが生じる確率が調べられた。**
  - 1-to-1 matching（1対1照合）：ある顔写真がデータベース内の同じ人物の別の顔写真と一致することを確認。スマートフォンのロック解除やパスポートの確認など、個人認証（verification）の用途で使われる。
  - 1-to-many matching（1対多照合）：ある顔写真の人物がデータベースで一致するかどうかを判断する。関心ある人物の識別（identification）のために用いられる。

顔認識技術に対する懸念：　③自動顔認識

（５）顔認識技術におけるバイアス　に関する米国NISTの報告書（続き）

- 国務省、国土安全保障省、FBIの運用データベースを情報源とする849万人の1827万枚の画像が使われた。データベースの画像には、当該人物の年齢・性別・人種（または出生国）に関するメタデータが含まれていた。
- 全体的な傾向としては以下の5つの傾向が見られた 。
- 1対1照合では、白色人種と比較して、アジア系およびアフリカ系アメリカ人の顔の偽陽性率が高かった。この差は、各アルゴリズムに応じて、しばしば10倍から100倍の範囲にも上った。偽陽性は、身元詐称者のアクセスを許可する可能性があるため、システム所有者にセキュリティ上の懸念を提示するおそれがある。
- 米国で開発されたアルゴリズムの共通傾向として、アジア人、アフリカ系アメリカ人、ネイティブグループ（ネイティブアメリカン、アメリカンインディアン、アラスカインディアン、太平洋諸島系住民を含む）の1対1照合で偽陽性率が高かった。アメリカインディアンは、偽陽性率が最も高かった。
- ただし、注目すべき例外はアジア諸国で開発された幾つかのアルゴリズムである。アジアで開発されたアルゴリズムでは、アジア人と白人の間で、1対1照合の偽陽性率にそのような劇的な違いはなかった。考えられる可能性は、アルゴリズムのパフォーマンスと学習用データの関係である。これらの結果は、より多様な学習用データがより公平な結果を生む可能性があるという兆候である。
- 1対多照合では、アフリカ系アメリカ人女性の偽陽性率が高かった。1対多照合における偽陽性率の差は、結果として誤った告発を導くおそれがあるため、特に重要である。
- ただし、すべてのアルゴリズムが1対多照合で偽陽性率（のバラつき）が高いわけではなく、最も公平なアルゴリズムは最も正確なものの中にランク付けされている。この最後のポイントは、レポートの全体的なメッセージの1つを強調するものである。すなわち、異なるアルゴリズムは異なるパフォーマンスを示す。

顔認識技術に対する懸念：　③自動顔認識（英国）

- 南ウェールズ警察は、2017年5月から2019年4月に大規模公共イベント（チャンピオンズリーグ決勝戦など）の際に警察車両やサッカー場などに設置した監視カメラで、自動顔認識を行っていた。
- これに対し、住民のEdward Bridges氏が訴訟。プライバシー団体Libertyがサポート。
- 南ウェールズ警察の自動顔認識に対する訴訟の第一審（高等法院、2019年9月）
  - 第一審は合法との判決。同年11月に控訴された。
  - 監視カメラコミッショナー（SCC）は同判決に対し、「警察側がこの判決を自動顔認識（AFR）の一般的な展開に対するゴーサインと見なすことには注意を求める。AFRは、人権や国民の信頼に対する影響を伴う侵害的なツールである」という声明を公表。2020年12月には新たなガイダンスを公表。
  - 情報コミッショナー・オフィス（ICO）は2019年10月に、警察による公共空間でのLFR（AFR）利用にする調査報告書、および意見書を公表。南ウェールズ警察による「厳密な必要性」と「比例性」の正当化が十分でないと指摘。
- 南ウェールズ警察自動顔認識に対する訴訟の第二審（控訴院、2020年8月11日）
  - 以下3つの理由で、違法判決。
    - どこでAFRが使用され、誰がウォッチリストに入るのか明確な条件が定められていない。
    - 英国データ保護法に則ったデータ保護影響評価が不十分である。
    - 英国の平等法に則り、顔認識ソフトウェアに人種・性別バイアスがあるか否か確認する合理的措置を取っていない。
  - ただし南ウェールズ警察は、同判決によってAFRを使用できる条件が明確化されたとして、控訴せず。

【ご参考】 英国ICOのライブ顔認識（LFR）に対する意見書

○「情報コミッショナーの意見：公共空間における法執行機関によるライブ顔認識技術の利用（Information Commissioner's Opinion: The use of live facial recognition technology by law enforcement in public places）」（2019年10月31日）

○サマリー

- コミッショナーは以前、ライブ顔認識（LFR）の比例的でない利用によって生じる個人の権利と自由へのリスク、個人の日常生活への不必要な侵入、警察の不当な介入等の潜在的な不利益に関する見解を表明した。また、コミッショナーはブログにおいて、そのような生体データの処理に対しデータ保護法令がいかに適用されるかについて述べた。
- 本意見書の目的は、法執行機関が公共空間で顔認識技術をデプロイする際の個人データ処理に関して、法執行機関をガイドすること。
- 本意見書の主たるメッセージは以下。
  - LFRの利用は、個人データの処理を伴うため、データ保護法（DPA）が適用される。これは、実証実験であろうと、日常的な運用であろうと同様である。
  - 「所管官庁」による「法執行目的」での個人データ処理は、DPA第3部によってカバーされる。
  - とりわけ、法執行目的でのLFRの利用は、個人をユニークに識別する目的での生体データの処理を伴うため、「センシティブな処理」（DPA第35条（8）b）を構成する。
  - そのようなセンシティブな処理は、LFRソフトウェアによって取得され分析された全ての顔画像に関係するものであり、DPA第35条、42条、64条の要件にとりわけ注意を払わなければならない。そのため、「データ保護影響評価（DPIA）」（第64条）や「適切なポリシー文書」（第42条）が実施されなければならない。

【ご参考】 英国ICOのライブ顔認識（LFR）に対する意見書

○サマリー（続き）

- センシティブな処理は、当該画像がウォッチリスト上の人物とマッチングしたか、それともマッチングしなかった人物の生体データが短時間で削除されたかに関わらず、発生している。
- データ保護法は、デプロイメントの必要性や比例性の検討から、ウォッチリストの編集、生体データの処理、生体データの保持や削除まで、LFRのプロセス全体に適用される。
- 管理者は、LFRの利用の適法性の基盤（DPA第35条）を識別しなければならない。適法性の基盤は、行動規範のような他の利用可能な法的文書とともに、識別され、適切に適用されるべき。
- コミッショナーは、政府によって発行される、法令に基づく拘束的な行動規範（statutory and binding code of practice）によって、法的フレームワークを強化するという見解のもと、関連する機関と協働することを目指している。コミッショナーの見解では、そのような行動規範は、監視カメラ行動規範（2012年自由保護法の下で発行されたもの）で設定された基準の上に構築され、データ保護法制と整合的なものとなるだろうが、LFRや他のバイオメトリック技術の法執行目的での利用に明確で特別な焦点を当てたものになるだろう。それは、現行や将来的なバイオメトリック技術に適用可能なものであることを保証するように開発されるべきである。
- コミッショナーは、警察やその他の法執行機関が、南ウェールズ警察に対する高等裁判所判決で規定された義務を遵守するために、DPA第42条を遵守するために何が必要かについてどう裁判所が提供した勧告を考慮しながら、何が必要とされるかの詳細なガイダンスを提供することを目指している。

