欧米におけるカメラ・顔認識サービスと規制動向

2019年10月

国際社会経済研究所

小泉　雄介

y-koizumi@pd.jp.nec.com

概要

- 近年の顔認識技術の精度向上により、空港、小売店、ショッピングセンター、ホテル、フィットネスセンター、交通機関、図書館、オフィスなど、様々な場面で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。
- ①スマホやPCのログイン、空港での入出国管理、テーマパークの入場管理など、本人の同意の下で個人認証（本人確認）の目的で行われる顔認識サービス（いわゆる顔認証：Facial Authentication）（多くは1-to-1）に対しては、懸念する声は少ない。
- ②また、警察機関が容疑者の顔写真と犯罪者データベース等の顔画像を捜査目的で照合する顔照合（Facial Matching）（1-to-many）に対しても、懸念する声は少ない。
- ③しかし、公道や店舗などで（本人同意なく）不特定多数の人々を対象に行われる顔認識、とりわけリアルタイムで個人を識別する自動顔照合（Automated Facial Recognition: AFR あるいは Live Facial Recognition: LFR）（many-to-manyまたはmany-to-1）についてはプライバシー等の問題が指摘され、欧米で同時並行的に規制化の動きが進んでいる。
- 欧米における規制化の動き
  - イギリス：　内務省の監視諮問委員会の設立、南ウェールズ警察に対する訴訟、データ保護監督機関（ICO）による調査など
  - アメリカ：　サンフランシスコ市の顔認識禁止条例制定、連邦法案など
  - EU：　一般データ保護規則（GDPR）の「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案」など

１．諸外国における顔認識技術利用動向

①本人同意の下の顔認証（Facial Authentication）

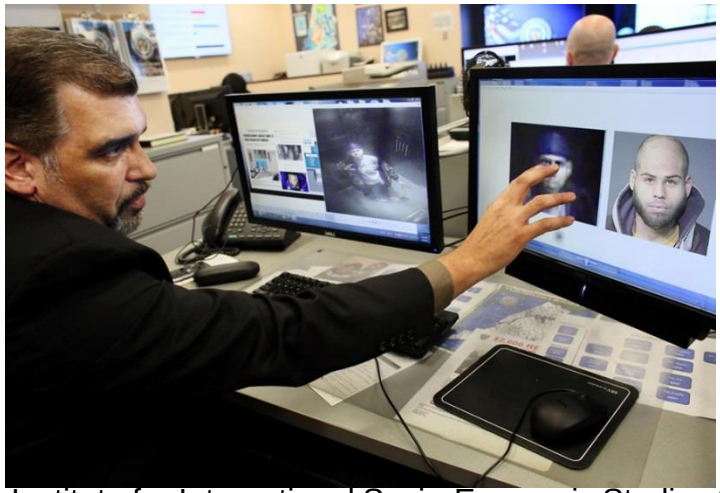
- 空港における顔認証サービス（全世界）
  - 「スターアライアンスとNEC、生体認証による旅客の体験価値向上を目的に協業」
    https://jpn.nec.com/press/201907/20190729_03.html
- イベントの入場管理（EU）
  - 「NEC、EU首脳会議の要人入場管理に顔認証システムを提供」
    https://jpn.nec.com/press/201907/20190717_01.html
- レンタカーでの生体認証（米国）
  - 「顔認証や指紋認証で借りられる米Hertzのレンタカーサービス--30秒で手続き完了」
    https://japan.cnet.com/article/35130220/
- ホテルでのVIP顔照合（インド）
  - 「NEC、インドのホテルグループLemon Tree Hotelsに顔認証ソリューションを納入」
    https://jpn.nec.com/press/201411/20141127_02.html
- 小売店での顔認証決済（中国）
  - 「QRコードはもう古い、アリババやテンセントが進めるのは「顔認証決済」」
    https://www.sbbit.jp/article/fj/36904
- 図書館での顔認証（中国）
  - 「顔認証と24時間化が進む中国の図書館」
    http://tamakino.hatenablog.com/entry/2018/09/04/080000

