論題 Title	第 4 部　国内動向と政策オプション
他言語論題 Title in other language	Part4 Domestic Trends and Policy Options
著者／所属 Author(s)	大阪大学
書名 Title of Book	生体認証技術の動向と活用：科学技術に関する調査プロジェクト（Current Trends in Biometrics）
シリーズ Series	調査資料 2018-6（Research Materials 2018-6）
編集 Editor	国立国会図書館 調査及び立法考査局
発行 Publisher	国立国会図書館
刊行日 Issue Date	2019-3-29
ページ Pages	103-127
ISBN	978-4-87582-839-6
本文の言語 Language	日本語（Japanese）
キーワード keywords	個人情報保護法、JTC1、SC37、プライバシー影響評価
摘要 Abstract	日本の公的機関による生体認証技術の利用、法規制、社会実装に必要となる国際標準化・ガイドライン策定の動きをそれぞれ取り上げ、政策オプションとしてプライバシー影響評価の導入等を挙げた。

第 4 部
国内の動向と政策オプション

第 4 部　国内の動向と政策オプション

【要　旨】

第 4 部では国内の動向を取り上げた。第Ⅰ章では公的機関による生体認証技術の利用についてまとめた。公的な個人 ID としての指紋の利用を戦前から振り返り、顔写真を組み込んだ IC 旅券とマイナンバーカードを取り上げた。次に、2018 年に主要な国際空港で、パスポート写真との同一性確認を顔認識技術によって行う顔認証ゲートの運用が開始されたが、それに至る 10 年間の試行錯誤をまとめた。近年急速に顔認識技術の精度が改善されたことが分かる。さらに、警察による生体情報の利用について、各モダリティ（指紋・掌紋、DNA、顔、歩容、行動）の現状を整理した。最後に、必ずしも公的機関によるものだけではないが、公共空間で実施される人物行動解析の試みを紹介した。最後の事例はマスメディアで取り上げられたことをきっかけに批判を浴びて中止に追い込まれたケースである。生体認証技術を実社会に適用するためのルールが十分に準備されていなかったことを示している。

第Ⅱ章では、生体認証技術に対する法規制に焦点を当てた。警察による指紋や DNA 型の利用に関する根拠法規と、取得から廃棄に至る運用に関する議論を取り上げた。次に、個人情報保護法が改正され、生体情報が第一号個人識別符号として個人情報の 1 つとして明示されたことを取り上げた。最後に、民間での顔画像と DNA 型の利用に関連する法規制の現状にも触れた。

第Ⅲ章では、生体認証技術を社会実装する上では、法規制の遵守に加えて、自主的な取組が必要であるため、国際標準化の動向や、業界団体や学会によるガイドライン策定の動きをまとめた。技術の進展のスピードが速いため、法規制だけに頼ることは不可能であり、多層のガバナンスが必要になってくる。

これらを踏まえて、第Ⅳ章では、生体認証技術がますます社会に適用され、また、ますます技術が進展することを鑑みて、日本で検討されるべき政策オプションとして、事前にプライバシーへの影響を検討し、対応策をあらかじめ組み込むことができるように「プライバシー影響評価」（PIA）を導入すること、生体認証技術の進展を見据えながら社会実装の動向を監視するための独立の「監督機関」を設置すること、生体認証技術の発展方向と適用ケースを展望し、潜在的なリスクを早い段階で指摘し、対応を促すための「ホライゾン・スキャニング」と「テクノロジーアセスメント」を制度化することを挙げた。

Ⅰ　公的機関による利用動向

1　公的な個人IDとしての利用

生体情報を用いて国民IDシステムを作る試みは、戦前の指紋の「発見」に遡る。1933年に満州国が建国されると、全「満州国民」を指紋によって把握する構想が浮上し、法案も用意されたが、実際には1938年、労働者のみを対象に指紋登録が開始された(1)。戦後にも、1948年に起きた帝銀事件の捜査が難航するなか、警察主導で全国民の十指指紋を登録する構想が浮上した(2)。この問題は国会でも取り上げられたが、全国民への拡大は、当時の予算、人員、技術からして実現可能なものではなかった。その後、警察主導の県民指紋登録が1950～51年に全国各地で開始されていったが、そのほとんどが短期間のうちに姿を消した(3)。しかし、県内の中学3年生を対象とした指紋採取が制度化されていた愛知県だけは、反対運動によって消滅する1970年まで続けられた。他方、外国人に対しては、1952年に施行された「外国人登録法」（昭和27年法律第125号。現在は廃止(4)。）の下で、1955年には「外国人登録法の指紋に関する政令」（昭和30年政令第26号）と「外国人指紋押捺規則」（昭和30年法務省令第46号）が施行され、14歳以上の外国人は原則として左手人差し指の一指指紋の押捺が義務付けられた(5)。1980年代には指紋押捺反対運動が起き、最終的に1999年に指紋押捺制度は廃止された。

米国が査証（ビザ）免除継続の要件として各国に生体認証技術を利用した旅券の導入を求めたことを受け、2005年6月に「旅券法」（昭和26年法律第267号）が改正され、2006年3月20日からIC旅券（バイオメトリック・パスポート）の発給が始まった。旅券冊子中央に非接触IC（集積回路）チップを搭載したプラスチックカードが組み込まれ、ICチップには旅券名義人の氏名、国籍、生年月日、旅券番号等の旅券面情報のほか、旅券発給申請書に貼付された写真から読み取られた顔画像が記録されている(6)。これらの記録事項は、国際民間航空機関（ICAO）が2005年に策定したIC旅券の国際標準において必須と規定されている(7)。2009年12月に犯罪対策閣僚会議で決定された「人身取引対策行動計画2009」(8)では、「我が国の旅券が人身取引の手段として使用されないようにするため、なりすましによる旅券の不正取得や偽変造を含めた旅券の不正行使事案への対策を強化する方法として第二バイオメトリクスを搭載した次世代IC旅券の導入を検討する。」とされ、顔写真に加えて指紋（あるいは虹彩等）も搭載す

＊　本稿におけるインターネット情報の最終アクセス日は2019年1月31日である。

(1)　本節の記述は、以下に基づく。高野麻子『指紋と近代―移動する身体の管理と統治の技法―』みすず書房, 2016.

(2)　同上, pp.164-165.

(3)　犯罪捜査を目的とした指紋採取は、「刑事訴訟法」（昭和23年法律第131号）第218条に規定があるため、それへの抵触を避けるために、あくまでも住民の自発的な活動として位置付けるしかなかった。同上, pp.169-174.

(4)　「出入国管理及び難民認定法及び日本国との平和条約に基づき日本の国籍を離脱した者等の出入国管理に関する特例法の一部を改正する等の法律」（平成21年法律第79号）の施行により、2012年7月9日に廃止された。

(5)　高野　前掲注(1), pp.212-218.

(6)　「平成18年3月20日からIC旅券（パスポート）の申請受付を開始します」2005.12.22. 外務省ウェブサイト <https://www.mofa.go.jp/mofaj/toko/passport/ic_kaishi.html>

(7)　「IC旅券FAQ（よくある質問）」2010.1. 外務省ウェブサイト <https://www.mofa.go.jp/mofaj/toko/passport/ic_faq.html#01>

(8)　「人身取引対策行動計画2009」（平成21年12月22日犯罪対策閣僚会議決定), p.5. 首相官邸ウェブサイト <https://www.kantei.go.jp/jp/singi/hanzai/kettei/091222/keikaku_hon.pdf> ただし、「人身取引対策行動計画2014」（平成26年12月16日犯罪対策閣僚会議決定）ではそのような記述はなくなった。

る可能性が示唆された[9]。

2013年に成立した「行政手続における特定の個人を識別するための番号の利用等に関する法律」（平成25年法律第27号。「マイナンバー法」）により、日本に住民票を有する全ての人が12桁のマイナンバーを持つようになり、マイナンバーの通知後、個人の申請により交付されるマイナンバーカード（個人番号カード）は表面に顔写真を持つ身分証明書として利用できる。マイナンバーカードの申請の際に用いられた交付申請書とそこに添付された顔写真の電子情報は、地方公共団体情報システム機構（J-LIS）[10]において、申請を受理した日から15年間保存され、当該期間経過後に破棄されることになっている。警察から、刑事訴訟法第197条第2項に基づく捜査関係事項照会という形で照会があった場合は、当該情報が被疑事実に直接関係するなど特段の事情がある場合に限って情報提供が行われるとされ、2016年までに顔写真データを含む形で提供した例が1件あったという[11]。

２　出入国時における生体認証の利用

（１）外国人を対象とするもの

「出入国管理及び難民認定法」（昭和26年政令第319号）の2006年（第9次）改正により、2007年11月20日から、「上陸しようとする外国人」は、「入国審査官に対し、（中略）電磁的方式（中略）によつて個人識別情報（指紋、写真その他の個人を識別することができる情報として法務省令で定めるものをいう。以下同じ。）を提供しなければならない。」とされた。すなわち、指紋（原則、両手の人差し指）を指紋読取器の上に置き、電磁的に指紋情報を読み取り、さらに上部にあるカメラで顔写真の撮影を行った上で、入国審査を受けることになった[12]。ただし16歳未満は免除される。取得した個人情報は、「行政機関の保有する個人情報の保護に関する法律」（平成15年法律第58号）に従って、法務省入国管理局により保持される。提供された個人識別情報が過去に日本から強制退去された者などに該当しないか確認し、該当している場合は、入国は認められない。2014年末までに累計5,219人の上陸を阻止したとされる[13]。

内閣に設置された国際組織犯罪等・国際テロ対策推進本部が2015年5月29日に決定した「邦人殺害テロ事件等を受けたテロ対策の強化について」では、「関係省庁との連携の下、顔画像照合機能の活用の強化を検討する。」とされた。これを受けて、法務省は2015年10月に「出

⑼　5年後の2014年には「人身取引対策行動計画2009」のフォローアップが行われ、次世代IC旅券発給に向けた検討（担当：外務省）については、「平成26年度において、日本の旅券の高度化に向けた調査検討関係経費（18百万円）を措置した」とのみ記載された。「「人身取引対策行動計画2009」フォローアップ」2014.12. 内閣官房ウェブサイト <https://www.cas.go.jp/jp/seisaku/jinsin/pdf/jinsinkeikaku2009.pdf> また、この年以降毎年、「旅券の高度化に係る調査一式」という委託事業が外務省より一般競争入札にかけられている。

⑽　「地方公共団体情報システム機構法」（平成25年法律第29号）に基づき、マイナンバー法等に関する事務のほか、地方公共団体の情報システムに関する事務を行うため、地方公共団体が共同で運営する組織として、2014年に設置された。

⑾　第193回国会　参議院総務委員会会議録第13号　平成29年5月16日　p.16.（山下芳生委員の質問に対する山口英樹地方公共団体情報システム機構理事（参考人）の答弁）

⑿　法務省入国管理局「新しい入国審査手続（個人識別情報の提供義務化）の概要について」法務省ウェブサイト <http://www.moj.go.jp/content/000001941.pdf>

⒀　法務省『第5次出入国管理基本計画』2015.9, p.14. <http://www.moj.go.jp/content/001158418.pdf> なお、我が国の「出入国管理及び難民認定法」では、「入国」と「上陸」を区別している。すなわち、「上陸」を日本の領土に立ち入ること、「入国」を本邦つまり日本の領域（領土、領海、領空）に入ることとしている。ただし日本は陸の国境を有していないことから、日本の領土に立ち入るためにはその前に必然的に領海又は領空に立ち入ることになるので、「入国」は日本の領海又は領空に立ち入ることを意味するとされている。多賀谷一照・髙宅茂『入管法大全―立法経緯・判例・実務運用 第1部（逐条解説）』日本加除出版, 2015, pp.1, 33.