【ご参考】 英国ICOのライブ顔認識（LFR）に対する意見書

○「厳密な必要性」の基準

- データ保護法第35条（５）(a)「当該処理が法執行目的で厳密で必要とされる場合」の「厳密に必要とされる」の基準は何か。（→前述p.9参照）
- 管理者は各々のデータ処理とそのメリットについて注意深く検討し文書化する必要がある。コミッショナーは、管理者がDPIAや適切なポリシー文書を含め、なぜ法執行目的でのLFRを通じたセンシティブな処理が「厳密な必要性」の基準を満たしているかを明確に説明することを期待する。この基準を満たすためには、管理者はセンシティブな処理の「比例性」と、LFRの代替手段とを検討しなければならない。
- LFRがデプロイされる目的は、重要性の高いものであるべきである。一般的に、LFRを特定の重大犯罪や暴力犯罪を軽減する目的で利用することと、既知の万引き犯を識別する目的でLFRを利用することの間には、かなりの違いがある。軽罪の中にはより重大な犯罪や組織犯罪の一部であるものが含まれうることは認めるが、各ケースでそのメリットについて検討されなければならない。
- LFRが狭く定義された目的のために、ターゲット化されて、または小規模にデプロイされる場合には、厳密な必要性や比例性の要件を満たす可能性が高い。一例として、容疑者が特定の場所に特定の時間にいる可能性が高いことを示すインテリジェンス（情報）を警察が持っている場合である。他の例として、LFRが、空港などで、所轄官庁によって法執行目的で実施されるセキュリティ措置の一環である場合である。
- 換言すると、LFRのデプロイメントが以下である場合は、センシティブな処理であることを正当化することのハードルはより低いだろう。
  - （対象者が）ターゲット化されている
  - インテリジェンスに基づいている
  - 時間が限定されている

【ご参考】 英国ICOのライブ顔認識（LFR）に対する意見書

○「厳密な必要性」の基準（続き）

- また、他のより侵害的でない選択肢の利用可能性がある場合、管理者はなぜLFRという侵害的な手段の利用が厳密に必要であるかを明確に説明できなければならない。
- ICOは、南ウェールズ警察による「厳密な必要性」と「比例性」の正当化が以下の点で十分でないと考えている。
  - なぜ目的を達成するためにより侵害的でない手段が考慮されていないかが十分に説明されていない。
  - LFRの利用のターゲット化が十分に保証されていない。
  - LFRを実施する場所の選択が特定の要因や合理的な疑いによって正当化されていることが十分に保証されていない。
- そのため、ICOは、センシティブな処理の厳密な必要性と、個人の権利の間の公正なバランスを両立させることを、SWPは保証していないとの見解である。

○行動規範の導入

- コミッショナーは、LFRのようなバイオメトリック技術の利用によって生じる特定の問題に対処するためのさらなる保護措置を提供する、法令に基づく拘束的な行動規範（statutory and binding code of practice）を早期に導入することを政府に要求する。これは、データ保護法令を遵守しながら、どのように、いつ公共空間においてLFRを利用してよいかについて、法執行機関にさらなる情報提供を行うものである。これは、LFRの利用が比例的であり、必要であり、ターゲット化されていることを保証し、データ保護・プライバシー・人権に関する法令への遵守を保証するような監督を可能とする。

顔認識技術に対する懸念：　③自動顔認識（米国）

- 2019年以降、連邦・州・市のそれぞれのレベルで、顔認識技術の利用を規制する法案の作成が活発化している。この背景には、以下の要因がある。
  - 顔認識技術のサーベイランス利用に歯止めをかけたい市民団体（特にACLU）による積極的なロビー活動
  - Microsoftによる連邦政府などへの顔認識を規制する法律制定の呼びかけ
  - MITによる顔認識アルゴリズムの実験結果（白人男性の性別認識率は高いが、有色人種女性の性別認識率は低い）の公表
- ACLU（全米市民自由連合）の活動
  - Amazonは顔認識システム「Rekognition」を地方警察に販売しているが、ACLU等の市民団体は2018年5月、2つの警察（フロリダ州オーランド、オレゴン州ワシントン郡）がRekognitionをボディカメラと地域監視で用いたことに関して異議申立てを行なった。
  - 訴えでは、同システムはリアルタイムの市民監視を可能にし、学習用データが白人に偏っているため黒人などのマイノリティに不利に機能するとして、同システムの販売を停止するように要求。
  - また2018年7月には、AmazonのRekognitionについて、連邦議員全員の顔データを入れて、初期設定の正確性80%で犯罪者の顔写真DBと照合する実験を行った。議員535人のうち28人がマッチングする結果となった。

顔認識技術に対する懸念：　③自動顔認識（日本）

○大阪駅ビルにおける顔認識技術の実証実験

- 情報通信研究機構（NICT）は2014年4月から2年間、大阪ステーションシティにおいて、映像センサー（90台のカメラ）から施設内の状況を映像データとして取得し、通行人の顔映像を顔特徴データに処理した後、顔特徴データで行動を追跡することにより、シティ内の人の流量や滞留の度合い等を把握し、災害発生時の安全対策等への利用可能性を検証する実証実験を計画していた。
- しかし、新聞報道後に「勝手に顔を撮ってほしくない」といった市民からの抗議が寄せられたため、4月開始は事実上断念することになったという。（毎日新聞2014年3月6日記事より）

○万引犯顔照合システム

- 来店客の顔特徴データに対して、「万引犯」「盗撮犯」といったフラグを立てて登録し、次回来店時に照合した場合に警備員のスマホにアラートを送ることが可能な防犯カメラ・顔認識システム。大手書店チェーン、ドラッグストアチェーン、百貨店等で導入が進む。
- 「特定の個人を追跡する機能をもつ顔認識システムの方が肖像権やプライバシー侵害の度合いが強く、（単なる防犯カメラと万引犯顔照合システムの）両者は区別する必要がある」と森亮二弁護士は指摘。（読売新聞2015年12月29日記事）

○札幌市の実証実験（2017年3月）

- 札幌駅前地下通路での実証実験に先立ち、マスコミの「顔認証実証実験」との誤認報道により、市民からの問合せが市に殺到。その結果、カメラ使用を中止。（属性推定のみの利用をするつもりだったが、自動顔認識するものと誤認された）

３．顔認識技術に対する規制の動向

EU：GDPRにおける顔認識データの扱い

- GDPR（一般データ保護規則）では、顔特徴データを含む生体データは、「特別な種類の個人データ」（センシティブデータ）として特別な保護が必要。

	GDPR（EU一般データ保護規則）（2016年制定）	（参考）EUデータ保護指令（1995年制定）
生体データ（顔特徴データを含む）の扱い	特別な種類の個人データ（GDPR第9条） （「自然人を一意に識別することを目的とする生体データ」が、これに含まれる）	通常の個人データ
生体データの処理の適法性の基準	（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	（EU指令第7条） ・データ主体の同意 ・契約の履行 ・法的義務の遵守 ・データ主体の生命に関する利益の保護 ・公共の利益/公的権限の行使における職務遂行 ・管理者等の正当な利益
生体データ処理に関する追加的規定	・加盟国は、生体データの処理に関し、その制限を含め、付加的な条件を維持または導入できる（GDPR第9条4項）	特になし
備考	自然人を一意に識別することを目的とする顔特徴データ（facial template）のみが上記「特別な種類の個人データ」（GDPR第9条）に相当する。単なる顔写真（個人データ）や、属性推定用の加工データは、これに相当しないと考えられる	―