①本人同意の下の顔認証： 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

- ニューヨーク市警察（NYPD）の顔識別ユニット（Facial Identification Section）
  - 2011年に設立。
  - 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、照合結果を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。
  - 顔照合ソフトウェアで使うデータベースは以下。
    - 逮捕者のデータベース（数百万人）
    - FacebookやInstagramといったSNSの情報
  - 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。
  - 顔照合でヒットしたことは、法的には警官が逮捕を行うための「相当な理由」とは見なされないが、捜査のきっかけとなる（被害者に見せる顔写真の用意等）。



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

【ご参考】ニューヨーク市警察の警察活動支援システム

- ニューヨーク市警察（NYPD）の警察活動支援システムDAS
  - DAS（Domain Awareness System：地域状況認識システム）は以下で構成
    - NYPD所有の監視カメラ（パトカーの車載カメラ含む）
    - NYPDとMOUを締結した民間企業や政府機関の監視カメラ
    - 車ナンバープレート読取機
    - その他のセンサー
  - 2009年から、NYPDがMicrosoft社と共同で開発
  - DAS では監視カメラをネットワーク化
    - NYPDは民間企業が所有する数千のカメラに直接アクセスできる
    - アクセスできるカメラは警察・民間合せて「7,000個」（JETRO／IPAレポート）
  - DASは原則的にテロ対策の目的でのみ利用可能
    - テロ組織による事前活動の観察
    - テロ攻撃の実行準備の検知
    - テロ攻撃の検知
    - インシデントへの反応時間の短縮　等
  - DASでは顔認識技術は使用しないというポリシー
  - 全てのNYPD所有の監視カメラは掲示を付ける。
    - DAS接続のその他の監視カメラにも掲示を付けるようレコメンド。

【ご参考】ワシントンDC首都警察の監視カメラネット

- 首都警察（Metropolitan Police Department：MPD）の監視カメラネットワークシステム
  - MPDのJOCC（共同オペレーションコマンドセンター、警察本部ビル5階）に接続され、JOCCがアクティベートされた場合のみ、監視カメラとの接続もアクティベートされる（＝JOCCでのリアルタイムのモニターが可能になる）。
    - アクティベート回数： 2014年17回、2015年13回。
    - 共同オペレーション： 連邦・州・地域の法執行機関が参加。
  - 監視カメラ接続のアクティベート条件：以下の場合、かつ本部長のオーソライズが必要。
    - 大規模イベント開催時：デモ、大統領就任式、マーチ、パレード、祝典などの際
    - テロ警戒レベル上昇時：テロ攻撃のリスクのある主要施設の周辺の公共空間をモニター
    - 非常時：犯罪発生時等
  - MPD所有の監視カメラ台数（2015年）
    - ①Homeland Security (Permanent) Camera：32台。ダウンタウンのみ。
      ホワイトハウス、USキャピタル、ナショナルモール等の重要施設と、主要幹線・高速道路。
    - ②Neighborhood Crime Camera：103台。犯罪発生件数や住民不安に応じて設置。
      パッシブモニタリング：通常は録画のみで、犯罪発生時に当該エリアの映像を再生。
    - ③トレーラー型可動式カメラ：5台。
  - 設置目的
    - ①テロ対策目的（2001年9月～）
    - ②犯罪捜査・犯罪予防目的（2006年8月～）
  - 監視カメラには、現地に目立つ掲示と、MPDホームページに設置場所の記載あり。

【ご参考】ワシントンDC首都警察の監視カメラネット

- 第三者の監視カメラ（ネットワーク）との接続
  - 他の公共機関の監視カメラネットワークとの接続
    - ワシントンDC交通省の交通カメラ
    - ヴァージニア州・メリーランド州の交通機関の交通カメラ
    - ワシントンDCのパブリックスクールのカメラネットワーク　等
    - 厳密なプロトコルと手続きの下、前頁の大規模イベント時や避難時、犯罪発生時に、接続がアクティベートされ、MPDはこれらのカメラ映像にアクセスできる。

  - 民間所有の監視カメラとの接続
    - Capital Shield プログラム：監視カメラ官民共有パートナーシップ（2014年10月発表）
    - 民間企業の既存の監視カメラをMPDの監視カメラネットワークに接続し、MPDは前頁の重要インシデント時にこれらの民間カメラにアクセスできる。
    - 2014年10月時点で約300台の民間カメラを登録・接続。
    - さらに1000台のカメラを民間に無償提供し、首都警察のネットワークに接続する計画。民間企業は当該カメラを所有できる。