入国管理インテリジェンス・センター」を設置し[14]、テロ対策として、国内外の関係機関からテロリスト等の情報・顔画像を収集し、顔画像ブラックリストを作成し、2016年10月17日から入国審査において顔画像照合を実施している[15]。

2018年4月22日、法務省は、東京国際空港（以下「羽田空港」）で日本人の帰国審査に使われている顔認証システムを2019年度から外国人の出国審査に使う方針を固めたと報じられた。また、羽田だけでなく、成田、中部、関西、福岡の各国際空港にも広げる予定である。法務省幹部によると「（これまで）誤認するケースはほとんどない」という[16]。また、プライバシーへの懸念に対しては、顔写真データは、確認が完了すると即座に削除されるという[17]。6月4日、入国管理局は、顔認証ゲートを外国人の出国手続に活用する実地検証を行うと発表し、同日から29日まで、羽田空港中央出国審査場で実施された[18]。

（2）日本人を対象とするもの：顔認証技術の採用が決まるまで

指紋認証を活用して日本人や在留外国人の出帰国手続を迅速化することを目的に、自動化ゲートが2007年11月に日本で初めて成田国際空港（以下「成田空港」）に導入され、その後、中部国際空港（以下「中部空港」）、関西国際空港（以下「関西空港」）、羽田空港に導入され、4空港を合計すると70台（2015年末時点）に増えた。しかし、利用希望者は事前登録の必要があることもあり、2016年時点での利用者はわずか7.9%に留まった[19]。

2010年6月18日に閣議決定された「新成長戦略」[20]で、訪日外国人を2020年初めまでに2500万人まで増加させることとされたことを受けて、法務省は2011年10月14日、有識者による「訪日外国人2500万人時代の出入国管理行政検討会議」を設置した[21]。6回の検討を経て、2012年3月26日には中間報告が発表された[22]。そこでは、日本旅券のICチップ内に顔写真の情報がすでに搭載されていることから、出帰国時の顔写真情報と照合することさえできれば、事前の登録も必要なく、同一人性を確認できるとしたものの、文献調査の結果から、顔認証技術の信頼性については疑問が残ると判断し、実証実験を実施しながら引き続き導入を検討することが望ましいとした。

そこで、法務省は、2012年度に委託調査「バイオメトリクスシステムの処理能力向上に係

---

⑭　「出入国管理インテリジェンス・センターの開設について」2015.9.25. 法務省ウェブサイト <http://www.moj.go.jp/nyuukokukanri/kouhou/nyuukokukanri04_00053.html>

⑮　法務省入国管理局「出入国審査について」（第3回第7次出入国管理政策懇談会資料1）2017.3, p.17. <http://www.moj.go.jp/content/001220308.pdf>

⑯　「出国外国人に「顔認証」　空港審査の人手　テロ対策へ」『読売新聞』2018.4.22, p.1.

⑰　Mizuho Aoki, “Japan to screen departing foreign flyers with facial recognition tech to shorten arrival process,” *Japan Times*, 2018.4.23. <https://www.japantimes.co.jp/news/2018/04/23/national/japan-screen-departing-foreign-flyers-facial-recognition-tech-shorten-arrival-process/>

⑱　「顔認証ゲートの外国人出国手続対応に係る実地検証の実施について」2018.6.4. 法務省ウェブサイト <http://www.moj.go.jp/nyuukokukanri/kouhou/nyuukokukanri07_00169.html>

⑲　法務省入国管理局　前掲注⑮, pp.6-7.

⑳　「新成長戦略―「元気な日本」復活のシナリオ―」（平成22年6月18日閣議決定）首相官邸ウェブサイト <https://www.kantei.go.jp/jp/sinseichousenryaku/sinseichou01.pdf>

㉑　法務省入国管理局「訪日外国人2500万人時代の出入国管理行政検討会議の設置等について」2011.10.14.（国立国会図書館インターネット資料収集保存事業（保存日：2018.10.1.）による）<http://warp.ndl.go.jp/info:ndljp/pid/11165226/www.moj.go.jp/nyuukokukanri/kouhou/nyuukokukanri01_00101.html>

㉒　法務省入国管理局「「訪日外国人2500万人時代の出入国管理行政の在り方に関する検討結果（中間報告）」について」2012.3.26.（同）<http://warp.ndl.go.jp/info:ndljp/pid/11165226/www.moj.go.jp/nyuukokukanri/kouhou/nyuukokukanri01_00107.html>

る調査・研究」[23]において、出帰国審査時に、IC 旅券の顔写真と自動化ゲート通過時に撮影した顔写真を照合する実験を行った。ところが、本人誤拒否率（FRR）[24]が 17.7%（取得時 5.9%、照合時 11.8%）という結果になった[25]。この結果は、2013 年 3 月から開催された「第 6 次出入国管理政策懇談会」において報告され、5 月には 1 年半の議論の結果をまとめた報告書が公表された。そこでは「直ちに顔認証のみによる自動化ゲートを導入することは困難である」とした上で、「法務省において、顔認証の技術的動向を注視しつつ、実証実験の結果を踏まえ、自動化ゲートに顔認証を活用するために解決すべき課題を示して民間事業者の技術開発等を促し、また、入国審査官等人の目による厳格性の確保方策等を引き続き検討し、可能な限り早期に顔認証による自動化ゲートの導入を図ることが望まれる。」とされた[26]。

改善すべき課題としては、①顔認証機器の能力向上、②カメラの位置、照明、背景等の撮影環境の改善、③画像補正ツールを用いた顔写真の傾き補正、④顔写真撮影のための立ち位置、顔の向き等の案内（表示、案内人等）、が挙げられた[27]。

法務省は引き続き、2014 年 8 月から 9 月にかけて成田空港と羽田空港において実証実験を行った[28]。実験参加事業者を公募した結果、5 社が選定された（サクサ、グローリー、日本電気、東芝、パナソニックシステムネットワークス[29]）。実験 1 は、IC 旅券の IC チップから読み出した顔画像と空港内で撮影した顔画像との一対一照合を行うもので、静止撮影（実験 1-1）とウォークスルー撮影（実験 1-2）の 2 通りが実施された。実験 2 は、なりすまし等の不正利用を意図する者を想定したもので、カメラに他人の顔写真を表示させたタブレットを向けたり、ラバーマスクを被ったりした。実験協力者は、実験 1 が（有効データ数で）22,341 人であった。5 社のシステムで、他人誤受入率（FAR）[30]の設定を、1%、0.1%、0.01%、0.001% の 4 通りとして実施された。表 1 に、実験 1-1 で、FAR を 0.001% に設定した最も厳しい場合の本人誤拒否率（FRR）を示す。事業者 A と D の 2 社の FRR が 1% を切った。また、実験 1-2 の方が本人誤拒否率（FRR）は高くなった[31]。

⑵3⑶　「委託調査に係る成果物の概要：バイオメトリクスシステムの処理能力向上に係る調査・研究」法務省ウェブサイト <http://www.moj.go.jp/content/000112236.pdf>　実証実験は次の 3 種類の方法で行われ、延べ約 56,000 人もの人々が参加した。第 6 次出入国管理政策懇談会『訪日外国人 2500 万人時代の出入国管理行政の在り方に関する検討結果（報告）』2013.5.20, p.3. 法務省ウェブサイト <http://www.moj.go.jp/content/000110955.pdf>

本文では①のみを紹介した。

① IC 旅券の顔写真と自動化ゲート通過時に撮影した顔写真との顔認証（事前登録は不要）

② 上記①の顔認証に加え、出国時に自動化ゲートで指紋情報を提供し、帰国時に出国時の指紋との指紋認証を実施（事前登録は不要）

③ 現行と同様の事前登録済み指紋情報との指紋認証を行う自動化ゲートを各審査場に複数台設置

⑵4⑶　（正しい）本人を誤って拒否してしまう確率。

⑵5⑶　なお、「実験 1 の認証の厳格性を米国国立標準技術研究所（NIST）が実施した各社の顔照合エンジンの評価で用いられた値に設定した場合，利用時のエラー率は 7.5%（取得時 2.5%，照合時 5.0%）に減少する。」とされている。第 6 次出入国管理政策懇談会　前掲注⑵3⑶, pp.3-5.（資料）

⑵6⑶　同上

⑵7⑶　同上, p.5.

⑵8⑶　「日本人出帰国審査における顔認証技術に係る実証実験の実施について」2014.7.24. 法務省ウェブサイト（国立国会図書館インターネット資料収集保存事業（保存日：2018.9.1.）による）<http://warp.ndl.go.jp/info:ndljp/pid/11152601/www.moj.go.jp/nyuukokukanri/kouhou/nyuukokukanri04_00042.html>　その募集案内において、実証実験で取得された個人情報について「本実験の実験参加事業者は、本実験結果の検証終了後（平成 26 年 12 月末まで）に消去します。法務省は、本実験結果の検証終了後 5 年間保存した上で消去します」とされた。

⑵9⑶　現在の社名は「パナソニックシステムソリューションズジャパン」。

⑶0⑶　他人を誤って（本人であると）受け入れてしまう確率。

⑶1⑶　出入国審査における顔認証技術評価委員会「日本人出帰国審査における顔認証技術に係る実証実験結果（報告）」2014.11.18, pp.8, 12. 法務省ウェブサイト <http://www.moj.go.jp/content/001140301.pdf>

表1　静止撮影（実験1-1）での本人誤拒否率（FRR）

実験参加事業者名	実験協力者数	他人誤受入率（FAR）を最も厳しくした（0.001%）場合	
		本人誤拒否件数	本人誤拒否率（FRR）
事業者A	5,800	15	0.26%
事業者B	4,132	932	22.56%
事業者C	5,084	350	6.88%
事業者D	3,726	20	0.54%
事業者E	3,599	345	9.59%
合計	22,341	1,662	−

（出典）出入国審査における顔認証技術評価委員会「日本人出帰国審査における顔認証技術に係る実証実験結果（報告）」2014.11.18, p.8. 法務省ウェブサイト <http://www.moj.go.jp/content/001140301.pdf>

実験結果を技術的な観点から評価するために、外部有識者から成る「出入国審査における顔認証技術評価委員会」が設置され[32]、2014年11月18日付けの報告書「日本人出帰国審査における顔認証技術に係る実証実験結果（報告）」が、11月28日開催の第16回「第6次出入国管理政策懇談会」で報告された。報告書には、「実験1-1（静止撮影）については，顔認証技術を日本人の出帰国審査に活用することについて十分可能性があると評価できる。また，実験1-2（ウォークスルー撮影）については，将来的な可能性を感じる結果が得られた。」と記載された[33]。

これを受けた2014年12月の「第6次出入国管理政策懇談会」報告書では、「法務省においては，（中略）顔認証技術の導入について速やかに検討を進めるべきである。」と導入に前向きな結論が書かれた[34]。法務省が2015年9月に策定した「第5次出入国管理基本計画」にも、「顔認証技術の導入について速やかに検討を行っていく。」と記載された[35]。また、2016年3月30日、「明日の日本を支える観光ビジョン構想会議」が発表した観光ビジョンにおいても「日本人の出帰国手続において、世界最高水準の顔認証技術を導入（2018年度以降早期の導入を目指す）」とされた[36]。

（3）日本人を対象とするもの：顔認証の本格実施に至るまで

2016年9月から開始された「第7次出入国管理政策懇談会」において、2017年3月、日本人の出帰国手続への顔認証技術について、2017年度に一部の空港で試行運用、2018年度中に主要空港へ配備するという、具体的なスケジュールが明らかにされた[37]。その際に、委員から寄せられたデータの保管方法についての質問[38]に対して、法務省からは、取得した指紋及

32）「「日本人出帰国審査における顔認証技術に係る実証実験結果（報告）」について」2014.11.18. 法務省ウェブサイト（国立国会図書館インターネット資料収集保存事業（保存日：2018.9.1.）による）<http://warp.ndl.go.jp/info:ndljp/pid/11152601/www.moj.go.jp/nyuukokukanri/kouhou/nyuukokukanri04_00044.html>

33）出入国審査における顔認証技術評価委員会　前掲注31), p.18.

