国立国会図書館 調査及び立法考査局

Research and Legislative Reference Bureau
National Diet Library

論題 Title	第 3 部　海外の法規制及び社会動向
他言語論題 Title in other language	Part3 Global Trends in Regulatory Policy and Governance
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	51-101
ISBN	978-4-87582-839-6
本文の言語 Language	日本語（Japanese）
キーワード keywords	生体認証、アメリカ合衆国、英国、オーストラリア、EU、インド、国際連合、UNHCR
摘要 Abstract	米国、英国、オーストラリア、EU、インド及び国際機関を取り上げ、顔認識技術を中心とする、生体認証技術をめぐる法規制や社会の反応に関する最新の動向をまとめる。

第 3 部
海外の法規制及び社会動向

第３部　海外の法規制及び社会動向

【要　旨】

第３部では米国、英国、オーストラリア、EU、インド及び国際機関を取り上げて、顔認識技術を中心とする、生体認証技術をめぐる法規制や社会の反応に関する最新の動向をまとめた。カメラの性能の向上と、機械学習の進展によって、生体認証技術の中でも、顔認識技術の普及が目覚ましいことから、様々な地域で、顔認識技術の利用をめぐって新たなガバナンス上の問題が生じている。

米国では近年、法執行機関が犯罪捜査と国境管理において顔認識技術を積極的に活用している。商業利用に関しては、マルチステークホルダープロセスが実施されたものの、市民団体が離脱し、所期の目的を十分に達成できなかった。連邦政府レベルでは、生体情報を包括的に規制する法規制はまだないが、イリノイ州では生体情報の利用を規制する法律があり、その条項を緩和したい事業者側と維持したい市民団体側の攻防が続いている。カリフォルニア州でも新たに「消費者プライバシー法」が成立し、生体情報が個人情報の１つに位置付けられた。

英国は1990年代以降、監視カメラ大国になったが、近年は、ロンドン警視庁やサウスウェールズ警察が、多数の人が集まるイベントを利用して、自動顔認識システムを精力的に試行している。正確性や適法性をめぐって市民団体から批判がある。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」によって、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置かれた。前者は国家戦略や行動規範を策定している。スコットランドでは、顔認識技術に関して、その利用を規制するルールがほとんど何もない状態から、2015年に問題提起されて以降、急速にガバナンスが整えられつつある。現在、行動規範の策定や、生体認証コミッショナーの設置、それらに必要な立法措置が具体的に議論されている。

オーストラリアでは、近年、パスポートや運転免許証まで含めて顔写真を中心とした生体情報を、連邦政府の中で、また連邦政府と州政府の間で共有するという合意ができあがり、それに基づき、顔認識技術を適用するための法案が審議中である。一部の州政府や市民団体からは、プライバシーへの懸念が表明されている。また、国際空港において、チェックインから搭乗までの手続を顔認証のみで行う実験が行われている。

EUでは2018年に一般データ保護規則（GDPR）が施行され、生体情報は特に慎重な扱いが必要であることが明記された。また、国民IDカードに生体情報を含めるように加盟国に対して提案している。移民の流入という事態を受けて、国境管理において生体情報を利用する動きが進んでいる。移民から生体情報を強制的に取得できる年齢の下限を14歳から６歳に引き下げる案については、子どもの権利の側面から批判もあり審議中である。

インドでは世界最大規模の国民IDシステムに生体情報を含める試みが始まっている。また、行方不明者の捜索にも生体データが利用されている。

国連の持続可能な開発目標（SDGs）では、全ての人に身分証明を提供することが掲げられており、生体認証の利用が検討されている。しかし、生体認証のリスクが便益を上回るとする人道支援団体もある。

Ⅰ　米国

連邦政府レベルでは、生体情報の取得や利用を包括的に規制する法規制はまだなく、法執行機関や民間の利用を制限する規制枠組みも存在しない。しかし、連邦機関は、「2002年電子政府法」において、個人情報の収集・保持・利用などを行う場合、「プライバシー影響評価」（Privacy Impact Assessment: PIA）を実施・公表することが義務付けられている(1)。他方、商業利用については、事業者や消費者団体といった関係者が一堂に集められ、マルチステークホルダープロセスによって行動規範の作成が試みられたが、重要なステークホルダーである市民団体が離脱し、所期の目的が達成できなかった。州レベルでは、イリノイ州が、顔写真を含む生体情報の利用を規制する法律を制定している。カリフォルニア州もそれに続いている。他の州でも生体認証技術を規制する州法の制定の動きが活発化しているが、州ごとのばらつきが懸念されており、連邦法への期待も高まっている。そのような中、Microsoft社のブラッド・スミス（Brad Smith）社長が2018年7月に同社のブログにおいて、自動車や医薬品の安全性に関する連邦政府規制が有益だったように、顔認識技術に対しても連邦政府規制が必要であると主張したことも話題になった(2)。

1　犯罪捜査

司法省（U.S. Department of Justice）の連邦捜査局（Federal Bureau of Investigation: FBI）では、刑事司法情報部（Criminal Justice Information Service: CJIS）が1999年から、指紋をコンピュータで自動検索できる「統合自動化指紋個人識別システム」（Integrated Automated Fingerprint Identification System: IAFIS）を運用していた。それに代わるデータベースとして、「次世代個人識別」（Next Generation Identification: NGI）プロジェクトを進め、2011年2月から利用を開始している(3)。

＊　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)　2002年電子政府法（E-Government Act of 2002, P.L.107-347）第208条による。国土安全保障省については、「2002年国土安全保障法」（Homeland Security Act of 2002, P.L.107–296）第222条にも関連規定がある。PIAの目的は、①プライバシー侵害のリスクを評価し、リスクの低減に有効な情報を見出し、事前の対策を促すこと、②国民への説明責任を果たすことである。米国では、連邦機関が個人情報の収集・保持・利用などを行う場合、最初に、プライバシーしきい値分析（Privacy Threshold Analysis: PTA）を実施し、PIAの必要性の有無を判断する。PIAが必要であると判断した場合は、当該連邦機関はPIAを実施し、内部レビューを経て、大統領府の行政管理予算局（Office of Management and Budget: OMB）に提出する。PIAの結果は原則公開される。システムの見直し等により、個人情報の取扱いを変更する場合は、その都度、更新が必要となる。2002年電子政府法を受けて、OMBが作成した指針は、①個人が特定できる形で情報を収集、保持、又は発信する情報技術を開発又は調達する場合、又は②10人以上に対して個人が特定できる形で新たに電子的に情報収集を始める場合に、連邦省庁が、PIAを実施することを義務付けている。指針では、PIAが言及すべき事項について次の7点を挙げている。①どのような情報が収集されるのか（例：性質や情報源）、②その情報が収集される理由は何か（例：適格性を判断するため）、③その情報の利用目的（例：既存データの検証のため）、④その情報を誰と共有する予定であるか（例：特定のプログラム目的で省庁と）、⑤個人が（情報提供が任意の場合）情報の提供を拒否する、あるいは、（義務付けられる、又は権限を与えられた用途以外で）情報をある用途に利用することに同意するために、どのような機会を持っているか、また個人がどのように同意を与えることができるか、⑥その情報はどのような技術や手続で安全に保管されるのか、⑦「1974年プライバシー法」（Privacy Act of 1974, P.L.93-579) (5 U.S.C. §552a)）の下で、記録システム（System of Records: SoR）が作成されるかどうか。“OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002,” M-03-22, 2003.9.26. Archived Obama White House website <https://obamawhitehouse.archives.gov/omb/memoranda_m03-22>

(2)　Brad Smith, “Facial recognition technology: The need for public regulation and corporate responsibility,” 2018.7.24. Official Microsoft Blog <https://blogs.microsoft.com/on-the-issues/2018/07/13/facial-recognition-technology-the-need-for-public-regulation-and-corporate-responsibility/>

(3)　“Next Generation Identification (NGI).” FBI website <https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/ngi>