②容疑者写真の顔照合： FBI（連邦捜査局）

- FBIの顔認識ユニットFACE（Facial Analysis, Comparison and Evalualtion）
  - 2011年8月から、FBIの捜査支援のために顔照合サービスを提供。
  - FBI捜査官からの要請に応じて、FBIの独自データベース（NGI-IPS）にアクセスできるのみならず、外部機関（国務省、国防総省、18州のデータベース）を直接検索したり、または検索リクエストを出すことが可能。
  - FACEでは照合結果に対して、バイオメトリクスアナリスト（FACE職員）が目視で候補写真をレビューした後、FBI捜査官に「捜査の端緒」として1～2件の照合結果（写真）を返す。
  - 2011年8月～2015年12月に、FACEは21万5000件の検索を外部機関のデータベースに対してリクエスト。
- FBIのデータベースNGI-IPS
  - Next Generation Identification-Interstate Photo System：次世代個人識別- 州間写真システム。
  - 米国の法執行機関（FBI、州、地域）の犯罪捜査を支援するために約3000万件の写真データベースを検索できるようにした顔照合システム。
  - 3000万件のうち、80%以上が犯罪者の写真。残りは市民の写真（免許、雇用、人物調査（security clearance）、軍隊、ボランティア活動、入国管理時に提出された写真）であるが、FBIは市民の写真については顔照合検索を行っていないという。

②容疑者写真の顔照合： FBI（連邦捜査局）

- FBIの顔認識ユニットFACEの照会先データベース

各機関の顔認識システム	データベースの内容	FBIのFACEユニットが照合結果を得る方法	照合結果の返信件数
FBIのNGI-IPS	刑事司法写真（FBIへの指紋提出に伴うもの）	直接アクセス	2～50件（指定できる）
国務省のFace Recognition on Demand	・ビザ申請者（外国人）の写真 ・Terrorist Screening Centerのデータベースの写真（テロ活動に関与した人、またはその疑いのある人）	直接アクセス	最大88件
	米国市民のパスポート申請写真	検索リクエスト	最大3件
国防総省のAutomated Biometric Identification System	主に、米軍が海外で拘束した個人の写真	検索リクエスト	照合した場合には1件のみ
州の顔認識システム	・運転免許証写真（18州） ・犯罪者写真（4州）	検索リクエスト	州により異なる

②容疑者写真の顔照合： FBI（連邦捜査局）

- FBIやニューヨーク市警などで、捜査支援のために顔認識技術を利用
  - 2017年3月、米国下院の監視・政府改革委員会で、顔認識技術のメリット・課題・法制化の必要性について検討し、FBIにおける顔認識の利用について吟味するために公聴会が開かれた。
- FBIがアクセスできる顔画像データ
  - FBI自前の顔認識システム： 約3000万人分
  - 国務省（パスポート申請者（米国人）、ビザ申請者（外国人））
  - 国防総省
  - 18州（運転免許証写真等）

合計1億2500万人のデータ（米国成人の51%）

- FBI等の顔認識システムに対する懸念：（米国のプライバシー団体が表明）
  - 「パスポートや運転免許といった犯罪と無関係のソースから収集した顔画像が80%を占め、それが犯罪捜査に使われている。照会にあたって令状も必要ない。」
    - これは、本人同意のない目的外利用に当たる。
  - 「シカゴ、ダラス、ロサンゼルス、ニューヨーク、ウェストバージニアの警察がリアルタイム顔照合技術を既に購入しているか、あるいは検討している。」
  - 「さらに、米国の18000の警察機関のうち6000がボディカメラを使っていると推定されるが、ボディカメラがリアルタイム顔照合システムにつながれるまで時間の問題だ。」

③自動顔照合： 警察による自動顔照合の実証実験（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50万人の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自動顔照合： 民間による自動顔照合の実証実験（英国）