EU：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

- EUの個人データ保護に関する諮問委員会であるEDPB（欧州データ保護会議）は2019年7月10日に、「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（Guidelines 3/2019 on processing of personal data through video devices）」案を公表し、パブコメ後、2020年1月29日に正式版を公表。
- これはGDPR（EU一般データ保護規則）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であり、事業者の立場から見ると非常に厳しい内容の規制も含まれている。
- EDPBが発行する指針はGDPRの法解釈を示すもので、EU各国の監督機関がGDPRの執行を行う際の根拠となる。（EDPBはEU各国の監督機関から構成。）
- 同ガイドライン案に対しては、JEITAやDigitalEuropeがパブコメ意見を提出したが、正式版では補足的な説明の追加、「てにをは」の修正などのマイナーな変更がなされたのみであり、基本的な内容は変更されていない。
- 同ガイドラインの構成
  - 1. はじめに
  - 2. 適用範囲
  - 3. 処理の適法性
  - 4. 第三者へのビデオ映像の提供
  - 5. 特別な種類のデータの処理
    - 5.1 生体データを処理する際の一般的留意事項
    - 5.2 生体データを処理する際にリスクを最小化するための推奨措置
  - 6. データ主体の諸権利
  - 7. 透明性と情報提供の義務
  - 8. 保存期間と消去の義務
  - 9. 技術的措置と組織的措置
  - 10. データ保護影響評価

EU：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

- 通常、個人的な活動として家庭内で個人データを利用する場合、GDPRの適用対象外となる。これは監視カメラについても同様である。しかし同指針では、自宅の監視カメラが公道や隣家を撮影している場合には対象外とならず、GDPRを遵守する必要があるとされた。
- 関連ケースとして、オーストリアのスポーツカフェが監視カメラで公道を撮影していた（防犯に必要な範囲を超えた）として、2018年にスウェーデンの監督機関から約5000ユーロの制裁金を科されている。

○ ガイドライン第12項

- ビデオサーベイランスの文脈における本条項（いわゆる家庭内利用の例外）は、狭く解釈されなければならない。欧州司法裁判所（European Court of Justice）によって認められたように、いわゆる「家庭内利用の例外」は、「個人データがインターネット上で公開され不特定多数の人々にアクセス可能となっているような個人データ処理の場合は明確に該当しないような、個人の私的な生活または家庭生活において実施された活動のみに関連するものとして解釈され」なければならない。さらに、ビデオサーベイランスシステムが、個人データの持続的な（constant）録画と保管を伴うものであり、「部分的にであれ公共空間をカバーし、私的敷地内から外側へ向けられたものである場合、EU指令95/46の第3条2項の第2インデントの目的での純粋に「個人的または家庭的」活動とはみなすことはできない。」（ECJ判例, C-212/13, 2014年12月11日）

EU：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

○ ガイドライン第73項

- 生体データの利用、とりわけ顔認識の利用は、データ主体の権利に対する大きなリスクを伴う。このような技術に頼る場合には、GDPRで規定された適法性、必要性、比例性、およびデータ最小化の原則を尊重することが極めて重要である。これらの技術の利用は効果的とみなされうる一方で、管理者はまず基本的人権と自由に対する影響を評価し、当該処理の目的を達成するためのより侵害的でない手段を検討するべきである。

○ ガイドライン第74項

- GDPRで定義された生体データに該当するには、自然人の身体的、生理的または行動的な特性などの生データ（raw data）の処理が、それらの特性の測定を伴うものでなければならない。生体データはそのような測定の結果であるため、GDPRは第4条14項において、生体データは「自然人の身体的、生理的または行動的な特性に関連する特別な技術的処理から得られ、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」と規定している。個人のビデオ映像は、それらが個人の識別に寄与するように特別に技術的に処理されていない場合には、それ自体ではGDPR第9条の生体データとはみなされない。

○ ガイドライン第75項

- 生体データが特別な種類の個人データの処理（第9条）とみなされるためには、生体データが「自然人を一意に識別することを目的」として処理されている必要がある。

EU：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

- 顔認識技術の利用に対しては、同指針でさらに厳しい法解釈が示されている。例えば、空港でチェックイン時に顔写真の登録を行うことで手荷物カウンターや搭乗ゲートでパスポート等を見せずに顔認証で通過できる顔パス認証サービスでは、顔認識システムを専用ゲート内に設置し、顔認識に同意していない旅客の顔特徴データを取得しないようにしなければならない。コンサート会場で顔パス入場を行う場合も同様である。
- またオフィス等の入退場管理に顔認証を使う場合も、全ての従業員に顔認証を強いるのではなく、それ以外の入場方法（社員証の提示等）も提供しなければならないとされている。

○ ガイドライン第78項

- 例：　ある民間企業が、サービスを改善するために、空港内の旅客識別チェックポイント（手荷物預かりカウンター、搭乗ゲート）を、顔認識技術を用いたビデオサーベイランスシステムに置き換える。このシステムでは、顔認識による手続きに同意した旅客を認証（verify the identity）する。当該処理には第9条が適用されるので、旅客は事前に明示的かつ情報提供された同意を与えた上で、顔特徴データを作成し、搭乗券やアイデンティティ情報と関連付けるために自動端末等で自分を登録しなければならない。顔認識を用いたチェックポイントは他と明確に区別されている必要がある。例えば、顔認識システムは専用ゲート内に導入され、顔認識に同意していない旅客の顔特徴データが取得されないようにしなければならない。事前に同意し、登録手続きを行った旅客のみが、そのような顔認識システムを用いたゲートを利用することとなるだろう。
- 例：　ある管理者が、顔認識技術を用いて自社ビルディングへの入館を管理している。個人が事前に明示的かつ情報提供された同意を与えた場合のみ、顔認識による入館方法を利用することができる。事前同意のない人のデータを取得しないことを保証するために、この顔認識技術はデータ主体自身によって「オン」になるようにするべきである（例えば、ボタンを押す）。処理の適法性を保証するために、管理者はビルへの他の入館方法も常に提供しなければならない（生体データの処理を伴わない方法、例えばバッジや鍵）。

EU：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

- 店舗での顔認識については、来店客を再認してリピーター分析を行う場合は全ての来店客から事前同意を得なければならない。ただし、年代・性別などの属性推定のみで、個人を識別する顔特徴データの作成を伴わない場合は、必ずしも本人同意は必要ない。
- また、ホテルの入口でVIP顧客を顔認識するサービスについては、登録済みのVIPか否かを判断するために撮影を行う際、全ての入館者から顔認識に関する事前同意を得なければならないとされている。

○ ガイドライン第81条

- 例：　ある店舗のオーナーが、ビデオサーベイランスシステムで取得された顧客の性別や年齢に基づいて広告をカスタマイズしたいと考えた。このシステムが個人を一意に識別するための生体テンプレート（特徴データ）を作成せず、カテゴリー分類（属性推定）をするために個人の身体的特性を検知してだけであれば、当該処理には第9条は適用されない。（他のタイプの特別な種類のデータが処理されていない限り）。