NGI には、指紋は「先進指紋個人識別技術」（Advanced Fingerprint Identification Technology: AFIT）として、さらに、掌紋が「全国掌紋システム」（National Palm Print System: NPPS）として、虹彩は「虹彩認識」（Iris Recognition: IR）として、そして顔は「州間写真システム」（Interstate Photo System: NGI-IPS）として含まれている。顔認識のためのデータベースである NGI-IPS は、2011 年からパイロット版の運用が開始され、2015 年から本格運用されている。NGI-IPS は、連邦、州、地方自治体の法執行機関から FBI に提出された 2500 万件近い犯罪者の顔写真（「マグショット」という。）からなる顔写真データベースである。CJIS では、「顔分析・比較・判定（Facial Analysis, Comparison, and Evaluation: FACE）業務ユニット」(4) が、NGI-IPS についての顔識別検索を行っている (5)。また、2016 年には FBI が 43 万人分の虹彩情報を収集していることが報道された (6)。

2016 年 5 月、政府アカウンタビリティ局（Government Accountability Office: GAO）(7) は、2015 年末時点で 16 の州が FBI と覚書を交わし、運転免許証や身分証（ID）カード (8) の写真を顔認識技術のために提供していることを上院司法委員会の「プライバシー・技術・法律小委員会」に報告した (9)。その結果、犯罪捜査のために 3000 万件を超える写真の検索が可能になっているとされた。さらに、2016 年 10 月、ジョージタウン大学ロースクールのプライバシー・技術センター（Center on Privacy and Technology at Georgetown Law）が、少なくとも 26（潜在的には 30 に上る）州の法執行機関が運転免許証や ID カードの写真の検索を認められており、すでに 1 億 1700 万人の成人、すなわち米国の成人の 2 人に 1 人が法執行機関による顔認識ネットワークに含まれていると推計されることを指摘した (10)。これらを受けて、顔認識技術の現状を把握し、法規制の必要性を判断することを目的として、2017 年 3 月 22 日に下院の「監視と政府改革に関する委員会」が公聴会を開催した (11)。公聴会を受けて、FBI と覚書を交わしている 18 の州の覚書が公聴会のウェブサイトに掲載された。

国土安全保障省（Department of Homeland Security: DHS）では、生体情報識別管理局（Office of

(4)　“Law Enforcement’s Use of Facial Recognition Technology,” 2017.3.22. FBI website <https://www.fbi.gov/news/testimony/law-enforcements-use-of-facial-recognition-technology>

(5)　“Privacy Impact Assessment for the Next Generation Identification (NGI) Interstate Photo System,” 2015.9. FBI website <https://www.fbi.gov/services/information-management/foipa/privacy-impact-assessments/interstate-photo-system>

(6)　Colin Lecher and Russell Brandom, “The FBI has collected 430,000 iris scans in a so-called 'pilot program',” 2016.7.12. The Verge website <https://www.theverge.com/2016/7/12/12148044/fbi-iris-pilot-program-ngi-biometric-database-aclu-privacy-act>

(7)　「会計検査院」と訳されることもある。

(8)　米国では、主に州政府が発行する運転免許証が身分証明に用いられている。運転免許証を持たない市民には、運転免許証と同様に写真付きの ID カードが申請に基づき交付されている。

(9)　顔写真は、犯罪者のものと一般市民のものからなる。U.S. Government Accountability Office, *Face Recognition Technology: FBI Should Better Ensure Privacy and Accuracy*, GAO-16-267, 2016.5. <https://www.gao.gov/assets/680/677098.pdf>　なお、GAO は、2017 年 3 月、再び報告書を公表し、先の報告書で GAO が FBI と司法省に提示した 6 つの勧告のうち、監査の実施など 3 つについて対応を行ったと評価した。U.S. Government Accountability Office, “Face Recognition Technology: DOJ and FBI Need to Take Additional Actions to Ensure Privacy and Accuracy,” GAO-17-489T, 2017.3.22. <https://www.gao.gov/assets/690/683549.pdf >

(10)　Clare Garvie et al., *Perpetual Line Up: Unregulated Police Face Recognition in America*, Center on Privacy and Technology at Georgetown Law, 2016.10. <https://www.perpetuallineup.org/sites/default/files/2016-12/The%20Perpetual%20Line-Up%20-%20Center%20on%20Privacy%20and%20Technology%20at%20Georgetown%20Law%20-%20121616.pdf>

(11)　“Committee to Review Law Enforcement's Policies on Facial Recognition Technology,” 2017.3.22. United States House Committee on Oversight and Government Reform website <https://oversight.house.gov/legislation/hearings/full-committee-hearing-law-enforcement-s-use-of-facial-recognition-technology>

Biometric Identity Management: OBIM）[12]が生体認証システムの管理運用を担当し、米国政府内で最大の生体情報データベースである「IDENT」（自動生体識別システム）を保持している[13]。IDENTは2億人以上の固有のIDを保有し、1日に30万以上の生体情報を処理しており、国防総省や司法省と相互運用されている[14]。

またDHSは、IDENTに代わる次世代の生体情報データベースとして「国土先進認識技術」（Homeland Advanced Recognition Technology: HART）を開発中である。HARTは少なくとも7種類の生体情報（顔、声、タトゥー、DNA、傷痕、その他の「身体的な記述子」（physical descriptors）を含む）を網羅するもので[15]、将来的に5億人以上（外国人も含む）がデータベースに登録されると予想されている[16]。2021年の完全実施に向けて、4段階で導入していくことになっている[17]。2019年初頭から第1段階としての使用を開始する予定である。また、2019年には虹彩と顔の照合能力を持つことを予定している。

地方自治体レベルでは、2001年にフロリダ州のタンパ警察（Tampa Police Department）が初めて、既存の36台の監視カメラに顔認識技術を組み込み、「スマートCCTV」[18]実験を試行したが、2年間の間に1度も容疑者の特定が行えなかったことから、2003年8月に打ち切られた[19]。その後は、州や地方自治体による顔認識技術を利用したカメラの導入は進展しなかったが、顔認識技術の急速な発展に合わせて近年再び注目されている。

2018年5月22日、米国自由人権協会（American Civil Liberties Union: ACLU）の北カリフォルニア支部がブログにおいて、Amazon社が「Rekognition」[20]と呼ばれる顔認識ソフトウェア

⑿　OBIMは2013年3月にDHS内に設置された。それ以前は、2004年に開始された出入国システムである「米国渡航者及び移民状況特定技術」（United States Visitor and Immigration Status Indicator Technology: US-VISIT）プログラムを通して、同省傘下の税関・国境取締局（Customs and Border Protection: CBP）が生体情報を収集していた。さらに、「2018年サイバーセキュリティ・インフラセキュリティ庁法」（Cybersecurity and Infrastructure Security Agency Act of 2018; P.L.115-278）によって、OBIMは旧国家保護・プログラム総局（NPPD）からDHS管理総局（Management Directorate）に移管された。“Office of Biometric Identity Management,” 2018.11.18. DHS website <https://www.dhs.gov/obim>

⒀　米国連邦政府の主要な生体情報データベースとして、DHSのOBIMが保持しているIDENT、司法省のFBIが保持しているNGI、そして国防総省の保持している海外の容疑者データベースABIS（Automated Biometric Identification System）の3つがある。FBIは、3つ全てにアクセスできる。DHS内でも、税関・国境取締局は3つとも使用できるが、運輸保安局（Transportation Security Administration: TSA）はIDENTのみにしかアクセスできない。

⒁　“Biometrics,” 2017.2.6. DHS wesbite <https://www.dhs.gov/biometrics>; *NPPD at a Glance: Biometric Identity Management*, 2018.2.13. *idem* <https://www.dhs.gov/sites/default/files/publications/nppd-biometric-identity-management-02132018-508.pdf>

⒂　Dan King, “The government's creepy obsession with your face,” *The Week*, 2018.6.18. <http://theweek.com/articles/779196/governments-creepy-obsession-face>

⒃　Glyn Moody, “DHS expanding national biometrics database to hold details on over 500 million people, including many US citizens,” 2017.10.31. Privacy News Online website <https://www.privateinternetaccess.com/blog/2017/10/dhs-expanding-national-biometrics-database-hold-details-500-million-people-including-many-us-citizens/>

⒄　以下、HARTについて、次を参照した。Jennifer Lynch, “HART: Homeland Security's Massive New Database Will Include Face Recognition, DNA, and Peoples' “Non-Obvious Relationships”,” 2018.6.7. Electronic Frontier Foundation website <https://www.eff.org/deeplinks/2018/06/hart-homeland-securitys-massive-new-database-will-include-face-recognition-dna-and>