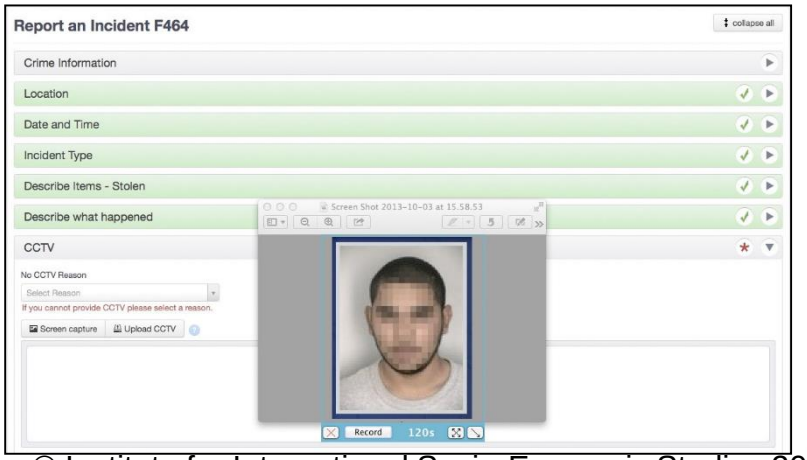
- キングスクロス再開発地
  - ロンドンのキングスクロス駅前の東京ドーム6個分の広さ（27万平方メートル）の再開発地。
  - 既にセントマーティンズ大学が入っており、Googleの英国本社も入居予定。その他、高級マンションや中学校などが入る予定。
  - 敷地内に240台のカメラがあり、不動産会社が保有。CCTV室で集中管理。

- リアルタイム顔照合
  - リアルタイム顔照合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。

地図の出典：www.kingscross.co.uk

③自動顔照合： 万引き犯顔照合（英国）

- Facewatch
  - 英国のベンチャー企業。小売店向けの犯罪オンライン通報プラットフォームを提供。
- 被害届手続きの効率化
  - 顧客となる小売店は、CCTV画像と被害届をオンラインで警察に提出できる。手続き時間を従来の28日間から20分に短縮。10,000以上の小売店が登録している（2015年12月時点）。
- ユーザ企業におけるデータの共有
  - Facewatchには、地域の顧客企業グループ内で、万引き犯その他の潜在的犯罪者のCCTV画像やアラート等を共有する機能がある。既知の万引き犯やバッグ置引き犯の画像等のウォッチリストを地域的に作成したり、共有することが可能である。
- 2017年6月現在、顔認識機能（ウォッチリストと来店客の顔画像を照合）のトライアル中である。



インシデント通報フォーム

③自動顔照合： 自動顔照合に対する懸念

- 自動顔照合の対象となる市民、個人への透明性の欠如
  - 英国の監視カメラコミッショナーによれば、「レスターシャーの事例では、自動顔照合を行なうことに関する通知はチケットの裏面に小さな文字でなされたのみであり、それに気付いた参加ミュージシャンが反対声明を出すなど、かなり大きな問題になった」「自動顔照合の問題は、市民は撮影されていることには気付いても、データベースと照合されていることについてはわからないことだ」とのことである。
- 顔認識技術は他の個人データ取得技術に比べてプライバシー侵害リスクが高い
  - 英国議会の2018年の報告書は、「顔画像は本人が知ることなく容易に取得され保持される。また、顔写真データベース（パスポート、運転免許証、拘留者画像）は既に成人人口の90%をカバーしているため、顔認識技術は他の生体認証技術よりも重大な倫理的問題が存在する」としている。
  - 「犯罪とは無関係の一般市民に対して一律に顔照合をかけてよいのか」「スタジアムに入るときに全ての観客が指紋採取をされているようなものではないか」という批判も。
- 自動顔照合は行動の自由を萎縮させる
  - 「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。政府は顔認識を使用して、特定個人の長期的監視を行うことができる。」（MicrosoftのCLO）

２．欧米におけるカメラ・顔認識の規制

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： EUの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： 地方自治体や警察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
  - 監視カメラ行動規範（2013年）： SCCが管轄