○ ガイドライン第83条

- 例：　ある店舗オーナーが、広告をカスタマイズするために、店舗内に顔認識システムを導入した。管理者は、このシステムを利用してカスタマイズされた広告を配信する前に、全てのデータ主体から明示的かつ情報提供された同意を得なければならない。このシステムが生体テンプレート（特徴データ）の作成に同意していない訪問客や通行人のデータを取得するならば、仮にそれらの生体テンプレートが可能な限り短い時間内に削除されたとしても、この顔認識システムは適法ではないだろう。これらの一時的な生体テンプレートの作成は、個人を一意に識別するための生体データの処理に該当する。

EU：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

○ ガイドライン第85条

- 例：　あるホテルが、顔認識によってVIP顧客の到着をホテルマネージャーに自動的に知らせるビデオサーベイランスを利用している。VIP顧客は事前に顔認識の利用について明示的な同意を与え、当該目的のデータベースに登録されている。このような生体データ処理システムは、VIP以外のモニターされる全ての他の客からも第9条2項(a)に従った同意を得ない限り、適法ではないだろう。

- 例：　ある管理者が、コンサートホールの入口に顔認識機能付きのビデオサーベイランスシステムを導入している。管理者は、顔認識システムの付いた入口と、そうでない入口（チケットをスキャンする入口等）の両方を、明確に区別して設置しなければならない。顔認識システムの付いた入口は、同意していない観客の生体テンプレート（顔特徴データ）を取得することのないように設置されなければならない。

EU：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

- 監視カメラ管理者は、個人からの本人映像の開示請求には原則として応えねばならず、映像に他の人が写っている場合はぼかし等を入れたコピーを渡さなければならない。

○ ガイドライン第97条

- 例： データ主体が、1日に3万人の来店客があるショッピングモールの入口におけるビデオサーベイランスを通じて処理された自分の個人データのコピーを請求した場合、データ主体は、2時間程度のタイムフレーム内で、いつ自分がモニターエリアに通りがかったかを特定するべきである。管理者がまだ当該ビデオ映像を保持している場合、そのコピーを提供するべきである。同じビデオ映像内で他のデータ主体が識別できる場合には、請求したデータ主体にコピーを渡す前に、コピーの一部を匿名化（例えば、コピーの一部にぼかしを入れる）するべきである。
- 例： 管理者がビデオ映像を例えば2日以内に自動的に消去している場合、管理者は2日後以降にデータ主体にビデオ映像を提供することができない。管理者が2日後以降に請求を受けた場合、データ主体は適切な情報提供を受けるべきである。

EU：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

- また、個人が撮影エリアに入る前に認識できるように、適切な場所に監視カメラに関する警告表示を設置せねばならないとされている。

○ ガイドライン第113条

- 当該情報は、モニターエリアにデータ主体が入る前にビデオサーベイランスの環境について容易に認識できるような態様で、モニターエリアから合理的な距離の位置に設置されるべきである。どのエリアがモニタリングの対象であるかについて疑いがなく、またサーベイランスの文脈が明確なものである限り、ビデオサーベイランスの設備の正確な位置を特定することは必ずしも必要ではない。データ主体は、サーベイランスを回避したり、必要あれば自分の振る舞いを調整したりできるように、どのエリアがカメラで撮影されているかについて想定できなければならない。

○ ガイドライン第114条

- 第一階層の情報（警告表示）は、一般的に最も重要な情報を掲載するべきである。例えば、処理目的の詳細、管理者の身元、データ主体の権利の存在、当該処理の最も大きな影響に関する情報を掲載するべきである。これには、例えば管理者の正当な利益や、データ保護責任者（DPO）の連絡先詳細なども含まれうる。また、より詳細な第二階層情報への言及や、第二階層情報へのアクセス方法についても含めなければならない。

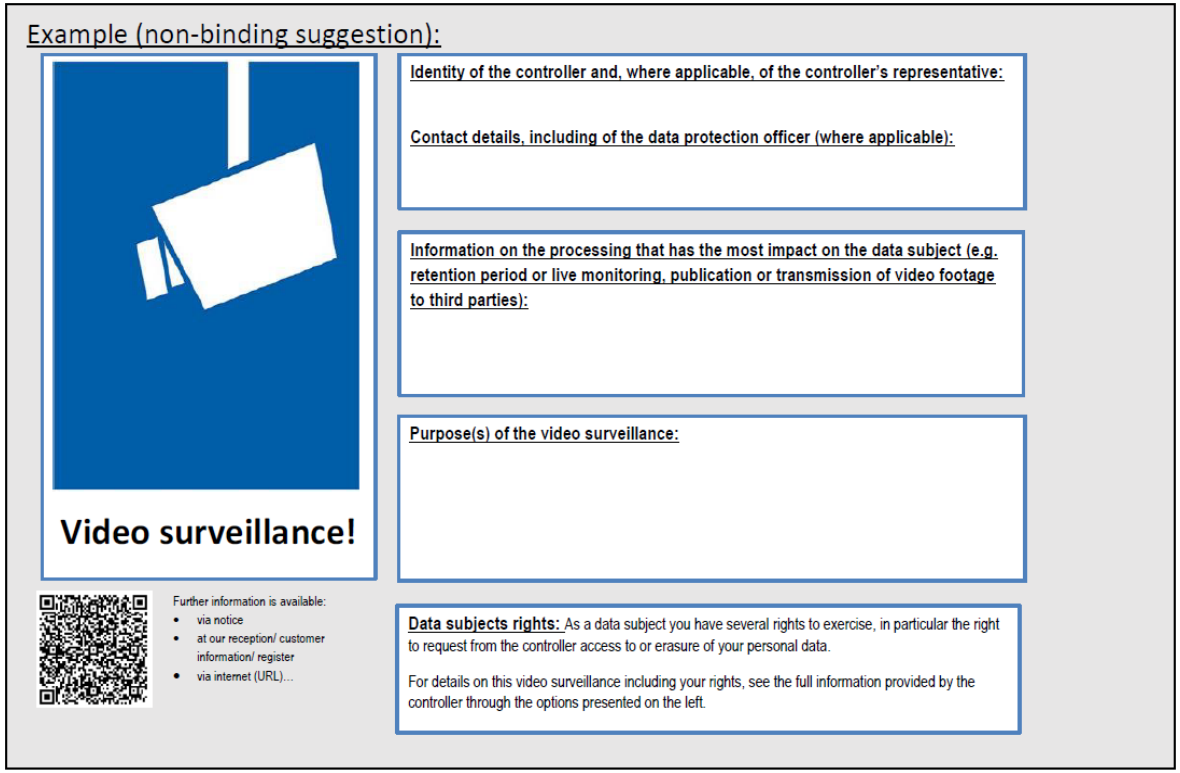
EU：ビデオ機器を通じた個人データ処理に関するガイドライン

○ ガイドライン第115条

- さらに、警告表示には、データ主体を驚かせる可能性のある情報についても含めるべきである。例えば、第三者への提供（とりわけEU域外の第三者への提供）や、保存期間などである。これらの情報が表示されていない場合、データ主体は、単にライブモニタリングが行われているだけ（データの記録や第三者への提供は行われていない）と信じることができるべきである。