⒅　CCTV（Closed-circuit Television）とは、もともとは文字どおり、回路が閉じているカメラを指していた。近年は一般に監視カメラを指すことが多い。

⒆　イーバー（Ybor）市の2つの大通りで実施され、Visionics Corporation社の顔認識技術「FaceIt」が利用された。詳しくは、次を参照。Kelly Gates, “The Tampa “Smart CCTV” Experiment,” *Culture Unbound: Journal of Current Cultural Research*, Vol.2, 2010.6, pp.67-89. <http://www.cultureunbound.ep.liu.se/v2/a05/cu10v2a5.pdf>

⒇　“Amazon Rekognition.” Amazon Web Services website <https://aws.amazon.com/rekognition/>

を地方自治体の法執行機関に売り込んでいることを取り上げるとともに[21]、41団体の連名で、Amazon社の最高経営責任者であるジェフ・ベゾス（Jeff Bezos）氏宛てに公開書簡を送り、警察機関に顔認識システムを売り込むことをやめるように要請した。オレゴン州のワシントン郡保安局（Washington County Sheriff's Office）やフロリダ州のオーランド市警察（Orlando Police Department）が2017年以来、顧客となっていることも指摘された。これに対して直ちに、2人の連邦議会下院議員からAmazon社に更なる情報公開を求める書簡が送付された[22]。Amazon社は、6月1日、ブログに回答を寄せ[23]、Rekognition自体は2016年から提供していること、同様のサービスはAmazon社以外からも多く提供されていること、Rekognitionについて法執行機関での濫用は報告されていないこと、利用規約（Acceptable Use Policy: AUP）を持っていること、などを指摘した上で、責任ある利用を通して、Rekognitionを使用することの便益がリスクを上回っていると主張した。その後も、Amazon社の株主[24]や従業員[25]から、法執行機関への販売を中止することを求める書簡が送付された。また、2018年6月、オーランド市と同市警察は、警察本部内の5台のカメラと、ダウンタウンの3台のカメラにRekognitionを導入し、7人の有志職員の顔との照合を試行したことを明らかにし[26]、試行はすでに終了したが、将来の実施については議論と評価を継続するとした[27]。

ACLUは続いて、2018年7月26日、Amazon社のRekognitionを使って（かかった費用は約12ドル）、米国連邦議会上院と下院の535人の全議員の顔写真を、誰でも利用できる25,000人の犯罪者の顔写真（マグショット）データベースとAmazon社の初期設定で照合した結果、議員28人を誤認識したと発表した[28]。有色人種の議員の比率は20%であるのに、誤認識した28人の議員のうち11人（39%）を占めた。同日午後、誤認識された3人の民主党議員は、ベゾス氏に書簡を送り、以下の7項目の質問・要望に対して8月20日までに回答するよう要請した[29]。

---

(21)　Matt Cagle and Nicole A. Ozer, "Amazon Teams Up With Law Enforcement to Deploy Dangerous New Face Recognition Technology," 2018.5.22. American Civil Liberties Union of Northern California website <https://www.aclunc.org/blog/amazon-teams-law-enforcement-deploy-dangerous-new-face-recognition-technology>

(22)　ACLUのブログ記事の3日後に、2人の下院議員が12項目の質問をベゾス氏宛に送付した。Keith Ellison and Emanuel Cleaver, II, [Letter to Jeffrey P. Bezos] 2018.5.25. <https://www.documentcloud.org/documents/4484636-Ellison-Cleaver-Letter-to-Jeff-Bezos.html#document/p1>

(23)　Matt Wood, "Some quick thoughts on the public discussion regarding facial recognition and Amazon Rekognition this past week," 2018.6.1. AWS Machine Learning Blog <https://aws.amazon.com/jp/blogs/machine-learning/some-quick-thoughts-on-the-public-discussion-regarding-facial-recognition-and-amazon-rekognition-this-past-week/>

(24)　Jeremy B White, "Amazon shareholders demand company stop selling facial recognition technology to governments," *Independent*, 2018.6.18. <https://www.independent.co.uk/news/business/amazon-recognition-shareholders-jeff-bezos-letter-privacy-surveillance-facial-recognition-a8405221.html>

(25)　Kate Conger, "Amazon Workers Demand Jeff Bezos Cancel Face Recognition Contracts With Law Enforcement," 2018.6.21. Gizmodo website <https://gizmodo.com/amazon-workers-demand-jeff-bezos-cancel-face-recognitio-1827037509>

(26)　Ryan Gillespie and Gal Tziperman Lotan, "Downtown Orlando has 3 Amazon facial-recognition cameras, police chief says – contrary to earlier claim," *Orlando Sentinel*, 2018.5.24. <https://www.orlandosentinel.com/news/breaking-news/os-amazon-orlando-police-cameras-downtown-20180524-story.html>

(27)　Scott Powers, "Orlando ends use of facial recognition software," 2018.6.25. Florida Politics website <http://floridapolitics.com/archives/267203-orlando-ends-use-of-facial-recognition-software>

(28)　Jacob Snow, "Amazon's Face Recognition Falsely Matched 28 Members of Congress With Mugshots," 2018.7.26. American Civil Liberties Union website <https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28>

(29)　Edward J. Markey et al, [A Letter to Mr. Jeffery Bezos], 2018.7.26. Edward J. Markey (United States Senator) website <https://www.markey.senate.gov/imo/media/doc/Amazon%20Facial%20Recognition%20Tech.pdf>　ただし、これに対する回答は公開されていない。

表1　Amazon社のRekognitionに関するベゾス氏への民主党連邦議会議員の質問・要望事項

・Rekognitionについて内部で実施された正確性やバイアスの評価結果の詳細 ・Rekognitionの利用に関して接触した、あるいは、現在利用している全ての法執行機関及びインテリジェンス機関のリスト ・Rekognitionを利用した又は利用している法執行機関が、不法又は差別的な警察活動に従事したとして、調査・提訴・非難された事例 ・無実の市民の生体データを削除するなど、市民のプライバシー権を保護する仕組み ・13歳未満の子どもの生体データを含んでいるか否か、もし含まれている場合、子どものプライバシー保護を確保する仕組み ・法施行機関のRekognition利用について、濫用や差別につながるような利用がないかどうかAmazon社が監査を実施しているか ・身体装着カメラや公共空間の監視カメラシステムに統合されているか、もし統合されている場合、当該組織名

（出典）Edward J. Markey et al, [Letter to Mr. Jeffery Bezos] 2018.7.26. Edward J. Markey (United States Senator) website <https://www.markey.senate.gov/imo/media/doc/Amazon%20Facial%20Recognition%20Tech.pdf> を基に筆者作成。

また翌日の7月27日には、3人の連邦上院議員が、39の法執行機関に対して、顔認識技術の利用の有無、濫用や誤用を防ぐための対策、利用目的や場面、参照しているデータベース、監査の有無とその結果、購入先、公共空間での利用やリアルタイムでの利用の有無などについての10項目の質問について9月12日までに回答を求める書簡を送付した[30]。また、7月31日には、5人の民主党議員らがGAOに書簡を送付し、FBI等の法執行機関による顔認識技術の利用や起こりうる誤用・濫用に関する調査を依頼した[31]。依頼項目は大きく3つに分かれ、1つ目は、州、地方、連邦のどの法執行機関がどのように顔認識技術を利用しているのか実態調査をしてほしいということ、2つ目は、顔認識技術を販売している営利主体が販売先の使い方の監査を適切に行っているかどうか調査してほしいということ、3つ目はアルゴリズムを訓練するために使用する顔写真データはどこから入手しているのか、それらを購入できる市場があるのかどうか調査してほしい、というものであった。

他方、2018年6月28日にメリーランド州の州都アナポリスで、日刊紙キャピタル・ガゼットの編集室を襲った銃撃事件の容疑者が自分の氏名を明かすことを拒んだため、メリーランド警察は顔認識技術を用いて、本人の顔を、運転免許証と勾留時の顔写真のデータベースと照合することで本人を特定したと報じられた[32]。本人特定に要する時間が大幅に節約できたことが強調されているが、ちょうど法執行機関による一般人をも対象とする顔認識技術の利用の是非が議論になっている最中であったために、賛成派からも反対派からも注目された。

2　国境管理

国境管理には、DHS内の税関・国境取締局（Customs and Border Protection: CBP）、移民・税関執行局（Immigration and Customs Enforcement Bureau: ICE）、運輸保安局（Transportation Security