34）第6次出入国管理政策懇談会「報告書「今後の出入国管理行政の在り方」」2014.12, p.24. 法務省ウェブサイト <http://www.moj.go.jp/content/001130126.pdf>

35）法務省　前掲注13), p.35.

36）明日の日本を支える観光ビジョン構想会議「明日の日本を支える観光ビジョン」2016.3.30, p.20. 首相官邸ウェブサイト <https://www.kantei.go.jp/jp/singi/kanko_vision/pdf/honbun.pdf>

37）法務省入国管理局　前掲注15), p.12.

38）市川正司「出入国審査についての質問・意見」（第3回第7次出入国管理政策懇談会資料2）2017.3.3. <http://www.moj.go.jp/content/001220309.pdf>

び顔写真は「個人識別情報システム」（Japan Biometrics Identification System: J-BIS）[39] データベースサーバに保管され、インターネット等の外部の一般回線とは接続されておらず、外部からアクセスできない構造となっていること、また、内部からのアクセスも担当職員に限定し、操作ログの管理などを行っている、と回答した[40]。

入国管理局は、2017年10月18日から顔認証ゲートを羽田空港上陸審査場（日本人の帰国手続）に3台導入した[41]。採用されたのは、パナソニックの社内分社であるコネクティッドソリューションズが新開発した「顔認証ゲート」である[42]。IC旅券のICチップ内の顔画像と顔認証ゲートのカメラで撮影した顔画像を照合して本人確認が行われる。顔写真データは、確認が完了すると即座に削除される[43]。カメラの撮影範囲に顔が収まる必要があるため、利用の条件の1つに、身長が135cm以上であることが挙げられた。

2018年10月1日、入国管理局は、羽田空港の上陸審査場に先行導入していた「顔認証ゲート」を、他の空港に順次導入することを発表した。日本人帰国（上陸審査場）については、成田空港に6月11日（第2及び第3ターミナルビルに15台）と6月18日（第1ターミナルビルに16台）、羽田空港に7月9日（10台）、関西空港に7月23日（12台）、中部空港に7月30日（6台）、福岡国際空港（以下「福岡空港」）に8月9日（5台）、 日本人出国（出国審査場）については、 成田空港に10月3日（第2及び第3ターミナルビルに14台）と10月22日（第1ターミナルビルに16台）、羽田空港に10月31日（13台）、中部空港に11月7日（9台）、関西空港に11月21日（15台）、福岡空港に11月28日（6台）である[44]。パナソニックは法務省が2018年内に5空港へ導入する134台全量を受注、受注額は15億8209万円になった[45]。8月までに帰国審査用に計61台、11月までに出国審査用に計73台を納めた。

3　犯罪捜査

（1）指紋・掌紋

日本では1908年に警察が指紋法を採用し、1911年には警視庁に新設された刑事課の中に、指紋事務を担当する鑑識係が設置された[46]。その後、1924年に、満鉄（南満州鉄道）支配下の

---

(39)　2007年11月20日から、上陸申請手続時の外国人から取得した指紋と顔画像のデータを管理するために運用が開始された。

(40)　「第3回「第7次出入国管理政策懇談会」議事録」法務省ウェブサイト <http://www.moj.go.jp/content/001226639.pdf>

(41)　「平成29年10月から顔認証ゲートの先行運用を開始します。」法務省ウェブサイト <http://www.moj.go.jp/nyuukokukanri/kouhou/nyuukokukanri07_00150.html>　調達は「顔認証ゲートアプリケーションの開発等の請負一式」として総合評価方式で行われ、パナソニックシステムネットワークスが2017年1月12日に落札した。落札価格は2754万円であった。「落札」『官報』号外政府調達48号, 2017.3.13, p.41. <https://kanpou.npb.go.jp/old/20170313/20170313c00048/pdf/20170313c000480041.pdf>

(42)　「法務省様がパナソニックの「顔認証ゲート」を採用」2017.12.15. Panasonic ウェブサイト <https://news.panasonic.com/jp/press/data/2017/12/jn171215-1/jn171215-1.html>

(43)　2017年6月28日に開催された第11回法務省契約監視会議において、顔認証データを後の開発に活かそうとしているのでは、という質問に対して「顔認証の際に撮影した画像については，認証が終われば，その場で直ちに消去することとしているので，データを流用することはできない。」との回答がある。「第11回法務省契約監視会議議事概要」法務省ウェブサイト <http://www.moj.go.jp/content/001237812.pdf>

(44)　法務省入国管理局「顔認証ゲートの運用開始時期（予定）について」2018.10.1. 法務省ウェブサイト <http://www.moj.go.jp/content/001270508.pdf>

(45)　「10年前のパスポート写真でも人物判別、顔認証ゲートが5空港へ　パナソニックが受注」2018.7.8. 日刊工業新聞ニュースイッチウェブサイト <https://newswitch.jp/p/13603>

(46)　高野　前掲注(1), pp.56-59.

撫順炭鉱で、労務管理のために最初の大規模な十指指紋登録を実施した。労働者は採用時に指紋が採取され、その情報は撫順炭鉱内で共有された。

他方、国内では、指紋採取の対象者は禁固刑以上の犯罪の被疑者に限定されており、指紋制度はあまり機能していなかった。戦後、GHQ（連合国軍最高司令官総司令部）の勧告を受けて指紋制度が大きく改革され、対象者が罰金以上の刑に該当する犯罪の被疑者となり、警察署で被疑者の指紋を採取して作成された指紋原紙は、警察庁や都道府県の鑑識課に送付されて、その被疑者の身元や犯罪歴を必ず照会することとなった。照会を受けた鑑識課は、保管資料と対照して該当の有無を回答する。1953年には、逮捕された被疑者全てが対象となり、更に必要な場合には承認を得た上での指紋採取も可能になった。

警察庁では、1982年、コンピュータを使ったパターン認識技術を応用した「指紋自動識別システム」を世界で初めて導入した。さらに1998年には、指紋を短時間で採取できるライブスキャナを導入し、現在では全ての警察署に設置している。2002年からは「掌紋自動識別システム」の運用を開始し、遺留掌紋から犯人を特定する遺留掌紋照合などに活用している。2007年からは「指掌紋自動識別システム」として統合された。

群馬県警察は、認知症などで徘徊し、保護された高齢者の身元特定のために、本人や家族らから同意を得て、高齢者の顔写真や掌（手のひら）の静脈データを事前に登録し、掌静脈認証機器で照合する「徘徊高齢者等事前登録制度における手のひら静脈認証による身元特定実証実験」を2018年3月から開始した[47]。6月末時点で約440件が登録されており、6人の保護につながったという[48]。

（2）DNA

DNA型鑑定は、ヒト身体組織の細胞内に存在するDNA（デオキシリボ核酸）の塩基配列を分析することによって、個人を識別する鑑定法であり、警察では主に、STRと呼ばれる特徴的な塩基配列の繰り返し回数に個人差があることを利用した「STR型検査法」を用いている[49]。警察庁では、犯罪現場に被疑者が遺留した試料のDNA型である「遺留DNA型記録」と、犯罪捜査上の必要があって被疑者の身体から採取された試料のDNA型である「被疑者DNA型記録」を登録・対照する「DNA型データベース」の運用を、2005年から開始した[50]。

犯罪捜査として実施されたDNA型鑑定件数は、2016年度には約30万件に上り、その結果として、「被疑者DNA型記録」を、DNA型データベースに登録された「遺留DNA型記録」と対照して余罪を確定することを目的とした「余罪照会」での一致数は約3,600件、「遺留DNA型記録」をDNA型データベースに登録された「被疑者DNA型記録」と対照して関係者

---

(47)　「静脈認証で認知症患者見守り」『日経産業新聞』2018.3.5, p.4.

(48)　「認知症高齢者の見守り 手のひら静脈で身元特定」『日本経済新聞』（北関東版）2018.6.28.

(49)　2003年8月には、9座位のSTR型とアメロゲニン座位の型を検出するSTR型検査法が導入され、日本人で最も出現頻度が高いDNA型の組合せの場合で、約1100万人に1人という確率で個人識別を行うことが可能となった。なお、アメロゲニン座位は性染色体上にあるため、性別により長さが異なり、その長さの違いを利用して、性別の判定を行う。2006年11月には、6座位を追加された15座位のSTR型とアメロゲニン座位の型を検出するSTR型検査法が導入され、現在、日本人で最も出現頻度が高いDNA型の組合せの場合で、約4兆7千億人に1人という確率で個人識別を行うことが可能となっている。警察庁編『平成20年　警察白書』警察庁, 2008, pp.33-35. <https://www.npa.go.jp/hakusyo/h20/honbun/pdf/20p00300.pdf>

(50)　同上

を割り出すことを目的とした「遺留照会」一致数は約 2,500 件であった[51]。また、2015 年 4 月からは、身元不明死体の身元確認のための「死体 DNA 型記録」と「変死者等 DNA 型記録」が作成され、特異行方不明者[52]の実子や実親の試料から作成した「特異行方不明者等 DNA 型記録」を対照させている。

（3）顔

2008 年度の警察白書は、「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顔画像とを照合し、両者が同一人物であるかどうかを識別するシステム」である「三次元顔画像識別システム」が、「一部の道府県警察で活用されている」と説明している[53]。

東京都では、2006 年に「10 年後の東京」が策定され、掲げられた 8 つの目標を達成するための施策の 1 つに「最先端技術の活用と官民パートナーシップ構築によるテロ対策」が挙げられた。そこでは「三次元顔形状データベース自動照合システムの構築」が主要な事業として取り上げられ、テロリストや指名手配被疑者等の写真のデータベースと、民間の防犯カメラにより撮影された顔画像とを自動照合するシステムを構築して、指名手配被疑者の発見・検挙につなげるとしている。これに対して、民間カメラの映像の目的外使用に当たる可能性、プライバシー侵害、情報漏洩の危険性、特定の人物の行動監視につながる可能性などが指摘されたため、警視庁は都市防犯研究センターに調査を委託した。同センターは学識経験者等から成る「コミュニティカメラシステムに関する調査研究委員会」を設置し、2009 年 12 月に報告書を公表した[54]。報告書は、「管理及び運用基準」と「技術的な側面」について検討した上で、データベースに合致した顔画像以外は瞬時に消去されるために、肖像権やプライバシーの問題はないとして、「テロを起こさせない社会づくり」の一環として「これまでに述べた厳格な運用に努める限りにおいて、妥当かつ必要な施策であると考える。」と結論付けた。しかし、第 3 部で紹介した近年の欧米でのガバナンスを巡る議論と照らし合わせると、情報公開、ステークホルダーの参加、第三者による監督といった点が不足している印象は否めない。本報告書に書かれていた「モデル地区における試験的運用」は、大規模集客施設 1 か所の民間防犯カメラ 20 台を対象に、2011 年 3 月から 2014 年 2 月まで実施されたが、試験的運用の検証結果は東京都公安委員会に報告するのみとされた。また、データベース作成の基準などについて「3 次元顔形状データベース自動照合システム運用要綱」を制定したとされている[55]が、公開されていない。

その後、警視庁が 2016 年 4 月から、逮捕された容疑者の顔を 3 次元で撮影する「3D 顔画像撮影装置」を東京都内にある全 102 の警察署で導入することが 1 月、報道された[56]。2016 年版の警察白書においても、2016 年から「三次元顔画像識別システム」が導入され、防犯カメ

⑸1　警察庁編『平成 29 年　警察白書』警察庁, 2017, pp.97-98. <https://www.npa.go.jp/hakusyo/h29/pdf/pdf/06_dai2syo.pdf>

⑸2　犯罪や事故等に巻き込まれ、生命又は身体に危険が生じているおそれ等のある行方不明者を指す。「行方不明者発見活動に関する規則」（平成 21 年国家公安委員会規則第 13 号）第 2 条第 2 項

⑸3　警察庁編　前掲注⑷9, p.36.