○ ガイドライン第116条

- 例：



EU：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

- **欧州での事業活動に影響を与える恐れのある規定**

顔認識サービス例	GDPRガイドライン案における要件	理由
空港での顔パス認証	顔認識システムを専用ゲート内に設置し、顔認識に同意していない旅客の顔特徴データを取得しないようにしなければならない	顔特徴データはセンシティブデータであるため、取得に当たって本人の明示的同意が必要（映り込みでの取得は不可）
コンサート会場での顔パス入場	顔認識システムの付いた入口と、そうでない入口（チケットをスキャンする等）の両方を明確に区別して設置しなければならない	
店舗でのリピーター分析	全ての来店客から事前同意を得なければならない	
ホテルでのVIP顔認識	登録済みのVIPか否かを判断するために入口で撮影を行う際、全ての入館者から顔認識に関する事前同意を得なければならない	
顔認証によるビル入退館管理	全ての入館者に顔認証を強いるのではなく、それ以外の入場方法（社員証の提示等）も提供しなければならない	強制的な同意は、有効な同意とみなされない

EU：欧州委員会のAIホワイトペーパー

- 欧州委員会は2020年2月19日に、「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」（White Paper on Artificial Intelligence - A European approach to excellence and trust） を公表。

  （https://ec.europa.eu/info/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en）

- 同ホワイトペーパーは、EUがAIに関する独自の「優越のためのエコシステム」と「信頼のためのエコシステム」を構築することを目標として掲げ、その実現に向けた政策オプションを提示。

- 前者の「優越のためのエコシステム」については、欧州産業および専門家市場の強化に向け、加盟国や民間部門と協力して、研究やイノベーションにおける投資を拡大し、AIスキル開発を強化し、中小企業等におけるAI導入にインセンティブを与えることを提案している。この目標のため、今後10年間にわたり、民間資金も合わせ、年間200億ユーロをAIに投資する方針。

- 後者の「信頼のためのエコシステム」については、AIが基本的人権や安全性に及ぼしうるリスクについて指摘した後、ハイリスクなAIアプリケーションについては、6つの義務的要件を含む新たな規制フレームワークが必要とし、更なる検討を行うとしている。また、ハイリスクなAIアプリケーションに対しては事前適合性評価が提案され、それ以外のAIアプリケーションに対しては自主的なラベリング制度が提案。

- リモート生体識別（公共空間での自動顔認識など）もハイリスクAIアプリケーションの1つとされているが、これについては特に1節を割いて言及がなされ、このようなAI利用が許可される条件について明確化するために、広範な関係者を巻き込んだ議論の場を立ち上げるとしている。

- 欧州委員会は2021年4月21日に、この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（AIシステムを規制する新たな規則案）を提出予定。

EU：欧州委員会のAIホワイトペーパー（リモート生体識別）

○ハイリスクなAIアプリケーションに課すべき要件

ｆ） リモート生体識別（自動顔認識など）に対する特別な要件

- リモートでの個人識別の目的での生体データの取得や利用は、例えば公共の場での顔認識のディプロイメントを通じたものは、基本的人権に特別なリスクをもたらす。リモート生体識別AIシステムを利用することの基本的人権への影響は、当該利用の目的、コンテキスト、範囲によってかなり変わりうる。
- EUのデータ保護ルールは、特定の条件下を除き、自然人をユニークに識別する目的での生体データの処理を原則として禁止している。とりわけ、GDPRの下では、そのような処理は限定された根拠に基づいてのみ行うことができる。そのうち主たる根拠は、重要な公共の利益である。そのようなケースでは、当該処理はEU法または加盟国の国内法に基づいて、比例性、データ保護の権利の尊重、および適切な安全管理措置の要件の下で、実施されなければならない。警察・刑事司法データ保護指令の下では、そのような処理に対する厳密な必要性や、原則としてEU法や国内法の規定、適切な安全管理措置がなければならない。自然人をユニークに識別する目的での生体データの処理はEU法で規定された禁止の例外に当たるため、EU基本権憲章の対象となる。
- EUの現行のデータ保護ルールやEU基本権憲章と整合的に、AIはリモート生体識別の目的では、そのような利用が十分に正当化され、比例的であり、十分な安全管理措置に服している場合にのみ、利用することができる。
- そのような公共の場でのAI利用に関連した社会的懸念に対処するために、またEU内部市場の断片化を避けるために、欧州委員会はそのようなAI利用（公共の場でのリモート生体識別の目的でのAI利用）を正当化するような特定の条件について、また共通の安全管理措置について、広範な欧州の議論を立ち上げる予定である。

【ご参考】 AI白書のリモート生体識別（顔認識等）に対するEDPS見解

- EDPS（European Data Protection Supervisor：欧州データ保護監察官）は2020年6月29日に、欧州委員会のAIホワイトペーパーに対する意見「EDPS Opinion on the European Commission's White Paper on Artificial Intelligence」を公表。
（https://edps.europa.eu/sites/edp/files/publication/20-06-19_opinion_ai_white_paper_en.pdf）
- EDPSは同意見書で、AIホワイトペーパーで挙げられたリモート生体識別（Remote biometric identification：RBI）に関して、EUにおける公共空間での利用を一時的に禁止する考えを支持。
- 以下、同意見書からの抜粋。

- 62. 欧州委員会のAIホワイトペーパーは、リモート生体識別（RBI）によってもたらされる基本的権利に対するリスクを認識しており、これはEDPSも共有する見解である。リモート生体認証は2つの問題を生じさせる。1つは（遠くからの、大規模で、時には秘密での）個人の識別であり、もう1つは（遠くからの、大規模で、時には秘密での）生体データの処理である。AIに依存しているか否かに関わらず、これら2つの特徴のいずれかに関連する技術は同様な問題があり、RBIと同じ制限を適用する必要があるかもしれない。
- 63. RBIシステムによって個人の権利と自由にもたらされるリスク、たとえば公共の場でのリアルタイム顔認識のリスクは、適切に特定および軽減されなければならず、そのようなプロセスには、そのような技術の利用によって最も影響を受ける人々が含まれるべきである。RBIのリスクの一部は、RBIシステムが簡単に隠され、摩擦がなく、多くの場合は単なる「実験」として提示されるが、ユビキタスで広範にわたる監視システムに簡単に変えることができるという事実から生じる。

【ご参考】 AI白書のリモート生体識別（顔認識等）に対するEDPS見解

- 64. RBIをサポートするインフラがひとたび整うと、簡単に他の目的で利用することができる（「ファンクションクリープ：機能の目的外利用」）。最近ではRBIシステムまたは他の技術インフラの一部を使用して、ソーシャルディスタンシングの測定やマスク使用の測定、温度チェック（カメラに温度計が統合されている場合）など様々な方法でパンデミックと戦うことができると主張する人もいる。これらの新しいアプリケーションの一部はGDPRの適用範囲に含まれない場合があるが、それでも民主主義社会では委縮効果をもたらすかもしれない。したがって、このようなAIの利用、およびそのようなファンクションクリープは、AIに関する規制で適切に対処するべきである。
- 65. RBIは重大な基本的権利の問題を生じさせる可能性があるが、EDPSは、個人の識別を目的としないRBI関連の技術も深刻なプライバシーの懸念を引き起こすことを強調したい。たとえば、リアルタイム顔認識に基づく感情検出では個人の感情を推測することができる。
- 66. このような技術がディプロイされる状況で、技術が必要であるか、比例的であるかどうか、またはそれが望まれているかどうかを評価することは最も重要である。EDPSはこの目的のために、情報に基づいた民主的な議論が行われるように、またEUや加盟国が特定のユースケースに対する各技術やシステムの比例性を保証するための包括的な法的枠組みを含めすべての適切な保護措置を講じるまで、EUにおける公共空間での自動認識のディプロイメントに対するモラトリアム（一時的禁止）の考えを支持する。それらには顔、歩容、指紋、DNA、声、キーストローク、その他のバイオメトリクスまたは行動信号などの人間の特徴の自動認識が含まれる。
- 67. 越境的・国内的な健康危機などの国家緊急事態の際の公的機関によるRBIの利用は、重要な公共の利益の理由で必要なものであり、EUまたは加盟国の法律に基づくものであり、透明性が高く、アカウンタブルであり、追求される目的に比例しており、特定の保護措置に服するものであり、期間が明確に制限されており、基本的人権の本質と人間の尊厳の尊重と矛盾しないもとであるべきである。