[30] Wyden, Booker, "Markey Question 39 Federal Law-Enforcement Agencies About Facial Recognition Policies," 2018.7.27. Ron Wyden (United States Senator) website <https://www.wyden.senate.gov/news/press-releases/wyden-booker-markey-question-39-federal-law-enforcement-agencies-about-facial-recognition-policies>

[31] Dell Cameron, "U.S. Lawmakers Call for Investigation Into Use and Abuse of Face Recognition Tech," 2018.7.31. Gizmodo website <https://gizmodo.com/u-s-lawmakers-call-for-investigation-into-use-and-pote-1828009886>

[32] Cade Metz and Natasha Singer, "Newspaper Shooting Shows Widening Use of Facial Recognition by Authorities," *New York Times*, 2018.6.29. <https://www.nytimes.com/2018/06/29/business/newspaper-shooting-facial-recognition.html>

Administration: TSA）が関わっている。1996 年に成立した「1996 年不法移民改革及び移民責任法」[33] がその第 110 条において、米国を訪問する外国人の入国と出国の記録を照合でき、在留期限を超えてオーバーステイ（不法滞在）となった者を特定できるように、「自動化された入国・出国管理システム」（Automated entry-exit control system）の開発を義務付けた。その後、2001 年の米国同時多発テロ事件を受けて 2004 年に制定された「情報活動改革テロ予防法」[34] は、DHS 長官に対して、「自動化された生体情報に基づく入国・出国管理システム」の完全実施を加速するための計画の策定を行うことを求めた。CBP は 2004 年から、米国の入国地点で、原則全ての外国人 [35] から人物情報（氏名や生年月日）と生体情報（顔写真と両手人差し指の指紋）を収集する「US-VISIT プログラム」の運用を開始した。2006 年 12 月からは陸・空・海、全ての入国地点で、指紋の取得が完全施行された [36]。

2015 年 3 月、CBP は、米国人の入国時に、顔認識技術を使って顔写真とパスポート写真を比較するパイロットプログラムを、ワシントン D.C. のダレス国際空港で実施した [37]。入国検査プロセスでは、最初に、税関及び入国検査の際に、CBP 担当官により顔写真が撮影され、顔比較ソフトウェアを用いて、IC 旅券（e- パスポート）のチップに含まれている顔写真と比較される（第 1 検査）。検査結果のスコアが低い場合、追加の検査が実施される（第 2 検査）。当初は、取得した顔写真は第 2 検査の間だけ保持されていたが、顔認識ソフトウェアの性能評価を行うためにはそれだけでは不十分であるとされ、2015 年 10 月から、第 1 検査で撮影された顔写真の一部と第 2 検査で撮影された全ての顔写真を、ソフトウェアの評価やデータ解析目的などに限って、保持し続けることとなった。

出国時に関しては、CBP は 2016 年 6 月、米国から出国する人を対象としたパイロットプログラムである「出国情報システム試験」（Departure Information System Test: DIST）を、アトランタ国際空港で開始した [38]。パイロットプログラムは 11 月まで続いた。搭乗口と航空機の間に設置されたカメラからのリアルタイム画像と、事前に得た搭乗者の顔写真データが比較された。DIST がうまくいったことから、CBP は同年 12 月、「出国確認システム」（Departure Verification

---

⑶3　Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (Omnibus Consolidated Appropriations Act, 1997 (P.L.104-208) Division C)

⑶4　Intelligence Reform and Terrorism Prevention Act of 2004, P.L.108-458. 策定を求めているのは 第 7208 条。なお、同法は米国同時多発テロ後、議会により設置された通称 9/11 委員会の報告書の勧告を受けて制定されたものである。National Commission on Terrorist Attacks Upon the United States, *9-11 Commission Report*, 2004, p.389. <https://www.9-11commission.gov/report/911Report.pdf>

⑶5　14 歳未満や 80 歳以上などは対象外である。「米国政府による外国人渡航者からの生体情報読み取り措置について」外務省ウェブサイト <https://www.mofa.go.jp/mofaj/toko/passport/us_visit.html>

⑶6　ただし、後述するように、出国時点での生体情報の取得については対応が遅れた。

⑶7　U.S. Department of Homeland Security, *Comprehensive Biometric Entry/Exit Plan: Fiscal Year 2016 Report to Congress*, 2016, pp.14-15. <https://www.dhs.gov/sites/default/files/publications/Customs%20and%20Border%20Protection%20-%20Comprehensive%20Biometric%20Entry%20and%20Exit%20Plan.pdf>　なお、以下の記述は、「一対一の顔認識空港入国パイロット」（1:1 Facial Recognition Air Entry Pilot）として開始日付で公表されたプライバシー影響評価による。2016 年 1 月には別の空港を対象とし、また、対象とする乗客の範囲を拡大したため、PIA が更新された。また、2016 年 10 月に取得データ保持期間を延長するため、再度 PIA が更新されている。“DHS/CBP/PIA – 025 1:1 Facial Comparison Project.” DHS website <https://www.dhs.gov/publication/facial-recognition-air-entry-pilot>

⑶8　Entry-Exit Transformation Office, Office of Field Operations, U.S. Customs and Border Protection, *Privacy Impact Assessment for the Departure Information Systems Test*, DHS/CBP/PIA-030, 2016.6.13. <https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp-dis%20test-june2016.pdf>

System: DVS）を開始した[39]。顔写真が一致しない場合は、当該人物をCBP担当官のところまで連れて行き、（外国人の場合は）指紋キャプチャを使ってIDENTで該当者を検索する、あるいは、有効な渡航文書（パスポートなど）を保持しているのかどうかについて徹底的な検査が実施される。CBP担当官がIDENTにおいて指紋を特定できなければ、FBIのNGIを検索して犯罪履歴のチェックを行うとともに、指紋をIDENTに登録する。

ドナルド・トランプ（Donald Trump）大統領は、2017年1月27日に公布した大統領令13769号[40]において、国土安全保障長官に、生体認証を使った出入国追跡システムの完成促進とその進捗状況の定期的な報告を求めた（第7条[41]）。2017年5月には、DVSは高度化された「旅行者確認サービス」（Traveler Verification Service: TVS）になった。その際、2つの重要な技術的変更があった[42]。1つは、旅行者の顔写真を、安全かつ承認された公用又は商用の仮想プライベートクラウド（Virtual Private Cloud: VPC）環境に一次的に保管すること、もう1つは、写真を比較するために、クラウドベースの生体情報照合サービスを利用することである。さらに6月、パートナーとして航空会社や空港当局にTVSプロセスへの参加を認めることとした。航空会社や空港当局は、CBPのクラウドベースの顔画像照合技術を利用することで、例えば、紙の搭乗券の代わりに顔画像を使うなど、乗客の利便性を高めることが可能になった。9月には、CBPはTSAと連携してTVSクラウドベースの照合サービスを使った生体認証技術の実証実験を実施することになった[43]。これは、チェックインから保安検査を経て搭乗に至るまでシームレスに生体認証技術が使えるかどうかを確認することも目的の1つである。10月、ニューヨークのジョン・F・ケネディ国際空港内のTSAが管理する保安検査場にカメラが30日間設置された[44]。

アトランタ国際空港で開始された出国時の生体認証プログラムは、全米に拡大しつつある。2018年6月には、CBPとグレーターオーランド空港公団（Greater Orlando Aviation Authority: GOAA）は、オーランド国際空港が米国で初めて、出入国する全ての旅客に対し顔認証技術を利用する空港になることを発表した[45]。また、同月、CBPは、生体認証に基づく出入国シス

39　Entry-Exit Transformation Office, Office of Field Operations, U.S. Customs and Border Protection, *Privacy Impact Assessment Update for the Departure Verification System*, DHS/CBP/PIA-030(a), 2016.12.16. <https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp-030-a-dvs-december2016.pdf>

40　"Protecting the Nation From Foreign Terrorist Entry Into the United States," Executive Order 13769, 2016.1.27. <https://www.federalregister.gov/d/2017-02281>

41　2017年1月に大統領令13769号に置き換わる大統領令13780号が公布されており（施行は3月16日）、この大統領令における該当条文は第8条となっている。"Protecting the Nation From Foreign Terrorist Entry Into the United States," Executive Order 13780, 2017.3.6. <https://www.federalregister.gov/d/2017-04837>