- 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： 最近の動向

- 内務省のバイオメトリクス戦略
  - 内務省は2018年6月28日にバイオメトリクス戦略「Biometrics Strategy: Better public services Maintaining public trust」を発行。内務省の取り組みとして以下を実施。
    - 内務省は法執行機関による顔画像と顔認識システムの使用についての検討を整合させるために、新たな監視・諮問委員会を設置。
    - 内務省や警察における新たなバイオメトリック技術の使用、あるいは既存のバイオメトリック技術の新たな適用に先立ち、関係機関に精査を求めながら、データ保護影響評価（DPIA）を実施。
    - 監視カメラコミッショナー（SCC）と連携して、監視カメラ行動規範を改定。
- 内務省の顔画像に関する監視・諮問委員会
  - 2018年7月に、「法執行機関における顔画像および新たなバイオメトリクスの利用に関する監視・諮問委員会」（Law Enforcement Facial Images and New Biometrics Oversight and Advisory Board）が立ち上げられた。
  - 同委員会の目的は、以下について、イングランドおよびウェールズにおける警察機関、並びに内務省およびその傘下機関による法執行目的での開発と利用を検討すること。
    - 顔画像の保存・照合システム
    - DNA、指紋、顔画像以外の新たなバイオメトリクス（音声、虹彩、指静脈、歩容認識を含む）
    - 警察機関が取得した顔画像の他機関との共有

英国： 最近の動向

- エセックス大学による評価報告書
  - 2019年7月に、ロンドン警視庁の自動顔照合（LFR）実証実験に対する批判的な評価報告書を発行。
  - 国内法でLFRを使用するための明示的な許可がないため、裁判所が異議を申し立てた場合、警察によるLFRの展開が違法と判断される可能性が高いと指摘。
  - 監視対象とする人物のリストに掲載される基準も明確ではなく、LFRで特定しようとしていた人々はカテゴリーもばらばらだった。リスト自体も正確さを欠き、すでに裁判が終わっている人物がリストに掲載されている事例もあったとのこと。
- また8月には南ウェールズ警察の自動顔照合（AFR）に対する訴訟の第一審があった。
  - 第一審は合法との判決。
  - 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。適切な状況ではAFRの使用は合法でありうるが、法的枠組みの中で実証的に実施され、良いガバナンスと取組みの正当性を実証しなければならないという確信が高まってきている」という声明を公表。
  - 情報コミッショナー・オフィス（ICO）は10月末に、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。
- キングスクロス駅の事案に対しては情報コミッショナー・オフィス（ICO）が調査を開始。

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、本人の同意なく、意図的に撮影することを犯罪とする。
  - 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。
- 第三者機関
  - 連邦取引委員会（FTC）：
    民間分野における公正な取引（個人データ保護を含む）を監督。
- ガイドライン
  - FTCの顔認識に関するスタッフレポート（“Facing Facts”）
  - 業界団体による自主規制ルール（マルチステークホルダープロセス）

米国： 最近の動向

- 2019年に入ってから、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は顔照合システム「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。

米国： 最近の動向

- 2019年に提出された顔認識技術に関する主な法案
  - 連邦レベル
    - 「Commercial Facial Recognition Privacy Act of 2019」（顔認識技術の商用利用を規制する法案）、
    - 「Transparency in Face Recognition Act of 2019（法案ドラフト）」（連邦政府機関が顔認識技術を利用する際にNISTの顔認識検証テストの実施を義務付けるもの。いまだ法案化されていない模様）
  - 州レベル
    - ワシントン州「Washington privacy act」（商用利用）
    - カリフォルニア州（行政利用：警察官のボディカメラにおける顔認識技術の利用を禁じる）
    - マサチューセッツ州（行政利用）
  - 市レベル
    - カリフォルニア州サンフランシスコ市、同州オークランド市、マサチューセッツ州サマービル市で条例制定
- サンフランシスコ市の顔認識技術禁止条例
  - 2019年5月31日に成立し、6月30日から施行（become effective）されている。警察など市の53の機関での顔認識技術の利用や顔認識技術で取得された情報の利用を禁止する内容であるが、連邦政府の管轄下にある空港や港湾での利用は認めるという。同条例における顔認識技術（face recognition technology）とは、「個人の顔に基づいて個人を識別したり認証（verify）することを支援する自動または半自動のプロセス」を意味し、必ずしも公共空間等でのリアルタイム顔照合技術に限定されない。なお、サンフランシスコ市はこれまで顔認識技術を利用していないという。

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案

- 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）」案を公表した。
- 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案であり、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。
- 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案

- 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。しかし指針案では、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。

- ガイドライン案の第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案

- 顔認識技術の利用に対しては、指針案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。

- ガイドライン案の第77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案

- 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、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。

- ガイドライン案の第80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、個人の身体的特性を検知してカテゴリー分類（属性推定）をするだけであれば、当該処理には第9条は適用されない。