【ご参考】 AIホワイトペーパーを巡る動き

- 欧州委員会DG Connect（コミュニケーションネットワーク・コンテンツ・技術総局）のグロス課長（デジタル化産業課）は9月3日、欧州議会IMCO（域内市場・消費者保護委員会）の議員団に対し、「AIホワイトペーパーのパブリックコンサルテーションの結果を検討中であり、欧州委員会は欧州での顔認識技術の利用の将来的な禁止の選択肢を排除してはいない」と述べた。
  - グロス課長は、GDPRは生体データの処理をカバーしうるが、欧州委員会は顔認識技術から取得したデータに関してGDPRの規定が十分であるかどうか、「追加の保護措置が必要かどうか、または特定ケース・特定エリアで一時的に顔認識を許可しない必要があるかどうかを検討する」と述べた。
  - AI白書のパブリックコンサルテーションでは、公共空間でのリモート生体識別に対する懸念が多く寄せられ、グロス課長は欧州での利用について「EUでの特別な議論が必要」とした。同氏によれば、回答者の28%が公共の場でのリモート生体識別の禁止を支持しているという。
- 出典：Euractiv 2020年9月3日記事（https://www.euractiv.com/section/data-protection/news/commission-will-not-exclude-potential-ban-on-facial-recognition-technology/）

EU：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、完全に新しく実際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オメト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

欧州評議会：　顔認識に関するガイドライン

- 欧州評議会は2021年1月28日に、「Guidelines on Facial Recognition（顔認識に関するガイドライン）」を公表。（https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3）
- 欧州評議会（Council of Europe, CoE）は、欧州連合（EU）とは全く別の国際機関。EUの加盟国27カ国すべてを含む47カ国から成る。日本は米国、カナダなどと共にオブザーバー国である。「顔認識に関するガイドライン」は、欧州評議会の「個人データの自動処理に係る個人の保護のための条約第108号（※）」の批准国向けのもの。

※ 同条約は1981年1月28日に各加盟国の署名に付された。2021年2月現在で欧州評議会加盟国47カ国と非加盟国8カ国（ウルグアイ、セネガル、チュニジア、メキシコ、アルゼンチン、モロッコ等）の計55カ国が同条約を批准。

- 「差別のリスクを回避するための適切な保護措置が法律で定められていない限り、人の肌の色、宗教上またはその他の信条、性別、人種的または民族的な出自、年齢、健康状態、または社会的状態を判断することのみを目的とした顔認識の使用は禁止するべきである。」（1.1節）
- 「同様に、感情認識（affect recognition） は、顔認識技術を使用して実行することもでき、顔画像から性格特性、内面の感情、メンタルヘルス、または労働者の関与度を高い可能性で検出できる。例えば、感情認識をスタッフの雇用、保険へのアクセス、教育に結び付けることは、個人レベルと社会レベルの両方で大きな懸念のリスクをもたらす可能性があり、禁止されるべきである。」（1.1節）
- 「民間企業は、ショッピングモールなどのuncontrolled environmentsにおいて、とりわけ関心のある人物を識別するために、マーケティング目的や民間の防犯目的で、顔認識技術を展開してはならない。顔認識技術が使用されている環境を通過することは、明示的な同意とは見なされない。」（1.2.3節）

英国：カメラ・顔認識に関連した法令・ガイドライン・制度

- 法令
  - 2018年データ保護法： GDPRおよび警察・刑事司法データ保護指令の下での新法
  - 2012年自由保護法： 警察や地方自治体によるカメラ設置を規制
- 第三者機関
  - 情報コミッショナー・オフィス（ICO）
    - 個人データ保護全般を監督。日本の個人情報保護委員会に相当。
  - 監視カメラコミッショナー（SCC）
    - 監視カメラに特化した監督機関。
- ガイドライン
  - CCTV行動規範（2014/2015年）：ICOが策定、官民全般が対象
  - 監視カメラ行動規範（2013年）： SCCが管轄、警察と地方自治体が対象

- 監視カメラに対する認証制度（2015年11月開始）
  - 監視カメラ行動規範の12原則を遵守していることを認証。
  - 認証マークはWebサイト等で使用可。
  - 40組織が認定取得（小売企業・病院・大学・警察等）。（2017年時点）

英国：2018年データ保護法

- 「所管官庁（competent authorities）」による「法執行目的（law enforcement purposes）」での個人データ処理は、2018年データ保護法（DPA）第3部によってカバーされる。
- とりわけ、法執行目的での自動顔認識（AFR、LFR）の利用は、個人をユニークに識別する目的での生体データの処理を伴うため、DPA第35条（8）bの「センシティブな処理」に相当する。
- そのようなセンシティブな処理においては、DPA第35条（第一のデータ保護原則）、第42条（保護措置：センシティブな処理）、第64条（データ保護影響評価）の要件がとりわけ重要。
- DPA第35条（第一のデータ保護原則）

（１）第一のデータ保護原則は、法執行目的での個人データの処理は適法（lawful）であり、公正でなければならないというものである。

（２）法執行目的での個人データ処理は、それが法令に基づくものであり、かつ以下のいずれかを満たす場合に限り適法である。

(a)データ主体が当該目的での当該処理に同意を与えている場合、または

(b)所管官庁によって当該目的で行われる職務の遂行に当該処理が必要となる場合

（３）さらに、法執行目的での処理がセンシティブな処理である場合、当該処理は（４）項と（５）項で規定された2つのケースにおいてのみ許可される。

（４）第一のケースは、

(a)データ主体が法執行目的での当該処理に（２）項(a)にいう同意を与えている場合、かつ

(b)当該処理が実施される時点で、管理者が適切なポリシー文書（第42条参照）を用意している場合

（５）第二のケースは、

(a)当該処理が法執行目的で厳密に必要とされる場合、

(b)当該処理が別表8の条件の少なくとも1つを満たしている場合、かつ

(c)当該処理が実施される時点で、管理者が適切なポリシー文書（第42条参照）を用意している場合

（６）～（７）、（８）(a)(c)(d)省略

（８）「センシティブな処理」は、以下を意味する。

(b) 個人をユニークに識別する目的での、遺伝子データまたは生体データの処理

英国：2018年データ保護法

- 「別表8：第3部におけるセンシティブな処理の条件」で規定された条件は以下の9つ。
  - 法令上の目的（Statutory etc purposes）
  - 司法行政（Administration of justice）
  - 個人の生命に関する利益の保護
  - 子どもおよび危険にさらされている個人の保護
  - 既に公開されている個人データ
  - 法的手続きなど法律上の要求（Legal claims）
  - 司法行為（Judicial acts）
  - 詐欺の防止
  - アーカイブ目的等