42　U.S. Customs and Border Protection, *Privacy Impact Assessment Update for the Traveler Verification Service (TVS)*, DHS/CBP/PIA-030(b), 2017.5.15, pp.4-5. <https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp030-tvs-may2017.pdf>

43　U.S. Customs and Border Protection, *Privacy Impact Assessment Update for the Traveler Verification Service (TVS): CBP-TSA Technical Demonstration*, DHS/CBP/PIA-030(d), 2017.9.25. <https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp030-tvs-september2017.pdf>

44　"CBP Deploys Facial Recognition Biometric Technology at 1 TSA Checkpoint at JFK Airport," 2017.10.11. U.S. Customs and Border Protection website <https://www.cbp.gov/newsroom/national-media-release/cbp-deploys-facial-recognition-biometric-technology-1-tsa-checkpoint>

45　"CBP Advances Biometric Exit Mission as Orlando International Airport Becomes First US Airport to Commit to Facial Recognition Technology," 2018.6.21. *idem* <https://www.cbp.gov/newsroom/national-media-release/cbp-advances-biometric-exit-mission-orlando-international-airport>　出国時に顔認証技術を利用している主要な空港は2018年6月時点で米国内に13あるという。

テムを、陸上の通関手続地における自動車による出入国者からの生体情報の収集を含むように改修することを提案した[46]。2018年8月には、CBPは、引き続きTSAと共同で、TVSの第2段階の開始を公表した。第2段階では、CBPとTSAは、過去に収集された顔写真（CBPが入国検査で撮影した写真や、パスポートやビザなど国務省が持つ写真などを含む）と、TSAの保安検査場に設置したCBPのカメラで撮影された乗客の写真を照合することになっている。TSA保安検査場の近くにはDHS名義のサイネージが置かれ、生体認証の利用は任意であり、撮影されたくない乗客は通常の検査手続きに進むことができることなどが通知されている[47]。撮影された顔写真は、TSAの保安検査官の持つタブレットからは最大2分以内に、TVSクラウドからは12時間以内に消去される。ただし、米国市民ではない場合は、その生体情報は、乗客が誰であるかの確定、技術の評価、アルゴリズムの正確性の確認、システム監査といった理由のために、自動的に監視リストと照合したり、セキュリティ上のリスクを数値化したりするシステム[48]に14日間保存される。

しかし、ジョージタウン大学ロースクールのプライバシー・技術センターは、2017年12月に公表した報告書[49]において、法的権限と正確性の2点からDHSは乗客の顔スキャンをすべきではないと主張している。前者については、外国人から生体情報を収集することは連邦議会から法律により何度も命じられているが、顔認識技術を使って米国市民の生体情報を収集することは明示的には権限が与えられていないこと、そしてそのために歯止めが用意されていない点が挙げられた。後者については、高い本人誤拒否率（FRR）（25人に1人を誤って拒否してしまう）や、もともと目的の1つに挙げられていた身分詐称（ID詐欺）の発見にどれくらい有効であるのかが示せていないことが挙げられている。

ワシントンD.C.のダレス国際空港で、入国審査場に「顔認証ゲート」が導入されて3日目の2018年8月22日、ブラジルのサンパウロから到着した26歳の男性が、顔認識技術により、提示されたフランスのパスポートの顔写真と本人の顔が一致しないと判断され、CBPの職員が検査したところ、靴の中からコンゴ共和国の身分証が発見され、身分や国籍を詐称していたことが分かったと報じられた。顔認識技術を使った初の摘発だという[50]。

TSAは、2018年9月に「生体認証ロードマップ」（TSA Biometrics Roadmap）を公表し、4つの目標と2018年から2026年までの見通しを示した。4つの目標は、①国境を超える旅行者の生体認証に関してCBPと協働する、②TSAの「プリチェック」（事前審査済み）旅行者[51]が

⑷⑹　Anthony Kimery, “CBP plans to expand biometric entry/exit program to include vehicles,” 2018.6.3. Biometric Update.com website <https://www.biometricupdate.com/201806/cbp-plans-to-expand-biometric-entry-exit-program-to-include-vehicles>

⑷⑺　U.S. Customs and Border Protection, *Privacy Impact Assessment Update for the Traveler Verification Service (TVS): CBP-TSA Technical Demonstration Phase II,* DHS/CBP/PIA-030(e), 2018.8.14. <https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp030e-tvs-august2018_0.pdf>

⑷⑻　自動ターゲティングシステム（Automated Targeting System: ATS) – 統一乗客モジュール（Unified Passenger Module: UPAX）と呼ばれている。

⑷⑼　Harrison Rudolph et al., *Not Ready for Takeoff: Face Scans at Airport Departure Gates*, Center on Privacy and Technology at Georgetown Law, 2017.12.21. <https://www.airportfacescans.com/sites/default/files/Biometrics_Report__Not_Ready_For_Takeoff.pdf>

⑸⑽　「米空港で顔認識技術がお手柄、偽造旅券で入国試みた男を見破る」2018.8.26. AFP BB Newsウェブサイト <http://www.afpbb.com/articles/-/3187288>; “CBP at Washington Dulles International Airport intercepted an imposter using new cutting-edge Facial Comparison Biometrics technology,” 2018.8.23. U.S. Customs and Border Protection website <https://www.cbp.gov/newsroom/local-media-release/cbp-washington-dulles-international-airport-intercepted-imposter-using>

⑸⑾　プリチェック（pre✔）とは、あらかじめオンラインで申請し、バックグラウンドチェックを受け、指紋を届け出て、認可されると、保安検査で靴やベルトを脱いだり、パソコンを取り出したりしなくて済むという制度である。

生体認証を利用しやすくする、③国内旅行者にも生体認証を拡大する、④生体認証技術の利活用のためのインフラを整備する、である[52]。2018年10月5日にトランプ大統領が署名して成立した「TSA近代化法」では、生体認証技術の利用について、TSAとCBPの局長が協議しながら進めるとともに、連邦議会両院の関係委員会に以下の内容を含む報告書を提出することをDHS長官に求めている[53]。

表２　生体認証技術の利用について、TSA近代化法が報告を求めた事項

（1）旅行者を識別するために生体認証技術を用いることの運用面やセキュリティへの影響
（2）生体認証技術の利用をそのように拡大することによるプライバシーへの影響（生体情報の収集に伴うプライバシーへのリスクを軽減するために提案あるいは実施される方法を含む）
（3）顔認識技術を含む生体認証技術の利用に関して発生する人種・性別・年齢に関連する照合性能のエラーを分析し、対処する手法
（4）実際の生体情報を利用した出入国プログラムに関する
（A）以下の評価
・偽陽性率（FPR）と偽陰性率（FNR）を含むエラー率と、生体認証技術の正確性
・特定のカテゴリーの旅行者（人種・性別・国籍）に過度の負担をかけていないかどうか
・在留期限を超えてオーバーステイとなった旅行者の問題にどれだけ・どのように対処できるか
・生体情報の収集に関して発生しうるプライバシーリスクの軽減方法を含む、生体認証技術利用のプライバシーへの影響
・毎年、在留期限を超えてオーバーステイとなった人の数
（B）　エラー率の値やエラー率が特定の人種・性別・国籍に偏っていないかどうかを評価したすべての監査結果の説明
（C）　米国人旅行者が、生体認証技術を使ったスキャンをオプトアウトできるプロセスの説明
（D）　生体認証技術を使って収集された旅行者データの種類と、それらにアクセスできる省庁の名称、それらのデータの保持期間、それらのデータの安全な管理のための措置、旅行者識別に用いられた後の米国市民データの即時の消去に向けた短期的目標についての説明

（出典）　FAA Reauthorization Act of 2018, P.L.115-254. Division K 第1919条（c）　を基に筆者作成。

デルタ航空は2018年9月、アトランタ国際空港のターミナルFが、チェックインから、手荷物預入れ、手荷物検査、搭乗を全て顔認識技術によって進められる全米初の「生体認証ターミナル」になると発表した[54]。

一方、生体認証技術の利用の拡大は絶えず批判を浴びてきた。CBPは、生体情報を利用した出入国プログラムに関して、複数のプライバシー擁護団体との意見交換会を2017年8月と2018年1月に開催した[55]。後者に出席した電子フロンティア財団（Electronic Frontier Foundation: EFF）は2018年2月15日付で、CBP宛てに書簡を送っている[56]。その中で以下の2点の懸念が表明されている。