⑸4　都市防犯研究センター「テロ対策へ向けた民間カメラの活用に関する調査研究報告書」2009.12. 警視庁ウェブサイト（国立国会図書館インターネット資料収集保存事業による）<http://warp.da.ndl.go.jp/collections/content/info:ndljp/pid/11236816/www.keishicho.metro.tokyo.jp/kurashi/heion/partner_camera.files/partnar_camera.pdf>

⑸5　平成 25 年東京都議会会議録第 15 号　平成 25 年 11 月 29 日（吉田信夫議員の文書質問趣意書及び同答弁書）<https://www.gikai.metro.tokyo.jp/record/proceedings/2013-4/01.html>

⑸6　「容疑者の顔 3D で撮影　防犯カメラと照合しやすく」『日本経済新聞』2016.1.24, p.31.

ラ等で撮影された画像と比較することがより容易になったとされている。

（4）歩容

2009年、前年に起きた放火未遂事件について、奈良県警察から提供された、犯人の顔は分からないものの歩行する姿が映っていた防犯カメラ映像を、大阪大学八木研究室が解析し、容疑者とされる人物と映像の男は「同一である可能性が高い」との鑑定を行った。これが決め手の1つとなり、犯人が逮捕された[57]。

（5）行動

警視庁は2018年度からパナソニックに委託し、AIを利用した不審者検知システムの開発を進めている。2018年7月20日、警視庁は、7月28日に隅田川花火大会の会場で、警察車両に設置したカメラから見物客を撮影し、不審人物の特定や、置き去りにされた荷物の検出などの実験を行うことを明らかにした[58]。2020年の東京オリンピック・パラリンピック競技大会での実用化を目指しているとのことである。

4　公共空間での行動解析

必ずしも公的機関によるものではないが、公共空間に多数のカメラを配置して、通行する人物の行動を追跡する試みがいくつか行われている。目的として、災害時に備えた人々の移動経路の確認などが挙げられることが多い。同様の技術は、店舗内での来店客の行動の可視化にも用いられている。顔画像は、その個人が誰であるかを特定することなく、目や鼻といった器官の配置等の特徴量データに変換した上で同一性を判断することにより、個人情報を取得しないよう設計されているものも多い。しかし、その中には、広報活動を含めた事前準備が不十分であったために「炎上」した事例もある。代表的な事例として、JR大阪駅ビルにおける「失敗」事例を取り上げる。

情報通信研究機構（NICT）が主体となり、西日本旅客鉄道（JR西日本）及び大阪ターミナルビルの所有する大阪駅ビル「大阪ステーションシティ」内に92台のデジタルビデオカメラを設置して、同所を通行する一般の人を撮影した上、災害発生時等の安全対策への実用に資する人流統計情報の作成が可能か否かを検証する実験が計画された。2014年4月から約2年間の実施が予定されていた。個人情報に該当する撮影画像は、そこから100以上の「特徴量情報」が生成された後、すぐに自動消去される仕組みになっていた。2013年11月25日にNICTから実証実験の実施に関するプレスリリースがあったが[59]、直後はあまり反応がなかった。しかし、12月から1月に各紙で報道されると、NICTやJR西日本に「映りたくないのでカメラの場所を教えて」などの声が数件寄せられたという。2014年3月5日には「監視社会を拒否する会」が「JR大阪駅ビルでの顔認証システム実験の中止を求める」要請書を提出した[60]。3月11日、

57　八木康史「歩く姿で人物を特定する！犯罪捜査に威力を発揮する認証システムを開発」2014.11.10. WAOサイエンスパークウェブサイト <http://s-park.wao.ne.jp/archives/2183>

58　「隅田川花火で不審者検知実験」2018.7.20. 共同通信社ウェブサイト <https://this.kiji.is/393012795677623393?c=39550187727945729>

59　「大規模複合施設におけるICT技術の利用実証実験を大阪ステーションシティで実施」2013.11.25. 情報通信研究機構ウェブサイト <https://www.nict.go.jp/press/2013/11/25-1.html>

60　監視社会を拒否する会「JR大阪駅ビルでの顔認証システム実験の中止を求める」2014.3.5. <http://www006.upp.so-net.ne.jp/kansi-no/opinion/documents/2014-3-5-kikoyosei.pdf>

NICT は最終的に、本実証実験の延期を公表するに至った[61]。

これに対して、外部有識者のみで構成される第三者機関である「映像センサー使用大規模実証実験検討委員会」が設置され、半年の検討を経て、10 月 20 日に報告書が公表された[62]。民法上の適法性について、肖像権とプライバシー権の侵害の有無が検討され、それぞれ「肖像権を侵害するとは認められない」、「利用者のプライバシー権を違法に侵害するとは認められない」とされた。また、「独立行政法人等の保有する個人情報の保護に関する法律」（平成 15 年法律第 59 号。「独立行政法人個人情報保護法」）についても違反していないとの結論となった。その上で、社会の信頼を得るために実施すべき措置が勧告された。これについては第Ⅲ章第 5 節で紹介する。

Ⅱ　法規制の現状

1　生体認証の流れと法規制

生体認証の基本的な流れは、第 1 部第Ⅰ章の図 1 のように、登録フェーズと認証フェーズに分けられる。前者では、何らかのセンサによってデータが取得され、特徴が抽出され、テンプレートが登録される。後者でもまずデータが取得され、特徴が抽出され、得られたテンプレートが、前者と照合（スコア計算）され、何らかの判定が行われる。スマホやパソコンの個人端末での生体認証は、端末内で完結するため、データが端末内できちんと管理されている限り、問題は起こらない。しかし、サーバ側で照合が行われる場合は、生体情報が不正に取得されたり、サーバから情報が漏洩したり、同意なく第三者にデータが販売されたりする可能性があるため、対応が必要である。

民間での生体情報の利用に際しては、プライバシーの保護と個人情報の保護の両面を検討する必要がある。プライバシーの保護については、憲法第 13 条[63] の個人の尊重や幸福追求権と「民法」（明治 29 年法律第 89 号）第 709 条の不法行為法が関係する。プライバシー権はもともと、私生活をみだりに公開されない権利（消極的な権利）と理解されていたが、コンピュータの発展やインターネットの普及に伴い、自己に関する情報をコントロールする権利（積極的な権利）とする学説が見られるようになっている[64]。ただし、プライバシー権の対象となる情報の範囲については論者によって異なり、また、個別ケースにおける被侵害利益の種類と侵害行為の態様の間の利益較量によって許容限界が決まる。他方、個人情報の保護については、「個人情報の保護に関する法律」（平成 15 年法律第 57 号。「個人情報保護法」）が関係する。以下、第 2 節で生体情報と個人情報保護法の関係を、第 3 節で警察による生体情報の利用を、第 4 節で顔画像を、第 5 節で DNA を取り上げる。

⑹1　清嶋直樹「JR 大阪駅ビルの「顔識別」実証実験、プライバシー侵害の懸念から延期」2014.3.11. 日経 xTECH ウェブサイト <https://tech.nikkeibp.co.jp/it/article/NEWS/20140311/542723/>;「大阪ステーションシティでの ICT 技術の利用実証実験の延期について」2014.3.11. 情報通信研究機構ウェブサイト <http://www.nict.go.jp/press/2014/03/11-2.html>

⑹2　映像センサー使用大規模実証実験検討委員会『調査報告書』2014.10.20. 情報通信研究機構ウェブサイト <http://www.nict.go.jp/nrh/iinkai/report.pdf>

⑹3　「第 13 条　すべて国民は、個人として尊重される。生命、自由及び幸福追求に対する国民の権利については、公共の福祉に反しない限り、立法その他の国政の上で、最大の尊重を必要とする。」

⑹4　TMI 綜合法律事務所編『個人情報管理ハンドブック　第 4 版』商事法務, 2018, pp.423-426.

２　個人情報の保護に関する法律

生体認証技術が扱う生体情報は、個人情報保護法[65]において、「個人情報」の１つとされている「個人識別符号」[66]（第２条第２項）の第１号「特定の個人の身体の一部の特徴を電子計算機の用に供するために変換した文字、番号、記号その他の符号であって、当該特定の個人を識別することができるもの」に該当する。これらは「一号個人識別符号」とも呼ばれ、「個人情報の保護に関する法律施行令」（平成15年政令第507号）と、個人情報保護委員会が策定したガイドライン（通則編）[67]で具体的な対象が示されている（表2）。

⑹5　ただし、国の機関は「行政機関の保有する個人情報の保護に関する法律」（平成15年法律第58号）が、独立行政法人は独立行政法人個人情報保護法が、地方自治体はそれぞれの個人情報保護条例が該当する。

⑹6　旧法で扱いが曖昧であった、個人の身体的特徴を変換した符号や個人に割り当てられた番号などを個人情報の１つとして位置付けたものである。

⑹7　個人情報保護委員会「個人情報の保護に関する法律についてのガイドライン（通則編）」2016.11.（2017.3一部改正）<http://www.ppc.go.jp/files/pdf/guidelines01.pdf>

表２　一号個人識別符号を構成する生体情報に関する定義規定等

一号個人識別符号：
特定の個人の身体の一部の特徴を電子計算機の用に供するために変換した文字、番号、記号その他の符号であって、当該特定の個人を識別することができるもの（個人情報保護法第2条第2項第1号）

施行令の規定	ガイドライン（通則編）の記述
細胞から採取されたデオキシリボ核酸（別名DNA）を構成する塩基の配列	ゲノムデータ（細胞から採取されたデオキシリボ核酸（別名 DNA）を構成する塩基の配列を文字列で表記したもの）のうち、全核ゲノムシークエンスデータ、全エクソームシークエンスデータ、全ゲノム一塩基多型（single nucleotide polymorphism: SNP）データ、互いに独立な40箇所以上のSNPから構成されるシークエンスデータ、9座位以上の4塩基単位の繰り返し配列（short tandem repeat: STR）等の遺伝型情報により本人を認証することができるようにしたもの
顔の骨格及び皮膚の色並びに目、鼻、口その他の顔の部位の位置及び形状によって定まる容貌	顔の骨格及び皮膚の色並びに目、鼻、口その他の顔の部位の位置及び形状から抽出した特徴情報を、本人を認証することを目的とした装置やソフトウェアにより、本人を認証することができるようにしたもの
虹彩の表面の起伏により形成される線状の模様	虹彩の表面の起伏により形成される線状の模様から、赤外光や可視光等を用い、抽出した特徴情報を、本人を認証することを目的とした装置やソフトウェアにより、本人を認証することができるようにしたもの
発声の際の声帯の振動、声門の開閉並びに声道の形状及びその変化	音声から抽出した発声の際の声帯の振動、声門の開閉並びに声道の形状及びその変化に関する特徴情報を、話者認識システム等本人を認証することを目的とした装置やソフトウェアにより、本人を認証することができるようにしたもの
歩行の際の姿勢及び両腕の動作、歩幅その他の歩行の態様	歩行の際の姿勢及び両腕の動作、歩幅その他の歩行の態様から抽出した特徴情報を、本人を認証することを目的とした装置やソフトウェアにより、本人を認証することができるようにしたもの
手のひら又は手の甲若しくは指の皮下の静脈の分岐及び端点によって定まるその静脈の形状	手のひら又は手の甲若しくは指の皮下の静脈の分岐及び端点によって定まるその静脈の形状等から、赤外光や可視光等を用い抽出した特徴情報を、本人を認証することを目的とした装置やソフトウェアにより、本人を認証することができるようにしたもの
指紋又は掌紋	（指紋）指の表面の隆線等で形成された指紋から抽出した特徴情報を、本人を認証することを目的とした装置やソフトウェアにより、本人を認証することができるようにしたもの （掌紋）手のひらの表面の隆線や皺等で形成された掌紋から抽出した特徴情報を、本人を認証することを目的とした装置やソフトウェアにより、本人を認証することができるようにしたもの