英国：監視カメラコミッショナーのカメラ顔認識に関するガイダンス

- 英国の監視カメラコミッショナー（Surveillance Camera Commissioner：SCC）
  - イングランドおよびウェールズにおける警察・自治体による監視カメラ使用を監督する第三者機関。

- 監視カメラ行動規範（https://www.gov.uk/government/publications/surveillance-camera-code-of-practice）
  - 2012年：　自由保護法が制定され、同法の下でSCCが新設されることになった。
  - 2013年6月：　自由保護法の下で、国務大臣によりに監視カメラ行動規範が策定された。
  - 自由保護法や監視カメラ行動規範（SCCが運用を監督する）は警察や地方自治体設置のカメラのみが規制対象であり、民間設置のカメラは対象となっていない。
    - 民間設置カメラはデータ保護法で規制され、ICOが監督。
  - 監視カメラ行動規範の主な内容は以下の通り。

- 監視カメラは適切に使用されれば、犯罪予防・犯罪捜査・起訴において、パブリックセーフティやセキュリティに貢献し、人と財産の両方を保護する有益なツールである。（1.3、2.1節）
- 公共空間における監視の濫用や誤用に対する懸念に対処するために策定された。（1.8節）
- プライバシーの権利への潜在的な干渉を考慮するに当たっては、プライバシーへの期待が時と場合によって異なるものであり、また主観的なものであるという事実を認識することが重要である。公共空間は他人と関わり合うゾーンであるが、私的生活の範囲に入ることもある。個人が、公共空間における監視は適切な安全管理措置と共に必要かつ比例的なものであるべきと期待することは間違っていない。（2.3節）
- 従って、監視カメラ技術の使用を決定するに当たっては、正当な目的と差し迫った必要性とを満たしていなければならない。そのような正当な目的や差し迫った必要性は、明確化され、特定された目的として文書化されなければならない。システムの設計は、特定された目的に比例的なものであるべきであり、予算消化や新技術導入を優先させるべきではない。（2.4節）
- システムオペレーター（監視カメラ設置者）が守るべき12原則を規定。（3節、4節）

【ご参考】監視カメラ行動規範の12原則

種別	原則	内容
監視カメラシステムの開発や使用に関する原則	原則1	監視カメラシステムの使用は常に、正当な目的の追求において、かつ特定された差し迫った必要性に不可欠なものとして、特定の目的の下でなされなければならない。 • 正当な目的や差し迫った必要性には、国家安全保障、パブリックセーフティ、経済福祉、秩序違反予防・犯罪予防、保健・道徳保護、人権や自由の保護が含まれる（3.1.1）。
	原則2	監視カメラシステムの使用は、個人とそのプライバシーに与える影響を考慮に入れなければならず、その使用が正当なものであることを保証するために定期的なレビューを行わなければならない。 • 顔認識その他の生体認識システムの利用は、特定された目的に合致する範囲内で、明確に正当化され比例的なものであり、適切に評価されたものである必要がある（そのようなシステムの評価についてはSCCが助言を提供する）。顔認識等を用いて個人にデメリットとなる決定が行われる場合には、必ずヒューマンチェックを行うべきである（3.2.3）。
	原則3	監視カメラシステムの使用には、情報へのアクセスや苦情申立てのためのコンタクトポイントの公表を含め、可能な限りの透明性がなければならない。
	原則4	全ての監視カメラシステムの活動には、取得・保持・利用される映像と情報を含め、明確な責任とアカウンタビリティがなければならない。 • 1つの監視カメラシステムが、犯罪予防・捜査と交通管理など、複数の目的で使用されてもよい（3.4.3）。

【ご参考】監視カメラ行動規範の12原則

種別	原則	内容
当該システムで取得された画像や情報の利用や処理に関する原則	原則5	監視カメラシステムの使用に先立って、明確なルール、ポリシー、手続きが用意されなければならない。そして、これらを遵守する必要がある関係者すべてに伝達されなければならない。 • 監視カメラシステムが公共空間をカバーする場合は、システムオペレーターは法的要件として、SIA（警備業監督委員会：Security Industry Authority）が発行するCCTVライセンスを持った職員に実施させなければならない（4.5.6）。
	原則6	監視カメラシステムの特定された目的に厳密に必要となる以上の映像や情報は保存されるべきではない。それらの映像や情報は当該目的が果たされた時点で削除するべきである。
	原則7	保持された映像や情報へのアクセスは制限されるべきであり、誰がどのような目的でアクセスできるかについて明確に規定されたルールがなければならない。映像や情報の提供（disclosure）は、当該システムの設置目的や法執行目的に必要な場合に限られるべきである。 • 本人によるアクセス請求（subject access request）に関してはICOのCCTV行動規範を参照（4.7.5）。
	原則8	監視カメラシステムのオペレーターは、当該システムとその目的に関連性のある、認定された運用基準・技術標準・資格能力基準を考慮に入れるべきであり、当該基準に適合するようにするべきである。
	原則9	監視カメラシステムの映像や情報に対しては、不正アクセスや不正利用から保護するための適切な安全管理措置を講じるべきである。
	原則10	法的要件、ポリシー、基準が実際に遵守されていることを保証するための有効なレビュー・監査メカニズムを設けるべきであり、定期的なレポートが公表されるべきである。
	原則11	監視カメラシステムの使用が正当な目的の追求においてなされ、かつその使用に差し迫った必要性がある場合、当該システムは、証拠としての価値がある映像や情報を処理する目的で、パブリックセーフティや法執行に最も効果的に役立つ方法で使用されるべきである。
	原則12	監視カメラシステムと連携して、照合目的で参照データベースにおいて使用される情報は、正確で最新のものであるべきである。 • 自動ナンバープレート認識（ANPR）や顔認識のような技術の使用は、他機関が提供するデータベース等の情報の正確性に依存しうるため、それらの基盤となる情報が目的に適合していることを保証するために定期的なアセスメントなくしては導入すべきでない（4.12.1）。

英国：監視カメラコミッショナーのカメラ顔認識に関するガイダンス

- カメラ顔認識に関するガイダンス（https://www.gov.uk/government/publications/police-use-of-automated-facial-recognition-technology-with-surveillance-camera-systems）
  - SCCは2020年12月3日に、「Facing the Camera」という警察向けのグッドプラクティス・ガイダンスを公表した。
  - 2020年8月の南ウェールズ警察控訴院判決を受けたもの。
  - イングランドとウェールズの警察が法制度（自由保護法、監視カメラ行動規範）に従って公共空間において自動顔認識（AFR）を組み込んだ監視カメラシステムを使用する方法を示している。
  - 同ガイダンス内で英国政府・警察向けに提言も行っており、主な推奨事項(recommendation)は以下。