⑸２　Transportation Security Administration, *TSA Biometrics Roadmap for Aviation Security & the Passenger Experience*, 2018.9. Homeland Security Digital Library website <https://www.hsdl.org/?view&did=817439>

⑸３　FAA Reauthorization Act of 2018,（P.L.115-254）Division K 第1919条（a）及び（c）

⑸４　“Delta to launch first biometric terminal in the U.S.,” 2018.9.20. Delta News Hub website <https://news.delta.com/delta-launch-first-biometric-terminal-us> 2018年12月から開始される。ただし、TSAチェックポイントでパスポートと搭乗券を提示しなければならない。また、顔認識技術を使わないオプションも残されている。

⑸５　“CBP Meets with Privacy Groups to Discuss Biometric Exit,” 2018.2.2. U.S. Customs and Border Protection website <https://www.cbp.gov/newsroom/national-media-release/cbp-meets-privacy-groups-discuss-biometric-exit-0>

⑸６　“EFF Follow Up Letter to U.S. Customs and Border Protection,” 2018.2.15. Electronic Frontier Foundation website <https://www.eff.org/document/eff-follow-letter-us-customs-and-border-protection>

1点目は、外国人については出国時の写真撮影が法律により義務付けられている[57]のに対して、米国市民から顔画像データを集めることについては法的根拠が欠けているというものである。このような批判に対しては、CBPは、顔画像の保持期間を14日に制限していること、また顔認証を使いたくない人には使わないオプションを提供していることを説明している。

2点目は、国際線の航空機の搭乗直前に顔画像が取得されていることについて、乗客への明示的な通知を行うべきことや、顔認証を使わないオプションを残しておく方法が航空会社にうまく伝わっておらず、また、航空会社による顔画像データの扱いに対する監督（oversight）メカニズムも欠けているというものである。

DHSには、プライバシー等の倫理的な側面を助言するための組織がいくつかある。法律に基づき、「チーフプライバシーオフィサー」（Chief Privacy Officer: CPO）[58]と監察総監室（Office of Inspector General: OIG）[59]が設置されており、また、諮問機関として、外部有識者からなる「データ・プライバシー及び完全性諮問委員会」（Data Privacy and Integrity Advisory Committee: DPIAC）も設置されている。CPOは2008年に、同省におけるプライバシー原則として、1974年プライバシー法[60]に基づく「公正情報実務諸原則」（Fair Information Practice Principles: FIPPs）を採用した[61]。FIPPsは、①透明性、②個人の参加、③目的の明確化、④必要最低限のデータ、⑤利用制限、⑥データの質及び完全性、⑦セキュリティ、⑧アカウンタビリティ及び監査の8原則からなる。DHSは、生体認証技術を使った新たな施策を導入したり、更新したりするたびに、プライバシー影響評価（PIA）を実施・公表しているが、FIPPsに照らして実施され、CPOがレビューを行っている。また、CPOは毎年、連邦議会に年次プライバシー報告書を提出している[62]。

OIGは、在留期限を超えてオーバーステイとなった者を検出するITシステムの有効性を監査した結果を、2017年5月に発表した[63]。その中で、DHSが、出国場所での包括的な生体認証出国システムを持っていないことから、正確ではないことも多い航空会社の乗客名簿を利用せざるを得ないことを指摘した。OIGは、2018年9月、フォローアップの報告書を公表し、CBPがパイロットプログラムを通じて、9つの空港で98％の照合率を達成するなど、顔認識技術を使って空路で出国する乗客を追跡する能力が大きく向上したことを指摘した[64]。それと同時に、技術的及び運用上の様々なトラブルにより、顔認識技術の対象となった乗客のうち実際に顔認識技術が適用された割合が85％に留まったことも指摘した。

⑸7　8 U.S.C.§1365b　なお、この規定は「1996年不法移民改革及び移民責任法」第104条等による。

⑸8　2002年国土安全保障法（「2007年9･11委員会勧告実施法」（Implementing Recommendations of the 9/11 Commission Act of 2007, P.L. 110-53.）第802条による改正を含む）に基づく。CPOを補助する組織として、「プライバシー室」（Privacy Office）が設置されている。

⑸9　「1978年監察総監法」（Inspector General Act of 1978, P.L.95-452, 5 U.S.C. App.§1-13）に基づき、連邦政府の各省庁等に監察総監（Inspector General）と監察総監室（Office of Inspector General）が置かれている。OIGは、GAOの定めた基準に基づいて監査を実施する。

⑹0　Privacy Act of 1974 (P.L.93-579) (5 U.S.C.§552a)

⑹1　Chief Privacy Officer, "The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security," *DHS Privacy Policy Guidance Memorandum*, 2008-1, 2008.12.29. <https://www.dhs.gov/publication/privacy-policy-guidance-memorandum-2008-01-fair-information-practice-principles> FIPPsは、もともと1970年代に連邦取引委員会（Federal Trade Committee: FTC）がその概念を提案したものである。

⑹2　"Privacy Office Annual Reports." DHS website <https://www.dhs.gov/publication/privacy-office-annual-reports>

⑹3　Office of Inspector General, DHS, *DHS Tracking of Visa Overstays is Hindered by Insufficient Technology*, OIG-17-56, 2017.5.1. <https://www.oig.dhs.gov/sites/default/files/assets/2017/OIG-17-56-May17_0.pdf>

⑹4　Office of Inspector General, DHS, *Progress Made, but CBP Faces Challenges Implementing a Biometric Capability to Track Air Passenger Departures Nationwide*, OIG-18-80, 2018.9.21. <https://www.oig.dhs.gov/sites/default/files/assets/2018-09/OIG-18-80-Sep18.pdf>

DPIACは、DHS長官とCPOの要請に従って、DHS内の個人情報やプライバシーに関連する問題に対して、技術面から政策面まで幅広く助言を与えることが期待されている。例えば、2017年7月にはDPIACの政策小委員会が、プライバシー室やCBPの担当者とともに、オーランド国際空港で、生体認証を利用した出入国パイロットプログラムの視察を行い、「旅行者に対して、生体情報を収集していることについて、サイネージを含む、適切な通知がなされており、パイロットプログラムへの参加が任意であることを知らされていること」を確認している[65]。

また、GAOも国境管理における生体認証の利用について第三者的な視点からの評価を実施し、報告書を公表している。2013年には、CBPによる生体認証に基づく出国管理について、計画の実施に時間枠やマイルストーンを設けるように勧告した[66]。2016年の報告書[67]では、3年前の勧告が十分に実施されていないことを指摘したものの、2017年の報告書では、パイロットプログラムの実施等、一定の進捗があったと評価されている[68]。

3　商業利用

生体認証技術、特に顔認識技術の商業利用に関しては、連邦取引委員会（Federal Trade Committee: FTC）と商務省の国家電気通信情報庁（National Telecommunications and Information Administration: NTIA）が扱っており、それぞれ近年、行動規範やガイドラインを発表している。

FTCは、顔認識技術の利用が様々な分野で拡大していることを踏まえ、2011年12月、消費者保護団体、学術界、事業者、業界団体、プライバシーの専門家など、多様な関係者を招いて、顔認識技術に関するフォーラムを開催し、プライバシーやセキュリティへの懸念も含めた幅広い話題を議論した[69]。フォーラムの資料や映像は公開され、2011年12月から2012年1月までパブリックコメントを募集したところ、80件の意見が集まった。それらも加味した上で、FTCは2012年10月、「顔認識技術の一般的な利用のためのベストプラクティス」と題する報告書を公表した[70]。最初に、プライバシーに関する3つの原則、すなわち、①プライバシー・バイ・デザイン（Privacy by Design: PbD. 製品開発の初期段階でプライバシーが組み込まれるべき）、②消費者に分かりやすい選択肢（消費者には適切な時機と文脈で選択肢を与えるべき）、③透明性（収集される情報とそれらの利用について知らせるべき）という3つの原則が挙げられた。その上で、よくある商業用途として、①眼鏡会社のウェブサイトに消費者が顔をアップロードして様々なタイプの眼鏡が似合うかどうか試すケース、②スポーツドリンク会社がスーパーマー