（出典）「個人情報の保護に関する法律施行令」（平成 15 年政令第 507 号）第 1 条第 1 号 ; 個人情報保護委員会「個人情報の保護に関する法律についてのガイドライン（通則編）」2016.11.（2017.3 一部改正）<http://www.ppc.go.jp/files/pdf/guidelines01.pdf> を基に筆者作成。

これらの個人識別符号は個人情報であり、生体情報は個人情報である。このため、生体情報を取り扱う場合は、個人情報取扱事業者として次のような義務が生じる（表３）。

表３　個人情報取扱事業者に課せられる主な法的義務

・個人情報を取り扱う際にその利用目的をできる限り特定し、目的内で利用する。
・適正な手段で個人情報を取得する。
・あらかじめ本人の同意を得ずに要配慮個人情報を取得してはならない。
・個人情報を取得した場合は、速やかにその利用目的を本人に通知、又は公表する。
・利用目的を変更した場合は、その旨を本人に通知、又は公表する。
・個人データを正確に保ち、不要時には速やかに消去する。
・個人データを安全に管理し、従業員や委託先の監督をする。
・本人の同意を得ずに個人データを第三者提供しない。

（出典）「個人情報の保護に関する法律」（平成 15 年法律第 57 号）第 15 条から第 35 条を基に筆者作成。

生体情報そのものは、原則として取得、取扱いに本人の同意が必要となる「要配慮個人情報」[68]には該当しない。しかし、生体情報は、パスワードなどと異なり、生涯、変更や削除ができないものであるため、漏洩した場合のリスクが大きいこと、さらには、第２部第Ⅳ章で事例を挙げたように、顔画像などの生体情報から、健康状態、感情、人種といったセンシティブな情報が推測され得ることなどを考慮すると、通常よりも慎重な取り扱いが望まれる。また、欧州一般データ保護規則（General Data Protection Regulation: GDPR）[69]では、「自然人を一意に識別することを目的とする生体データ」は、「特別な種類の個人データ」、いわゆるセンシティブデータと分類されており（第３部第Ⅳ章）、本人の同意がない場合は取扱いが原則禁止されている。

３　警察による生体情報の利用

警察による生体情報の利用については、刑事訴訟法第 218 条第３項が「身体の拘束を受けている被疑者の指紋若しくは足型を採取し、身長若しくは体重を測定し、又は写真を撮影するには、被疑者を裸にしない限り、第一項の令状によることを要しない。」としている。この規定を根拠に、「指掌紋取扱規則」（平成９年国家公安委員会規則第 13 号）が定められ、第３条第１項において、警察署長等は、「所属の警察官が被疑者を逮捕したとき又は被疑者の引渡しを受けたときは、指紋記録等及び掌紋記録等（中略）を作成しなければならない。」とされている。また、「被疑者写真の管理及び運用に関する規則」（平成２年国家公安委員会規則第９号）でも、第２条第１項において、警察署長等は「所属の警察官が被疑者を逮捕し、又はその引渡しを受けたときは、画像を電磁的方法により記録することにより当該被疑者の写真（以下「被疑者写真」という。）

[68]　要配慮個人情報は、「本人の人種、信条、社会的身分、病歴、犯罪の経歴、犯罪により害を被った事実その他本人に対する不当な差別、偏見その他の不利益が生じないようにその取扱いに特に配慮を要するものとして政令で定める記述等が含まれる個人情報をいう」（第２条第３項）と定義され、その取得には、特別な場合を除き、あらかじめ本人の同意を得ることが必要とされている（第 17 条第２項）。

[69]　Regulation (EU) 2016/679 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 and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L119, 2016.5.4, pp.1-88. <http://data.europa.eu/eli/reg/2016/679/oj>
日本語仮訳として次がある。「個人データの取扱いと関連する自然人の保護に関する、及び、そのデータの自由な移転に関する、並びに、指令 95/46/EC を廃止する欧州議会及び理事会の 2016 年４月 27 日の規則 (EU) 2016/679（一般データ保護規則）」個人情報保護委員会ウェブサイト <https://www.ppc.go.jp/files/pdf/gdpr-preface-ja.pdf>; <https://www.ppc.go.jp/files/pdf/gdpr-provisions-ja.pdf>

を撮影し、当該被疑者写真及び当該被疑者の氏名、生年月日その他当該被疑者を識別するために必要な事項を電磁的方法により記録したもの（中略）を作成しなければならない。」とされている。これらが、警察が生体情報を取得するための法的根拠となっている。

ただし、前者では同条第 2 項に「警察署長等は、身体の拘束を受けていない被疑者について必要があると認めるときは、その承諾を得て指掌紋記録等を作成するものとする。」、後者でも同条第 2 項に「警察署長等は、身体の拘束を受けていない被疑者について必要があると認めるときは、その承諾を得て被疑者写真を撮影し、被疑者写真記録を作成するものとする。」という規定があり、任意での事情聴取を受けた際にも、多くのケースで指紋、掌紋、顔写真が警察によって取得されていると考えられる。両規則において、指掌紋記録等や被疑者写真記録を保管する必要がなくなったとき、「当該指掌紋記録」や「当該被疑者写真記録」を抹消しなければならないとされているが（それぞれ第 5 条第 3 項、第 5 条）、「死亡したとき」と違って、「保管する必要がなくなったとき」が具体的にどういう場合であるかは明示されていない[70]。防犯カメラや身体装着カメラのライブ映像で自動顔認識システムが利用されるようになると、英国（第 3 部第Ⅱ章）と同様に、照合されるデータベースに含まれる顔写真がどこで取得されたものであるかに関心が寄せられることになるかもしれない。

警察庁による容疑者の DNA 型データベースの運用に関し、新たな立法が必要かという点については、法律専門家等からの問題提起が存在する。その論点は、主に① DNA 型を取得するための試料を容疑者から採取することは適法か、②試料採取が適法である場合でも、DNA 型をデータベース化することまで適法なのかの 2 つに分けることができる。

①の試料採取の適法性については、さらに次の 2 つの場面で論じられる。

1 つ目は、すでに起きた犯罪の捜査の場面で、身体の拘束を受けている被疑者から、指紋等と同様に血液や口腔粘膜の細胞を、令状によらずに採取できるか否かである。指紋同様に採取できる、できないで意見が分かれており[71]、現在も解決が見られないようである。「DNA 型記録取扱規則」（平成 17 年国家公安委員会規則第 15 号）が定められているものの、指紋、掌紋、顔写真と違って、刑事訴訟法の第 218 条第 3 項では DNA には言及されていない。なお、身体拘束をされていない被疑者が、任意で試料を提出することは適法であるが、DNA 型取得のための試料を、本人が知らない間に水を飲んだ紙コップから警察官に取られた[72]、あるいは、拒否したにもかかわらず長時間にわたる説得の末に応じさせられたといった事件が存在する[73]。前者は強制処分に該当し違法であると認定された。後者は、「承諾書」が無効だとする申立が行われた。

2 つ目は、まだ犯罪は起きていない状態で、性犯罪や凶悪犯罪の再犯の防止や、再犯時の速

⑺⓪　なお、被疑者指紋については、警察庁は、採取に瑕疵があれば削除するものの、採取に違法性がなければ、保管が違法になることはないという取得時主義を採用し、無罪判決が確定しても削除は行わないという立場を示している。例えば、田村正博『警察行政法解説　全訂第 2 版』東京法令出版 , 2015, p.340; 第 186 回国会　衆議院内閣委員会議録第 13 号　平成 26 年 4 月 16 日 , pp.19-20. 指紋以外についても、基本的に同様の方針と考えられる。

⑺① 岡田薫「DNA 型鑑定による個人識別の歴史・現状・課題」『レファレンス』660 号, 2006.1, pp.7-31. <http://dl.ndl.go.jp/view/download/digidepo_999857_po_066002.pdf?contentNo=1>

⑺② 久岡康成「警察官らが，被告人に対し，その DNA 型検査の資料を得るため，紙コップを手渡してお茶を飲むように勧め，そのまま廃棄されるものと考えた被告人から同コップを回収し，唾液を採取した行為につき，強制処分に該当するとされた事例」『立命館法學』No.378, 2018, pp.359-383. <http://www.ritsumei.ac.jp/acd/cg/law/lex/18-2/010hisaoka.pdf>

⑺③ 日本弁護士連合会人権擁護委員会「警察における DNA 採取に関する人権救済申立事件調査報告書」2017.4.13. <https://www.nichibenren.or.jp/library/ja/opinion/hr_case/data/2017/complaint_170420.pdf>

やかな犯人逮捕のために、これらの者の出所時に試料を採取してDNA型を取得するという場面である。これについては、日本では、法律上できないことに意見が一致している。そこで、これらの行為をできるようにすべきか（すべきなら当然立法が必要）という議論が存在する(74)。

②は、試料の採取が適法であるとしても、DNA型を取得してデータベースへ登録して保管したり検索したりすることは、必ず適法になるのかという問題である。捜査機関が取得した試料や情報は、広く捜査の目的で利用するのであれば、どのように利用しようと自由であるという考え方で、現在すでに、指掌紋やDNA型がデータベース化されている(75)。しかし、現場の遺留試料がない場合など、DNA鑑定を実施する必要がないときにおいても被疑者のDNA型を取得してデータベースに登録し、余罪を調べる目的やその者が将来罪を犯すと見越して検索可能なようにしておくのは、正当性がないのではないか、ということである(76)。これに関連して、記録の削除に関するDNA型記録取扱規則の規定が不明確という指摘もある。同規則第7条では、「被疑者DNA型記録を保管する必要がなくなったとき」には、被疑者DNA型がデータベースから抹消されることとされている。しかし、この規定は、無罪が確定した場合でもその者の記録を抹消する義務を課すものではなく、個別に判断すると理解されている(77)。また、有罪となった者のDNA型記録についても、抹消せずに登録しておく必要性は明確ではない(78)。

４　顔画像

防犯カメラの映像がデジタル化され解像度が上がったことで、撮影された顔画像の個人識別性が増し、個人情報該当性が当然のように認められるようになってきた。そのため、撮影された映像を取り扱う場合は、先に述べたような、個人情報取扱事業者としての義務が生じる。すなわち、顔認識技術を用いていることと、その目的を通知することが必要になる。公共スペースに設置されたカメラで映像を取得する場合は、撮影される人に100%通知することは困難であるため、どのように、どれくらい通知の努力をすれば十分なのか判断が難しい。ただし、防犯カメラを本来の目的で使う場合は、「取得の状況からみて利用目的が明らかであると認められる場合」(79)とみなせるので、その限りにおいては個別の通知は不要であるとみなすことができる(80)。

生体認証に顔画像が用いられる場合は、プライバシー権だけでなく、肖像権も問題になる。肖像権とは、自己の顔や容姿などの肖像を勝手に撮影されたり、公表されたりするのを禁止することができる権利である(81)。防犯カメラの映像を用いて自動顔認識システムで監視リスト

(74)　岡田　前掲注(71)
(75)　徳永光「立法を伴わない犯罪捜査のためのDNAデータベース」『甲南法学』Vol.46 No.3, 2005.12, pp.115-134. <https://konan-u.repo.nii.ac.jp/?action=pages_view_main&active_action=repository_view_main_item_detail&item_id=622&item_no=1&page_id=40&block_id=38>
(76)　同上, p.127.
(77)　同上, p.123.
(78)　同上, p.124.
(79)　個人情報保護法第18条第4項第4号
(80)　個人情報保護委員会『「個人情報の保護に関する法律についてのガイドライン」及び「個人データの漏えい等の事案が発生した場合等の対応について」に関するQ＆A』2017.2.16（2018.7.20更新）, p.3. <https://www.ppc.go.jp/files/pdf/180720_APPI_QA.pdf>
(81)　村上康二郎『現代情報社会におけるプライバシー・個人情報の保護』日本評論社, 2017, pp.196-197.