- ガイドライン案の第82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案

- ガイドライン案の第84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案

- 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。

- ガイドライン案の第96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、データ主体は2日後以降に管理者に請求したならば、当該映像は削除されたという情報のみにアクセスできるかもしれない。

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案

- 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。

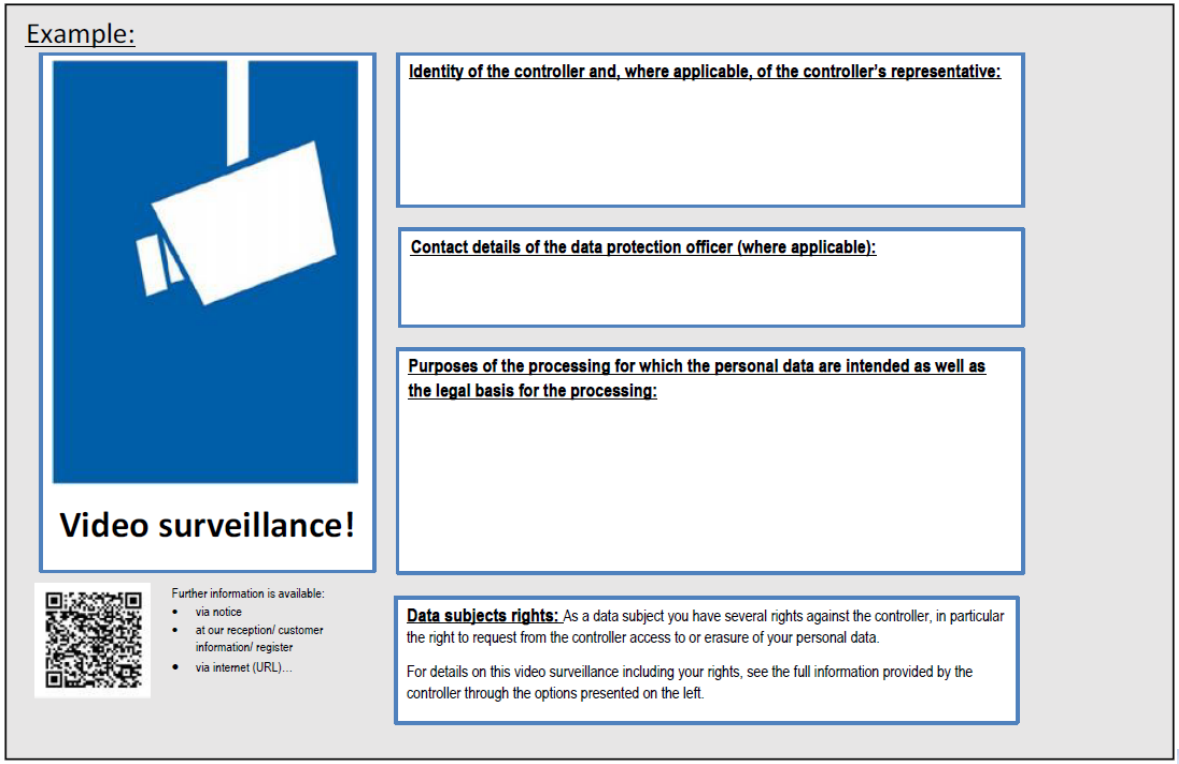
- ガイドライン案の第111条
- 当該情報は、モニターエリアにデータ主体が入る前にビデオサーベイランスの環境について容易に認識できるような態様で、モニターエリアから合理的な距離の位置に設置されるべきである。どのエリアがモニタリングの対象であるかについて疑いがなく、またサーベイランスの文脈が明確なものである限り、ビデオサーベイランスの設備の正確な位置を特定することは必ずしも必要ではない。データ主体は、サーベイランスを回避したり、必要あれば自分の振る舞いを調整したりできるように、どのエリアがカメラで撮影されているかについて想定できなければならない。

- ガイドライン案の第112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案

- ガイドライン案の第113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。

- ガイドライン案の第114条



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案

- 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（個人を一意に識別する目的の場合）「特別な種類の個人データ」であるため、取得に当たって本人の明示的同意が必要（写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： 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案