⑹5　Department of Homeland Security, *2018 Privacy Office Annual Report to Congress: For the period July 1, 2017 – June 30, 2018*, 2018.10.10, p.30. <https://www.dhs.gov/sites/default/files/publications/dhs%20privacy%20office%202018%20annual%20report%20FINAL%2010-10-2018.pdf>

⑹6　U.S. Government Accountability Office, *Overstay Enforcement: Additional Actions Needed to Assess DHS's Data and Improve Planning for a Biometric Air Exit Program*, GAO-13-683, 2013.7.30. <https://www.gao.gov/products/GAO-13-683>

⑹7　U.S. Government Accountability Office, *Border Security: Actions Needed by DHS to Address Long-Standing Challenges in Planning for a Biometric Exit System*, Testimony Before the Subcommittee on Immigration and the National Interest, Committee on the Judiciary, U.S. Senate, GAO-16-358T, 2016.1.20. <https://www.gao.gov/assets/680/674704.pdf>

⑹8　U.S. Government Accountability Office, *Border Security: DHS Has Made Progress in Planning for a Biometric Air Exit System and Reporting Overstays, but Challenges Remain*, GAO-17-170, 2017.2.27. <https://www.gao.gov/assets/690/683036.pdf>

⑹9　"Face Facts: A Forum on Facial Recognition Technology," 2011.12.8. FTC website <https://www.ftc.gov/news-events/events-calendar/2011/12/face-facts-forum-facial-recognition-technology>

⑺0　FTC, *Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies*, 2012.10. <https://www.ftc.gov/sites/default/files/documents/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies/121022facialtechrpt.pdf>

ケット内にカメラ内蔵のデジタルサイネージを置いて前に立つ消費者の年齢層と性別を推定しターゲット広告を表示するケース、③ SNS においてユーザーが新たに写真をアップロードするとユーザーが過去に「友達」としてタグ付けした情報を基にタグ付けを行うケース、の 3 つのケーススタディを基に、ベストプラクティスが検討された。

NTIA は、2012 年に大統領府が発表した枠組文書[71]に基づいて、「消費者プライバシー権利章典」（A Consumer Privacy Bill of Rights）の理念を実践するためのマルチステークホルダープロセスを通して、消費者データ・プライバシーのための行動規範（Code of Conduct）を策定することになった。具体的には、顔認識技術の商業利用に関して、自発的ではあるが法的拘束力のある行動規範[72]を作成すべく、2013 年 12 月に通知した上で、2014 年 2 月、産業界、市民団体、学術関係者が集まるプライバシー・マルチステークホルダー会合を開催した[73]。その後も月に 1 ～ 2 回の頻度で会合を重ねたが、2015 年 6 月 11 日の会合の後、参加していた 9 つのプライバシー擁護団体が共同声明を発表し、顔認識技術の利用においてプライバシーを十分に保護するための一連のルールが策定できそうもないことを理由に、マルチステークホルダープロセスから離脱した[74]。会合は他のステークホルダーにより継続され、当初の予定から大幅に遅れ、2 年半かかって、2016 年 6 月に、3 ページの「顔認識の商業利用のためのプライバシー・ベストプラクティス勧告」が公表された[75]。顔認識技術の用途があまりに広範にわたり、技術の発展スピードも速いため、具体的で詳細な内容とすることは不可能で、またそれは役に立たないと判断され、勧告の基礎となる原則として、広く受け入れられている枠組みである FIPPs を採用した上で、以下の 6 点をまとめた。

⑺1　米国のプライバシー保護法制は、公的部門に対しては、1974 年プライバシー法が制定されたが、民間部門に対しては、分野ごとに個別法が制定されたほかは、自主規制を基本としていた。そのような中、2012 年 2 月にバラク・オバマ（Barack Obama）大統領の下、大統領府は、消費者データ・プライバシーに関する枠組文書を発表し、その中で「消費者プライバシー権利章典」の草稿や、それに基づき、法的拘束力のある行動規範を策定するためのマルチステークホルダープロセスなどを示した（The White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, 2012.2. <https://obamawhitehouse.archives.gov/sites/default/files/privacy-final.pdf>）。消費者プライバシー権利章典の草稿は、FIPPs をベースとし、個人のコントロール、透明性、背景情報の尊重、セキュリティ、アクセスと正確性、適切な範囲の収集、アカウンタビリティといった原則を挙げ、連邦議会にこれらの権利等の立法化を求めていたが、その後、立法化は進まなかった。

⑺2　事業者が自発的に行動規範を策定し、策定後に、事業者がその規範に従うことを約した後には、FTC によって法的拘束力を持つことになる。U.S. Government Accountability Office, *Facial Recognition Technology: Commercial Uses, Privacy Issues, and Applicable Federal Law*, GAO-15-621, 2015.7.30, p.20. <https://www.gao.gov/assets/680/671764.pdf>

⑺3　“Privacy Multistakeholder Meetings Regarding Facial Recognition Technology: February – June 2014,” 2013.12.3. NTIA website <https://www.ntia.doc.gov/other-publication/2013/privacy-multistakeholder-meetings-regarding-facial-recognition-technology-feb>

⑺4　Jeff Chester, “Privacy and Consumer Advocates Leave Administration’s “Multistakeholder” Negotiations on Facial Recognition,” 2015.6.16. Center for Digital Democracy website <https://www.democraticmedia.org/filing/privacy-and-consumer-advocates-leave-administrations-multistakeholder-negotiations-facial>

⑺5　“Privacy Best Practice Recommendations For Commercial Facial Recognition Use,” 2016.6.15. NTIA website <https://www.ntia.doc.gov/files/ntia/publications/privacy_best_practices_recommendations_for_commercial_use_of_facial_recogntion.pdf>

表３　NTIAのマルチステークホルダープロセスでまとめられた顔認識の商業利用に関する原則

	原則	内容
1	透明性の確保	データを収集・共有・利用する合理的に予見可能な目的、データ保持や匿名化の実施などについてのポリシーの公表や、顔認識技術の利用に関する消費者への通知といった透明性を確保する
2	適正なデータ管理実務の策定	参加が任意か否か、顔以外のセンシティブデータの取得の有無、データの保持・利用方法、当人の雇用・ヘルスケア・金融商品及びサービス・信用取引・住宅・保険などへの適格性や利用の可否の判断に用いられるかどうか、ありうるリスクや危害、データの利用に関する消費者の合理的期待を考慮し、データ管理実務を検討する
3	利用の制限	第三者提供などの利用を個人がコントロールする機会を提供する
4	セキュリティの保護	データのセキュリティを手続的、技術的、及び物理的に保護する
5	データの品質	データの完全性を維持する
6	問題解決と救済	消費者からの問い合わせ窓口を用意する

（出典）“Privacy Best Practice Recommendations For Commercial Facial Recognition Use,” 2016.6.15. NTIA website <https://www.ntia.doc.gov/files/ntia/publications/privacy_best_practices_recommendations_for_commercial_use_of_facial_recogntion.pdf> を基に筆者作成。

一方、具体的に小売店で顔認識技術が活用されている事例もわずかであるが報じられている。小売大手のウォルマート（Walmart）社が、入店する全ての人の顔をスキャンして、万引き容疑者が入店すると即座に店の警備員の携帯機器に警告が届く顔認識技術システムを 2014 年後半から数か月試行したことが報じられている[76]。その際、万引き犯のプライバシー保護の問題も提起されたと書かれている。このシステムを納入した FaceFirst 社の CEO は、フォーチュン 500 に名を連ねる小売業のうちの数社が、すでに同システムを利用していると明かしているが、フォーチュン誌がいくつかの大企業に問い合わせた際、明確な回答があったのがウォルマート社のみだった。しかし、ウォルマート社は 2015 年初頭、導入を中止した。理由は「十分な投資対効果が得られないから」であった。2018 年現在、ウォルマート社は顔認識技術を採用していないが、2017 年、レジのビデオカメラを用いて顧客の満足度を測定する顔認識技術の特許を出願し[77]、2018 年には従業員同士や従業員と客の間の会話を捕捉する音センサに関する特許を取得するなど、引き続き生体認証技術の利用に関心を持っているようである[78]。また、住宅リフォーム会社のロウズ（Lowe's）社も、2014 年に 3 店舗で試行した後に実施を取りやめたことを明らかにした[79]。