と照合するような場合、防犯カメラに適用されてきた許容基準が参考になるだろう。例えば、大阪市西成区の通称「あいりん地区」に警察が設置した15台の防犯カメラの適法性が争われた事件に関する大阪地裁判決[82]では、「その設置・使用にあたっては、①目的が正当であること、②客観的かつ具体的な必要性があること、③設置状況が妥当であること、④設置及び使用による効果があること、⑤使用方法が相当であること、が必要である」[83]とされた。やはり、被侵害権利に対して、その目的が正当であり、便益が十分に大きく、かつ、代替手段がない、などといった評価が必要になるだろう。

5　DNA

DNAによる個人識別の分野では、近年、消費者直販型の遺伝子検査サービス会社による個人鑑定に係る商品が販売されており、倫理的観点からしばしば問題視されている。例えば現在、インターネットショッピングサイトには、父子鑑定、母子鑑定、出生前親子鑑定、浮気鑑定、祖父母孫鑑定、家系図作成といった商品が存在し、誰でも購入できるようになっている。価格帯は1万円台から20万円を超えるものまであり、海外で検査するものと、国内で検査するものとがある。これらのサービスでは、個人情報保護法を遵守しプライバシーは守られるとしている。しかし、これらの検査を購入する側に、周囲に知られずに実子であるか検査したい、浮気をされているか知りたいといった事情がある場合、鑑定当事者間で、検査することについて、そもそも合意がなされていない可能性がある。特に幼児や胎児が検査される場合には、この検査に同意や拒否をする術がない状態であり、検査結果によって子どもや胎児が不利な影響を被ったり、鑑定結果が間違っていたりしたときに、自ら救済を求めることは不可能である。これらの検査によって子の福祉が著しく損なわれる可能性は否定できないため、子の人権保護の観点から、安易な利用を危惧する意見が存在する[84]。

Ⅲ　社会的及び倫理的な取組

生体情報の利用に関しては、法規制に加えて、自主的な取組が行われている。ここでは、カメラを使った顔画像の利用に焦点を当てて、各種団体による自主的な取組をまとめた。

1　国際標準化

生体認証技術の国際標準化は、国際標準化機構（International Organization for Standardization: ISO）と国際電気標準会議（International Electrotechnical Commission: IEC）によって設立された情報技術を対象とする第1合同技術委員会（Joint Technical Committee 1: JTC1）内の専門委員会（Sub Committee: SC）の1つであるSC37（バイオメトリクス）で議論されている。2002年に米国の提

⑻　「警察署が、街頭防犯用の目的で設置した監視用テレビカメラがプライバシーの利益を侵害するとして、撤去が命じられた事例（大阪地方裁判所（平成2年（ワ）第5031号）平成6年4月27日判決）」『判例時報』No.1515, 1995.3.1, pp.116-138.

⑻　映像センサー使用大規模実証実験検討委員会　前掲注⑹, p.23. 同判決では、個別に検討されるべきだとした上で、15台のテレビカメラについて個別に検討され、1台の撤去が命じられた。なお、同事件の控訴審判決（大阪高裁：平成8年5月14日判決）も一審とほぼ同様の内容となっており、また原告、被告双方の上告は棄却されている（最高裁：平成10年11月12日決定）。警備判例研究会編著『警備判例解説集 第4版』立花書房, 2016, p.76; 棟居快行「公道上の監視カメラに文句がいえるか」棟居快行ほか『基本的人権の事件簿―憲法の世界へ―』有斐閣, 1997, pp.94-102.

⑻　大橋範子「遺伝子医療」霜田求編『テキストブック生命倫理』法律文化社, 2018, pp.129-130.

案により設置されたSC37には6つの作業グループ（WG）が設置されている（表4）。SC37の幹事国は米国で、事務局は米国国家規格協会（American National Standards Institute: ANSI）に置かれている。日本の国内専門委員会は、情報処理学会の情報規格調査会に設置され、この構成に対応した6つの小委員会から成る。ただし、カード及び個人識別についてはSC17（カード及び個人識別）で、情報セキュリティについてはSC27（セキュリティ技術）で扱われている[85]。

表４　JTC1 SC37（バイオメトリクス）の構成

WG名	対象
WG 1	バイオメトリック専門用語（Harmonized Biometric Vocabulary）
WG 2	バイオメトリック・テクニカル・インタフェース（Biometric Technical Interface）
WG 3	バイオメトリックデータ交換フォーマット（Biometric Data Interchange Formats）
WG 4	バイオメトリックシステムの技術的実装（Technical Implementation of Biometric Systems）
WG 5	バイオメトリック技術の試験及び報告（Biometric Testing and Reporting）
WG 6	バイオメトリクスに関わる社会的課題（Cross-Jurisdictional and Societal Aspects of Biometrics）

（出典）“ISO/IEC JTC 1/SC 37: Biometrics.” ISO website <https://www.iso.org/committee/313770.html>;「委員会」情報規格調査会ウェブサイト <https://www.itscj.ipsj.or.jp/hyojunka/h_sn_member/h_sn_member_01.html> を基に筆者作成。

社会的側面を扱うWG6からは、2008年に、生体認証技術の商業利用時の社会的な課題を網羅した技術報告書[86]が出版され、その第4章では、法的側面、アクセシビリティ、健康と安全、ユーザビリティ、社会的・文化的・倫理的側面、受容性が採り上げられた。本技術報告書は、2015年に再審議され、内容の妥当性が確認されたために、現在も有効な文書である。アクセシビリティの観点からは、子どもへの配慮[87]や、障害を持つ人たちが使いやすいインクルーシブな設計[88]、モダリティごとの生体認証システムで利用されるシンボルや図記号[89]について標準化が行われている。

２　IoT推進コンソーシアム

IoT推進コンソーシアムは2015年に産官学の協力により設立され、コンソーシアム内の3つの作業グループの1つである「データ流通促進ワーキンググループ」の下に、「カメラ画像利活用サブワーキンググループ」が2016年に設けられている[90]。2017年1月31日、「カメ

(85)　山田朝彦「JTC1における国際標準化」『ITUジャーナル』Vol.46 No.8, 2016.8, pp.7-10. <https://www.ituaj.jp/wp-content/uploads/2016/07/2016_08-02-SpecialJTC11.pdf>

(86)　“ISO/IEC TR 24714-1:2008: Information technology -- Biometrics -- Jurisdictional and societal considerations for commercial applications -- Part 1: General guidance.” <https://www.iso.org/standard/38824.html> ISO規格には、国際規格（IS）、技術仕様書（TS）、公開仕様書（PAS）、技術報告書（TR）の4種類があり、ISとTSは規範的出版物であるが、TRは関連情報やデータ集といった参考出版物という扱いである。

(87)　“ISO/IEC TR 30110:2015: Information technology -- Cross jurisdictional and societal aspects of implementation of biometric technologies -- Biometrics and children.” <https://www.iso.org/standard/53230.html>

(88)　“ISO/IEC TR 29194:2015: Information Technology -- Biometrics -- Guide on designing accessible and inclusive biometric systems.” <https://www.iso.org/standard/45273.html>

(89)　“ISO/IEC 24779-1:2016: Information technology -- Cross-jurisdictional and societal aspects of implementation of biometric technologies -- Pictograms, icons and symbols for use with biometric systems -- Part 1: General principles.” <https://www.iso.org/standard/57379.html>; “ISO/IEC 24779-4:2017: Information technology -- Cross-jurisdictional and societal aspects of implementation of biometric technologies -- Pictograms, icons and symbols for use with biometric systems -- Part 4: Fingerprint applications.” <https://www.iso.org/standard/60477.html> など

(90)　「カメラ画像利活用SWG」IoT推進コンソーシアムウェブサイト <http://www.iotac.jp/wg/data/camera/>

ラ画像利活用ガイドブック ver1.0」[91] が、2018 年 3 月 30 日には適用ケースを増やした ver2.0 [92] が公表された。ただし、ガイドブックは「事業者に対し、その対応を強制するものではない」として任意であることが強調されている。ガイドブック ver2.0 では、カメラで人物の容姿や顔を撮影する際の配慮事項を整理し、6 つの適用ケースを例に解説している（表 5）。撮影した顔画像を、別途あらかじめ保有する特定の顔画像リストと照合するケースはスコープ外である。ガイドブックは最初に、事業者が配慮すべき範囲が、個人情報保護法がカバーしている領域よりもずっと大きいことを確認している。そして、カメラ画像の取得から処理・保存利用、廃棄に至るプロセスで必要となる「配慮事項」を、事前告知時、取得時、取扱い時、管理時に分けて、説明している。例えば、事前告知が求められる内容として表 6 の事項を挙げている。また、基本原則として、データのライフサイクルを定めた上で、リスク分析を行うことが推奨されている。これは後述するプライバシー影響評価（Privacy Impact Assessment: PIA）の実施に該当する。

表５　「カメラ画像利活用ガイドブックver2.0」が取り上げた6ケース

ケース	撮影対象	概要
属性の推定	私的空間に設置されたカメラ（店舗内等）	入店の時点で、画像を取得し、特徴量データ（個人識別符号）を抽出し人物属性を推定した後、速やかに撮影画像と特徴量データ（個人識別符号）を破棄するもの。
人物の行動履歴の生成		空間内を人物等が行動する画像を取得し、座標値を取得し、動線データを生成した後、速やかに撮影画像と特徴量データ（個人識別符号）を破棄するもの。
リピート分析		入店の時点で画像を取得し特徴量データ（個人識別符号）を抽出し、人物属性の推定、及び空間内を人物等が行動する画像を取得し座標値を取得し動線データを生成した後に、速やかに撮影画像を破棄。特徴量データのみ一定期間保持し、同一人物の 2 回目以降の入店の判定キーとする。一定期間中、特徴量データをキーにして、来店履歴、店舗内動線、購買履歴等をひも付けて保存する。一定期間経過後、速やかに特徴量データを破棄するもの。
人物形状の計測	公共空間に向けて設置されたカメラ	通行する人・車等を（特定はせずに）識別し、それぞれの数を計測した後、速やかに撮影画像を破棄するもの。
写り込みが発生し得る風景画像の取得		街中の看板・交通標識、及び道路の混み具合を（特定はせずに）識別し、これらの情報を抽出した後、速やかに撮影画像を破棄するもの。
人物の滞留状況把握	公共空間に準じた場所に設置されたカメラ（駅構内等）	通行する人物を撮影し、アイコン化処理の後、速やかに撮影画像を破棄するもの。