- ガイドライン案に対し、特に全ての顧客からの本人同意を必須とする法解釈に対しては、日本の電子情報技術産業協会（JEITA）からもパブリックコメントをEU側に提出している（https://home.jeita.or.jp/press_file/20190909170648_4dJDMVL5fG.pdf）。意見の骨子は以下である。
- 同ガイドライン案では、顔特徴データの取得・利用について同意していない利用者からの顔特徴データの取得は、GDPR第9条の特別な種類の個人データの処理に当たるとみなしているため、処理の適法性の根拠として企業側の「正当な利益」を用いることができない。そのため、本人同意を得ない限りはそのような利用者からの顔特徴データの（照合目的のみでの）一時的な取得も違法とみなしている。
- しかし、（同案の74項で規定されているように、）生体データがGDPR第9条の特別な種類の個人データに該当する条件の1つは、「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ことである。しかるに、84項や82項の事例において明示的な同意を得ていない利用者から顔特徴データを取得することは、当該データが顔認識システムに登録されていないことを確認することが目的であり、個人を一意に識別することが目的ではない。したがって、このようなデータは第9条が適用される特別な種類の個人データではなく、一般的な個人データとみなすべきであり、その処理の適法性の根拠としては（GDPR第6条1項(f)の）「正当な利益」を許容するべきである。すなわち、本人同意を得ていない利用者からの顔特徴データの（照合目的での）取得も、「正当な利益」の根拠に基づき許容するべきである。

【ご参考】 欧州委員会AI倫理ガイドライン（2019年4月）

〇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

国連： 監視と人権に関する報告書

- 国際連合（国連）の「意見および表現の自由に関する特別報告者」であるDavid Kaye氏は、2019年6月25日に、監視技術は人権への有害な影響を軽減するための有効な国内的または国際的コントロールが適切に行われるまでは直ちに禁止されるべき（民間企業による監視技術のグローバルな販売や輸出を停止するべき）とする報告書（「Surveillance and human rights」）に関して記者会見を行った。
- 「監視ツールは、プライバシーの権利や表現の自由から、結社・集会の権利、宗教的信条の権利、被差別の権利、国民参加の権利まで、人権に干渉するものとなりうる。監視ツールはいまだ、有効なグローバルまたは国内的コントロールの下にない」という。
- Kaye氏の勧告の中には、各国が個人を不法な監視から保護するために国際的な人権法と合致した国内的な保護措置を採用することが含まれている。とりわけ、Kaye氏は、監視技術の承認と監視を行う公営制度（公営メカニズム）の開発を要請している。さらに、各国は輸出管理を強化するべきであり、また被害者の法的な救済を保証するべきとする。「各国が、監視技術の使用を、最も厳密な種類の監視と承認に服するような、合法的なものに限定すること、また各国が、最も厳格な人権のデューデリジェンスを、監視技術の輸出の必要条件とすることが必須である」という。
- Kaye氏はまた、企業は何らの制約なく活動しているように見えるため、人権に対する責任を遵守するべきだと主張する。企業はデータ移転について開示し、厳格な人権影響評価を実施し、人権規範の遵守を保証できないような国々への移転を回避するべきであるとする。

（出典：http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/41/35、https://news.un.org/en/story/2019/06/1041231）

まとめ

- 近年、海外において公共空間等での自動顔照合システムの導入事例が散見されるようになったが、その先駆けとなっている英国においても、未だ社会的なコンセンサスが十分に取られていない状況。
- 万が一、日本において公共空間での自動顔照合システムを導入するようなことになった場合には、住民のプライバシーへの影響が甚大であるため、大規模イベント時など期間と場所を限定した利用に留めるべきだろう。また、プライバシー影響評価（PIA）等を通じて、事前に住民への周知徹底や社会的コンセンサスの獲得を十分に行なうべき。
- 個人データ保護法制は従来、その国の歴史的文化的背景の違いを受けて各国・地域で異なるものであったが、個人データ越境流通が拡大する中で、基本的な原則は世界的に収斂（convergence）しつつある。顔認識技術に対する規制も、昨今の日EU相互十分性認定やDFFT等の流れを受け、少なくとも日米欧といった先進国のレベルでは徐々に歩みが揃っていくことが予想される。
- 産業界としては引き続き、欧米の規制動向を注視する必要がある。

まとめ：　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照合（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'店舗等での自動顔照合（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

〇小泉　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

y-koizumi@pd.jp.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）
  - 「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