- 内務省が英国警察本部長評議会（NPCC）および警察犯罪コミッショナー協会（APCC）等と協議して、以下を策定すること。
  - a）国民の信頼を生み出すような国家調達戦略。
  - b）LFR技術の信頼性（精度、しきい値、人間の意思決定など）を適切に分析および評価できる手段。
  - c）警察がLFR使用に関して法定のリスク評価義務を遵守できるようにするための国内基準（例えば、PbD）。
- 警察がLFRの運用を検討している場合、意思決定と運用に関して有意義で独立した「倫理的監督」を提供するメカニズム（倫理委員会など）を開発すること。
- 内務省、規制当局、その他の利害関係者が協力して、LFRなどの問題への包括的なアプローチを提供する単一の「統合的影響評価」プロセスの開発を検討すること。
- 内務省と政府が、バイオメトリクスや同様に侵害的な技術を使用するような警察による（公開の）監視行為を規制する法律をレビューすること。
- 内務省がSCCと協力して監視カメラ行動規範をレビューおよび更新すること。
- 特に、法律や行動規範において、侵害的な監視行為の倫理基準、平等性、合法性、ガバナンス、アカウンタビリティについて明確な規定を設けること。

米国：カメラ･顔認識に関連した法令･ガイドライン･制度

- 法令
  - （個人情報保護法に相当する民間分野の一般法（連邦法）は無い）
  - 連邦取引委員会（FTC）法第5条：
    - 企業のプライバシーポリシーに虚偽の記載があれば、FTCは当該企業を訴追できる。
  - ビデオ隠し撮り防止法：
    - 個人の「私的領域」の写真を、本人同意なく意図的に撮影することを禁止。
  - 州法： テキサス州、イリノイ州、ワシントン州
    - 民間企業･民間団体は生体認証識別子（顔特徴データを含む）の取得に先立ち、本人の同意を得なければならない。
  - 州法： カリフォルニア州、オレゴン州、ニューハンプシャー州
    - 警察官のボディカメラや携帯端末における顔認識技術の利用を禁じる。
  - 州法： ワシントン州（2020年3月成立）
    - 州と地方政府機関を規制。①は対象外、②は一定条件下でOK、③は原則禁止。
  - 市の条例： サンフランシスコ市、加州オークランド市、マサチューセッツ州サマービル市
    - 警察など市の機関による顔認識技術（①②③すべて）の利用を禁じる。
  - 市の条例： オレゴン州ポートランド市（2020年9月成立）
    - サンフラン市と同様な規定に加え、市の公共施設での民間企業による利用を禁じる。

４．顔認識技術の3つの用途ごとの対応

まとめ：顔認識技術の3つの用途ごとの対応

①本人同意の下での顔認証サービス

- 空港ゲートでの顔認証や店舗での決済時の顔認証、オフィスへの入退時の顔認証などは、本人が同意した上でのデータ利用であるため、（日米欧の）法律上は基本的には問題ない。（前述のようにEU・英国では同意強制や映り込みは不可。）
- また、顔認証以外の選択肢を用意することで「同意強制」を避ける、顔認証には専用レーンを用意することで「映り込み」を避けるといった対応を行うことで、社会的な受容性の面でも問題ないと考えられる。

②法執行機関による容疑者写真の顔照合

- あくまで犯行現場等で取得された「容疑者」の顔写真に対する顔照合であり、犯罪と無関係の一般市民の権利を侵害するものではない。
- 顔照合DBの内容が（一般市民を含まない、不正確な情報に基づかない、SNSなどの情報を目的外利用しないなど）適切であり、人種・性別的バイアスに十分に配慮されたソフトウェアが用いられ、またシステムによる自動判断ではなくヒューマンチェック（人間の関与）を保証する制度設計がなされていれば、特に利用を制限する理由は見当たらない。

まとめ：顔認識技術の3つの用途ごとの対応

③公共空間等での不特定多数に対する自動顔認識

- 欧米における顔認識技術に対する批判は③の用途に集中。主な懸念は前述の5点 。
- 日本での炎上事例（大阪駅ビル実証、札幌市実証）も③の用途（誤認を含む）。

（１）警察による利用

- EUや英国では警察や自治体等の公的機関が、犯罪捜査目的などで監視カメラを用いて顔特徴データを取得したり自動顔認識を行うことについては、EU法令や英国データ保護法上で禁止されてはいないが、「厳密に必要とされる場合に限る」など、取得・利用に当たって厳格な要件が課されている。
- 日本においては、警察や自治体等の公的機関が公道などの公共空間で監視カメラを用いて顔特徴データを取得したり自動顔認識を行うことは、明示的に規制されている訳ではない。しかし、不特定多数の個人に対する自動顔認識に対しては国内においても抵抗感が強く（※）、社会的コンセンサスが得られにくい用途となっている。
  - ※ クレスト社の2019年12月の調査では、「顔認証サービスの利用に抵抗がある」回答者は65%であり、抵抗がある理由は（複数回答）、「目的は何であれ、無断で自分の顔や姿を撮影されることが不快」が48%、「自分の写った画像や動画がどのように利用されるかわからない」が46%であった。日本経済新聞記事より。
- 警察や自治体等の公的機関による利用については、目的（犯罪予防・犯罪捜査・テロ対策など）と手段（自動顔認識）との比例性（proportionality）に基づき慎重に検討するべきであり、万が一導入する場合であっても、「厳密に必要とされる」場合、例えば、大規模イベント開催時、テロ警戒レベル上昇時など期間と場所とを限定した利用にとどめるべき。

まとめ：顔認識技術の3つの用途ごとの対応

③公共空間等での不特定多数に対する自動顔認識

（２）民間企業による利用

- EUや英国では、民間企業が一般市民から明示的な同意なく顔特徴データを取得することはGDPRや英国データ保護法上で原則禁止されている。米国の一部の州でも、民間企業が本人同意なく顔特徴データを取得することが禁止されている。
- 日本では、民間企業が店舗等で個人の顔特徴データを取得する際に、個人情報保護法上は、本人同意までは求められず、本人に利用目的等を通知または公表をすればよいこととなっている。
- しかし、前述のように不特定多数の個人に対する自動顔認識に対しては抵抗感が強く、社会的コンセンサスが得られにくい用途であるため、民間企業が日本国内でこの③の利用を行うに当たっては慎重な検討と対応が求められる。例えば、以下の検討や対応が求められるだろう。
  - 自動顔認識の実施に先立ち、プライバシー影響評価（PIA）を実施する。
  - 同じ目的（リピート顧客の分析、万引き犯顔照合等）を、よりプライバシー侵害性の低い他の手段で実現できる場合は、そちらの手段を優先的に検討する。
  - 地域住民が利用せざるを得ないエリア（駅、ショッピングモール、商店街等）では実施しない。
  - 地域住民への事前告知・通知を十分に行う。

日米欧における顔認識と法規制/社会的受容性

		日本	米国	欧州・英国
①本人同意の下の顔認証	法律上は可能か	○	○	○ （ただし同意の強制や、同意のない個人からの顔特徴データ取得は×）
	社会的受容性はあるか	○	○	○
②容疑者写真の顔照合	法律上は可能か	○？	△ （サンフランシスコ市等で×）	○
	社会的受容性はあるか	○	○	○
③公共空間での自動顔認識（警察利用） ※本人同意なし	法律上は可能か	○？	△ （サンフランシスコ市等で×）	○
	社会的受容性はあるか	△	△	△
③'店舗等での自動顔認識（民間利用） ※本人同意なし	法律上は可能か	○	△ （テキサス州、イリノイ州、ワシントン州で×）	×
	社会的受容性はあるか	△	△	×

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 ―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Ⅷ：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