（出典）IoT 推進コンソーシアム・総務省・経済産業省『カメラ画像利活用 ガイドブック ver.2.0』2018.3, pp.5-7. 経済産業省ウェブサイト <http://www.meti.go.jp/press/2017/03/20180330005/20180330005-1.pdf> を基に筆者作成。

⑼1　IoT 推進コンソーシアム・総務省・経済産業省『カメラ画像利活用 ガイドブック ver.1.0』2017.1. 経済産業省ウェブサイト <http://www.meti.go.jp/press/2016/01/20170131002/20170131002-1.pdf>

⑼2　IoT 推進コンソーシアム・総務省・経済産業省『カメラ画像利活用 ガイドブック ver.2.0』2018.3. 同上 <http://www.meti.go.jp/press/2017/03/20180330005/20180330005-1.pdf>

表６　カメラ画像の撮影・利活用において求められる事前告知の内容

・カメラ画像の内容及び利活用目的 ・運用実施主体の名称及び連絡先 ・カメラ画像の利活用によって生活者に生じるメリット ・カメラの設置位置及び撮影範囲 ・カメラ画像から生成または抽出等するデータの概要 ・生成または抽出等したデータからの個人特定の可否 ・生成または抽出等したデータの第三者への提供の可否、及び提供する場合、その提供先 ・データ利活用の開始時期

（出典）IoT 推進コンソーシアム･総務省･経済産業省『カメラ画像利活用 ガイドブック ver.2.0』2018.3, p.21. 経済産業省ウェブサイト <http://www.meti.go.jp/press/2017/03/20180330005/20180330005-1.pdf>

３　電子情報通信学会

電子情報通信学会内の「パターン認識・メディア理解研究会」（Pattern Recognition and Media Understanding: PRMU）において、「画像・映像のプライバシー・イノベーション検討 WG」（IPI-WG）が立ち上げられた。大学等がこのようなデータを扱う場合のデータ取得、手順やデータ管理のガイドライン策定を目指している。2017 年 9 月 12 日に開催された第 16 回情報科学技術フォーラムにおいて、中間報告が行われた。その際に、研究を実施する際に公開すべき「プライバシーポリシー」のひな型（表 7）や、カメラ撮影中の通知を行うためのポスターのひな型が提示された。

表７　画像・映像のプライバシー・イノベーション検討WG中間報告におけるプライバシーポリシーのひな型

	内容
第1条	プライバシーポリシーの目的
第2条	定義（撮影データ、特徴量データ、属性データ、統計データ）
第3条	本研究によって取得する撮影データ
第4条	本研究の目的
第5条	撮影の実施方法
第6条	実施主体の義務
第7条	データ収集管理責任者の義務
第8条	撮影データの管理
第9条	関連法規等の遵守
第10条	個人情報に関するお問い合わせ窓口

（出典）「○○研究プロジェクトに関するプライバシーポリシー（案）」（第 16 回情報科学技術フォーラム「画像・映像のプライバシー・イノベーション検討 WG からの報告～プライバシー問題で炎上せずに研究を進めるための処方箋～」配布資料）, 2017.9.12 を基に筆者作成。

４　日本画像認識協会

2012 年に発足した日本画像認識協会では、「高度な解析ソフトウエアを備えた次世代の防犯カメラと見守りカメラの開発と普及を通して、安心安全社会の実現に寄与すること」を目的に、調査・研究、標準化、認定などの事業を行っている[93]。委員会の 1 つとして「次世代ネットワーク型監視カメラのプライバシー保護研究専門委員会」が設置され、2015 年 9 月に第 1 回監視カメラワーキンググループキックオフミーティングを開催した。10 月には、第 1

[93]「会則」一般社団法人日本画像認識協会ウェブサイト <http://jniaa.com/rules>

回次世代ネットワーク型監視カメラのプライバシー保護研究委員会が開催された。議論を重ねたのち、2017年には「ネットワーク型監視カメラシステムガイドライン」と「ネットワーク型監視カメラシステムの運用・設置ガイドライン」が会員向けに作成された[94]。また、「プライバシー影響評価マニュアル」も会員向けに作成されている[95]。

５　情報通信研究機構（NICT）映像センサー使用大規模実証実験検討委員会の調査報告書

計画されていた実証実験の概要は第Ⅰ章第4節で紹介したとおりである。民法の観点からも、独立行政法人等の保有する個人情報の保護に関する法律の観点からも、法律に違反していないと結論付けられたものの、実証実験の計画が多くの人々に不安を与え、その結果、批判を浴びたことから、実験の手順ややり方に問題があったことは明らかであるとして、次の7項目（表8）の勧告が行われた。

表８　情報通信研究機構（NICT）の映像センサー使用大規模実証実験に対する勧告の概要

・実験手順や実施状況等を定期的に確認し公表すること
・個人識別のリスクを市民に対して事前に説明すること
・撮影を回避する手段を設けること
・映像センサーの存在と稼働の有無を利用者に一目瞭然にすること
・人流統計情報の提供に際しては委託契約又は共同研究契約を締結すること
・安全管理措置を徹底すること
・本実証実験に関して適切な広報を行うこと

（出典）映像センサー使用大規模実証実験検討委員会『調査報告書』2014.10.20, pp.46-50. 情報通信研究機構ウェブサイト <http://www.nict.go.jp/nrh/iinkai/report.pdf> を基に筆者作成。

Ⅳ　今後の政策オプション

生体情報は個人情報であり、削除したり変更したりできないこと、場合によっては生体情報から感情や疾病などのセンシティブな情報を推察できることなどを考慮すれば、通常よりも慎重に取り扱うのが好ましいということは、第Ⅲ章で紹介した各種ガイドラインからもうかがえる。また、プライバシーの概念は、個人情報保護法の改正によって比較的白黒がはっきりするようになった個人情報保護の問題と異なり、生体認証システムの目的と被侵害利益とのバランスによっても、社会のプライバシー意識の変化によっても変化し得る。また、生体認証技術やそこから派生する技術の進展の速度は速く、法規制が十分に追い付けないことは容易に想像できる。そのギャップを補完するために、法的拘束力はないものの、業界団体や学会などがガイドラインや行動規範などを策定している。訴訟が提起され、裁判所によって判例という形での判断が明示されることがない限りは、これらが日本社会における生体認証技術の利用場面におけるルールのデファクトスタンダードとなっていくことが予想される。欧州では近年、「責任ある研究とイノベーション」（Responsible Research and Innovation: RRI）という概念が提唱され、新規技術の研究開発に並行して（あるいは、むしろ先行して）、将来、当該技術が

⑼4　「次世代ネットワーク型カメラのプライバシー保護研究専門委員会資料ダウンロード」同上 <http://jniaa.com/pbldownload>

⑼5　舟橋信「防犯カメラとデジタル・フォレンジック、プライバシー影響評価について」（第462号コラム）2017.5.15. デジタル・フォレンジック研究会ウェブサイト <https://digitalforensic.jp/2017/05/15/column462/>

社会に広まった際に生じるであろう倫理的・法的・社会的課題（Ethical, Legal and Societal Issues: ELSI）を早期に特定し、対処方策を検討することが当たり前のこととなりつつある。

しかし、技術進展の後追いで、ルールを定めるだけではなく、様々な事態に社会として素早く対応するためには、必要なガバナンスの仕組みをあらかじめ検討し、用意しておくことが必要不可欠である。そのためにも、第 3 部で紹介したような、諸外国における、生体認証技術の社会実装に伴う試行錯誤の様子は、日本社会にとっても大いに参考になると考えられる。そのような観点から、以下では考えられるいくつかの政策オプションを紹介する。

1　プライバシー影響評価の導入

プライバシー影響評価（Privacy Impact Assessment: PIA）は主として英米法系の国々において行われてきた[96]。個人情報の収集を伴う情報システムの導入などに当たり、あり得るプライバシーへの影響（リスク）を事前に評価し、プライバシー・バイ・デザイン（Privacy by Design: PbD）[97]概念に基づき、運用面あるいは技術的な対策を実施する一連のプロセスであり、通常、検討の結果は評価書としてまとめられ、公表される。米国では、「2002 年電子政府法」[98] 第 208 条において、連邦政府の行政機関に対して、PIA の実施と公表を義務付けている。オーストラリアでは、PIA の実施は推奨されているが、義務付けではなく、任意である。2018 年 5 月に施行された欧州一般データ保護規則では、後述するように、データ保護影響評価（Data Protection Impact Assessment: DPIA）が義務付けられている。

国内でも、行政機関が、マイナンバーを含む個人情報ファイルを保有、取扱いの変更を行おうとするときには、特定個人情報保護評価という名称の PIA に類似した特定個人情報保護評価が必要となる[99]。これは、個人情報一般を対象とするものではない。

しかし、米国のように PIA の義務付け対象を行政機関とするか、EU のように民間部門も含めたものとするかといった制度設計の議論はあり得るものの、個人情報一般を扱う場合に拡大することは将来的に考えられるオプションであろう。その際に、生体認証技術の大規模な導入は当然、PIA の対象となる。ただし、何をもって「大規模な」と判断するかが問題になるだろう。これは「しきい値判断」と呼ばれる。日本の特定個人情報保護評価では、対象人数が 1,000 人以上で実施が義務付けられている。諸外国では人数だけでなく、質的な情報も考慮されることが多い。欧州一般データ保護規則では、DPIA が求められるのは、データの取扱いが「自然人の権利及び自由に対し高いリスクをもたらすことが予想される場合」（第 35 条第 1 項）のみである[100]。DPIA が特に求められる 3 つの例が挙げられており（第 35 条第 3 項）、その1つに「公衆のアクセス可能な地域で大規模に体系的な監視を行う場合」がある。理由として、データ主体が、個人データが収集されていることに気付かない場合があり、公共の場所だと回避することが個人には不

96　村上　前掲注81，pp.244-251.

97　カナダ オンタリオ州の情報及びプライバシーコミッショナーであった、アン・カブキアン（Ann Cavoukian）氏が 1990 年代に提唱した概念。システムや制度の設計や仕様の段階からプライバシー保護を組み込んでおくという考え方である。PIA とも密接に関係している。

98　E-Government Act of 2002 (P.L.107-347)

99　マイナンバー法第 28 条第 1 項による。

100　Article 29 Data Protection Working Party, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*, WP 248 rev.01, 2007.4.4, p.5. (2017.10.4. Last Revised and Adopted) <http://ec.europa.eu/newsroom/document.cfm?doc_id=47711>　なお、日本語訳として、次がある。個人情報保護委員会訳「データ保護影響評価（DPIA）及び取扱いが 2016/679 規則の適用上、「高いリスクをもたらすことが予想される」か否かの判断に関するガイドライン（仮日本語訳）」p.6. <https://www.ppc.go.jp/files/pdf/dpia_guideline.pdf>

可能な場合があることが挙げられている[101]。また、何が「大規模である」かどうかの判断基準としては、データ主体数、データ量・範囲、期間、地理的範囲などが挙げられている[102]。

2　監督機関の設置

日本では生体認証技術のガバナンスが曖昧であることが度々指摘されている。防犯（監視）カメラについても、自治体ごとに条例や要綱で運用を規定しており、国としてのルールはない。同様に、顔認識技術の利用に関するルールも必ずしも定まっておらず、商業利用や研究利用に関しては業界団体や学会などがルールを提案しているところである。

イングランドとウェールズでは、情報コミッショナーに加えて、「2012 年自由保護法」[103]により、 独立した権限を持つ、 監視カメラコミッショナーと生体認証コミッショナーが任命された。前者は、国家戦略[104]や行動規範[105]、DPIA のガイドライン[106]などを策定している。後者も、年次報告[107]に加えて、 内務省が策定した国家戦略[108]へのコメント[109]を公表するなどしている。ただ、監視カメラコミッショナーが監視カメラを、生体認証コミッショナーは主に DNA と指紋を管理し、また個人データ全体を情報コミッショナーが管轄しているため、顔認識技術については、中心となる監督主体が明確ではなく、3 つの独立コミッショナーがそれぞれ関与する状態になっている。このようなガバナンス上の課題は、今後見直される予定である。

日本でも、生体情報は個人情報である以上、個人情報保護委員会が生体認証技術を所管し、ガイドラインなどでルール策定を主導することはあり得る。しかし、イングランドとウェールズのように、別の独立機関を設置する選択肢もあり得るだろう。その点、スコットランドにお

101　Article 29 Data Protection Working Party, *ibid*, p.9; 個人情報保護委員会訳　同上, p.16.

102　Article 29 Data Protection Working Party, *ibid*, p.10; 個人情報保護委員会訳　同上, pp.17-18; Article 29 Data Protection Working Party, Guidelines on Data Protection Officers ('DPOs'), 2016.12.13, pp.7-8. (2017.4.5. Last Revised and Adopted) <http://ec.europa.eu/newsroom/document.cfm?doc_id=44100>; 個人情報保護委員会訳「データ保護オフィサー（DPO）に関するガイドライン（仮日本語訳）」pp.12-15. <https://www.ppc.go.jp/files/pdf/dpo_guideline.pdf>

103　Protection of Freedoms Act 2012 (2012 c. 9) legislation.gov.uk website <http://www.legislation.gov.uk/ukpga/2012/9/contents/enacted>

104　Surveillance Camera Commissioner, *A National Surveillance Camera Strategy for England and Wales*, 2017.3. <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/608818/NSCS_Strategy_post_consultation.pdf> 本戦略は 2016 年に草稿が公表され、6 週間のコンサルテーション期間を経て公表された。2020 年よりも先を見据えた長期的な目標を示すものであると同時に、急速な技術革新に対応して適宜修正される作業文書としての性格も持つ。戦略は以下の 10 の作業項目に分けられる；標準化と認証、ホライゾン・スキャニング、市民参加、警察、地方自治体、自発的に採用する組織、監視カメラ設置者･製造者、訓練、規制。また、顔認識技術については、継続的に検討すべき課題として言及されている。

105　Home Office, *Surveillance Camera Code of Practice*, 2013.6. <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/282774/SurveillanceCameraCodePractice.pdf>

106　Surveillance Camera Commissioner, *Data protection impact assessment*, 2018.10. <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/750168/Data_Protection_Impact_Assessment_191018.docx>

107　Paul Wiles, Commissioner for the retention and use of biometric material, *Annual report 2017*, 2018.6. <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/714055/CCS207_CCS0518559084-1_Biometrics_Commissioner_s_ARA_FINAL_PRINT_version..pdf>

108　Home Office, *Biometrics Strategy: Better public services Maintaining public trust*, 2018.6. <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/720850/Home_Office_Biometrics_Strategy_-_2018-06-28.pdf>

109　Biometrics Commissioner, "Biometrics Commissioner's response to the Home Office Biometrics Strategy," 2018.6.28. GOV.UK website <https://www.gov.uk/government/news/biometrics-commissioners-response-to-the-home-office-biometrics-strategy>

いて、事実上何もルールがない状態から、コンサルテーションも経て[110]、独立した議会コミッショナーの設置などを含む「生体認証データ法案」を2019年に議会に提出すべく、政府が準備を進めていることは特筆すべきである[111]。

3　ホライゾン・スキャニングとテクノロジーアセスメントの活用

生体認証技術とそれらの派生技術は、特に機械学習の発展を受けて、急速に、発展・普及が進んでいる。特に、顔認識技術とその派生技術については、使い方によっては、プライバシーへ重大な影響を与える可能性がある。

通常、法規制の更新には時間がかかるため、スピードの速い技術革新と法規制枠組みの間のギャップは放っておくと広がっていく一方である。その差がある程度大きくなると、事故や事件につながる場合もある。こうした「法規制ギャップ」（regulatory gap）を早期に見出し、適切な対処をすることは、科学技術イノベーションを進めるためにも不可欠である。法規制ギャップを早期発見し、早期に対処するためのツールとして、ホライゾン・スキャニングとテクノロジーアセスメント（Technology Assessment: TA）を紹介する[112]。これらは欧州諸国では制度化されているケースが少なくないが、日本ではこれまで制度化されていない。

ホライゾン・スキャニングとは、将来の兆候を早い段階で幅広くとらえる活動である。英国政府では、予言を行うのではなく、将来のトレンドに関するエビデンスを体系的に調査することで、政府が、将来起こり得る機会と脅威に十分に備えができているかどうかについて分析することを支援するものとされている[113]。政府主導のホライゾン・スキャニングは，英国、オランダ、カナダ、シンガポールで実施されており、最近は欧州議会科学技術オプション評価委員会（Science and Technology Options Assessment: STOA）[114]もホライゾン・スキャニングを明示的に導入している。欧州議会STOAによるホライゾン・スキャニングでは、技術開発プロジェクトの初期の段階で「STEEPLE分析」が行われる[115]。STEEPLEとは、社会（Social）、技術（Technological）、環境（Environmental）、経済（Economic）、政治（Political）、法（Legal）、倫理（Ethical）の頭文字をつなげたものである（これに人口動態（Demographic）を追加してSTEEPLEDとするものもある[116]）。

---

[110]　“Consultation on enhanced oversight of biometric data for justice and community safety purposes.” Consultation Hub website <https://consult.gov.scot/safer-communities/use-of-biometric-data/>

[111]　Scottish government, *Delivering for Today, Investing for Tomorrow: The Government's Programme for Scotland 2018-19*, 2018.9, p.28. <https://www.gov.scot/binaries/content/documents/govscot/publications/publication/2018/09/delivering-today-investing-tomorrow-governments-programme-scotland-2018-19/documents/00539972-pdf/00539972-pdf/govscot%3Adocument>

[112]　松尾真紀子・岸本充生「新興技術ガバナンスのための政策プロセスにおける手法・アプローチの横断的分析」『社会技術研究論文集』Vol.14, 2017.6, pp.84-94. <http://shakai-gijutsu.org/vol14/14_84.pdf>

[113]　“Horizon Scanning Programme team.” GOV.UK website <https://www.gov.uk/government/groups/horizon-scanning-programme-team>

[114]　STOAの正式名称は、2018年6月に「科学技術の未来のためのパネル」（Panel for the Future of Science and Technology）に変更された。“Minutes: STOA Panel meeting,” 2018.6.14, p.5. European Parliament website <http://www.europarl.europa.eu/cmsdata/151061/STOA%20Panel%20meeting%2014-06-2018%20-%20minutes.pdf>

[115]　Lieve Van Woensel and Darja Vrščaj, “Towards Scientific Foresight in the European Parliament,” In-Depth Analysis (Science and Technology Options Assessment), PE 527.415, 2015.1, pp.15-16. <http://www.europarl.europa.eu/RegData/etudes/IDAN/2015/527415/EPRS_IDA%282015%29527415_REV1_EN.pdf>

[116]　*ibid.*; Centre for Strategic Future and Civil Service College, Singapore, *Foresight: A Glossary*, p.43. <https://www.csf.gov.sg/docs/default-source/default-document-library/csf-csc_foresight--a-glossary.pdf>

テクノロジーアセスメントは、特定の科学技術にフォーカスしたアプローチで、科学技術の潜在的な正と負の社会的影響を予想し、技術開発やその利用についての課題設定や社会の意思決定を支援する活動である[117]。その手法は様々であるが、以下の3つに大きく分けられる。1つ目は、専門家の科学的な分析を主とする伝統的な手法である。2つ目は、ステークホルダーや一般市民の参加により多様な視点や社会的要素を取り込む参加型の手法である。コンセンサス会議、シナリオワークショップ、市民陪審など、様々な形式がある。3つ目は、科学技術の萌芽段階から、研究開発の進展に合わせて影響評価を行い、両者の相互作用により展開していく手法である。テクノロジーアセスメントは、1960年代に米国で始まり、1990年代に入って、英国、ドイツ、フランス、オランダ、スイス、オーストリア等多くの国で行政や議会の中に専門組織が設置されるなど、制度化が進展した。日本でもかつて1970年代、当時の科学技術庁や通商産業省でその必要性が議論され、テクノロジーアセスメント報告書がいくつか作成されたが、制度化されるには至らなかった[118]。しかし、東日本大震災と福島第一原子力発電所事故の直後に策定された「第4期科学技術基本計画」(平成23年8月19日閣議決定)[119]では、「Ⅴ. 社会とともに創り進める政策の展開」の中で、倫理的・法的・社会的課題への対応の1つとして、「国は、テクノロジーアセスメントの在り方について検討するとともに、生命倫理等の問題に関わる先端的な科学技術等について、具体的な取組を推進する。また、政策等の意思決定に際し、テクノロジーアセスメントの結果を国民と共有し、幅広い合意形成を図るための取組を進める。」という文言が挿入された[120]。テクノロジーアセスメントには脚注が付けられ「研究開発の発展段階に応じ、科学技術が社会や国民に与える影響について調査分析、評価を行う活動」と定義された。続く「第5期科学技術基本計画」(平成28年1月22日閣議決定)においても、「第6章　科学技術イノベーションと社会との関係深化」の中で、「社会における科学技術の利用促進の観点から、 科学技術の及ぼす影響を多面的に俯瞰するテクノロジー・アセスメント(中略)を促進する」としている[121]。生体認証技術に限らず、バイオテクノロジーや情報技術の研究開発のスピードがますます速くなる中、同時並行でこうした取組を実施することで、倫理的・法的・社会的な課題を早期に発見し、円滑な社会実装につなげていくことができるものと考えられる。

執筆：大阪大学データビリティフロンティア機構　教授　岸本(きしもと)　充生(あつお)
特任講師　山本(やまもと)　奈津子(なつこ)

⑴17　城山英明ほか「制度化なき活動―日本におけるTA(テクノロジーアセスメント)及びTA的活動の限界と教訓―」『社会技術研究論文集』Vol.7, 2010.3, pp.199-210. <http://shakai-gijutsu.org/vol7/7_199.pdf>

⑴18　吉澤剛「日本におけるテクノロジーアセスメント―概念と歴史の再構築―」『社会技術研究論文集』Vol.6, 2009.3, pp.42-57. <http://shakai-gijutsu.org/vol6/6_42.pdf>

⑴19　『科学技術基本計画』(平成23年8月19日閣議決定)内閣府ウェブサイト <https://www8.cao.go.jp/cstp/kihonkeikaku/4honbun.pdf>

⑴20　同上　p.41. さらに続いて、「国は、東京電力福島第一原子力発電所の事故の検証を行った上で、原子力の安全性向上に関する取組について、国民との間で幅広い合意形成を図るため、テクノロジーアセスメント等を活用した取組を促進する。」(同上, p.41)と書かれた。その後、このような形ではテクノロジーアセスメントは実施されていない。

⑴21　『科学技術基本計画』(平成28年1月22日閣議決定)p.48. 内閣府ウェブサイト <https://www8.cao.go.jp/cstp/kihonkeikaku/5honbun.pdf>