４　イリノイ州

連邦レベルでは、民間における生体情報の利用に関する法規制はまだ存在していないが、州

(76)　Jeff John Roberts, “Walmart's Use of Sci-fi Tech To Spot Shoplifters Raises Privacy Questions,” 2015.11.9. Fortune website <http://fortune.com/2015/11/09/wal-mart-facial-recognition/>

(77)　Hayley Peterson, “Walmart is developing a robot that identifies unhappy shoppers,” 2017.7.19. Business Insider website <https://www.businessinsider.com/walmart-is-developing-a-robot-that-identifies-unhappy-shoppers-2017-7>

(78)　Caroline O'Donovan, “Walmart's Newly Patented Technology For Eavesdropping On Workers Presents Privacy Concerns,” 2018.7.11. BuzzFeed News website <https://www.buzzfeednews.com/article/carolineodonovan/walmart-just-patented-audio-surveillance-technology-for>

(79)　Leticia Miranda, “Thousands Of Stores Will Soon Use Facial Recognition, And They Won't Need Your Consent,” 2018.8.17. BuzzFeed News website <https://www.buzzfeednews.com/article/leticiamiranda/retail-companies-are-testing-out-facial-recognition-at>

レベルでは2008年にイリノイ州、2009年にテキサス州、2017年にワシントン州で生体認証技術の商業利用の手順を定めた法律が制定された。しかし、後述するように、ワシントン州の法律では顔は一切対象とされておらず、テキサス州の法律では「顔の形状」（face geometry）は対象とされているものの、同法に基づく個人訴訟が認められていない。そのため、顔の形状が対象とされており、かつ、個人訴訟が可能なイリノイ州の法律が、近年、注目を集めている。

2008年、生体情報を用いた決済サービス会社、Pay By Touch社が倒産し、所持していたおよそ300万人の顧客の生体情報が破産手続を通して販売されてしまうおそれが生じた[80]。このことをきっかけとして、同年、生体情報利用に伴うプライバシー侵害のおそれを懸念したイリノイ州議会議員の発議によって、「イリノイ生体情報プライバシー法」（BIPA）[81]が制定された。立法の意図は、生体情報の活用のための人々の懸念を拭い去ることにあった。

BIPAは、事業者が、顧客や被雇用者等の生体識別子（biometric identifier）、それを基にした生体情報（biometric information）を収集する際には、収集目的やデータ保持期間などを、事前に書面で通知し、同意を取得しなければならないとしている（第15条(b)）。また、売買等により、生体識別子や生体情報から利益を得ることも禁じている（第15条(c)）。BIPAの適用対象となる生体識別子は、「網膜や虹彩のスキャン、指紋、声紋、あるいは手や顔の形状のスキャン」（a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry）と定義されている（第10条）。

これらの規定に基づき、近年、オンラインサービスのユーザーがFacebook社等を訴えるタイプの訴訟と、被雇用者が雇用主を訴えるタイプの訴訟が数多く起こされている。前者は、シカゴ在住の3人のFacebookユーザーがそれぞれ2015年に提訴したものである。その後これらの訴えは1つに併合されている[82]。原告のユーザーらは、Facebook社による写真へのタグ付け提案が、ユーザーの明示的な同意なしに生体情報を収集しているとして、BIPA違反であると主張した。Facebook社は、顔認識技術の適用はイリノイ州の外のサーバで行われているためBIPAは適用されない、さらにBIPAはそもそも、合衆国憲法の休眠州際通商条項（dormant commerce clause）[83]に違反すると主張した[84]。イリノイ州の600万人以上のFacebookユーザーを代表して起こされた訴訟では、原告はBIPA違反で1人につき最大5,000ドルの支払いをFacebook社に求めた。2018年4月16日、サンフランシスコの連邦地方裁判所は、「Facebookにより2011年6月7日以降に顔テンプレートが作成・保管されたイリノイ州のFacebookユー

---

(80)　Chris Trytten, “Has BIPA Succeeded or Failed to Fulfill its Objectives?” Crossmatch Blog website <https://blog.crossmatch.com/enrollment/commercial/bipa-succeeded-or-failed/>

(81)　Biometric Information Privacy Act, P.A.95-994.（740 ILCS 14）<http://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57>

(82)　Dawn Rhodes “California judge: Illinois Facebook 'tagging' lawsuit can proceed,” *Chicago Tribune*, 2016.5.10. <https://www.chicagotribune.com/news/local/breaking/ct-facebook-lawsuit-20160510-story.html>　Facebook社だけでなく、Google社も同様にGoogle Photosについて提訴された。

(83)　州際通商条項は、合衆国憲法第1条第8節第3項に規定されており、連邦議会に州際通商を規制する権限を与えている。州際通商について、連邦議会が立法措置を講じず、沈黙している場合は「休眠」と呼ばれ、裁判所が決定することになる。インターネットを通じた情報流通は通常、複数の州にまたがるため、州の規制が休眠州際通商条項に違反しているかが問われることが増えているという。辻雄一郎「〈論説〉最近の州際通商条項についての憲法学的考察」『筑波法政』No.60, 2015.6, pp.111-136. <http://tsukuba.repo.nii.ac.jp/?action=repository_uri&item_id=34214&file_id=17&file_no=1>

(84)　Ndidi M. Elue and Jason Gordon, “Illinois Biometric Lawsuit Against Facebook Moves Through Court System,” 2018.2.5. mondaq website <http://www.mondaq.com/unitedstates/x/670694/Data+Protection+Privacy/Illinois+Biometric+Lawsuit+Against+Facebook+Moves+Through+Court+System>

ザー」による集団訴訟（クラスアクション）を認める判断を行った[85]。「2011年6月7日」は、Facebook社が「タグ付け提案」を開始した日である。なお、2017年12月からFacebook社はタグ付けの有無によらず顔写真が誰かによってアップロードされると自動的に通知される仕組みを開始した。

これらの訴訟と並行して、Facebook社は2016年にBIPAを改正させるためのロビー活動を精力的に行ったことが明らかになっている。イリノイ州議会上院のビル・カニンガム（Bill Cunningham）議員（民主党）らは、2018年2月にBIPA改正案を提出したが、2018年内には審議は行われなかった。

他方、2017年以降、雇用主に対する、BIPAに基づいた集団訴訟が多数起こされている[86]。被告には様々な雇用主が含まれており、典型的には、指紋認証による入退管理を行っている事業者である。被告の雇用主が適切な事前説明と同意の取得を欠き、さらに、生体情報の利用、保持、破棄についての方針を説明していないこと、場合によっては第三者と不適切に共有していることが指摘されている。例えば、2017年11月7日に提訴されたユナイテッド航空（United Airlines）は、BIPAに違反しているとして1人5,000ドルの支払いを請求された[87]。本件に関して、2018年7月31日、イリノイ州北部地区連邦地方裁判所は、十分な損害が生じておらず単純な法的違反の問題にすぎないなどとして、訴えを却下した[88]。

BIPAとよく似た州法は、テキサス州とワシントン州でも施行されている。

テキサス州では、「生体識別子の取得や利用に関するテキサス州法」[89]が2009年に制定された。同州法は、イリノイ州のBIPAとは異なり、事前説明と同意の取得は求めるものの、同意は書面による必要はない[90]。また、テキサス州司法長官（Attorney General）だけが違反を提訴できるとし、私人の請求権は保証していない。

ワシントン州でも、「生体識別子に関する州法」[91]が2017年5月16日に成立し、7月23日に施行された[92]。事業者が商業目的で指紋、声紋、網膜、虹彩等の生体識別子を収集し、利

(85)　Joel Rosenblatt, “Facebook Photo-Scanning Suit Is a Multibillion-Dollar Threat,” 2018.4.17. Bloomberg website <https://www.bloomberg.com/news/articles/2018-04-16/facebook-must-face-group-suit-claiming-it-stole-biometric-data>　原告と被告で州が異なるため、連邦裁判所の管轄権が認められる（合衆国憲法第3条第2節第1項）。Facebook社は、同日付で、連邦第9巡回区控訴裁判所に控訴し、2018年12月現在係争中である。Martina Barash, “Facebook Tells 9th Cir. to Block Users’ Privacy Class Suit,” 2018.12.11. Big Law Business website <https://biglawbusiness.com/facebook-tells-9th-cir-to-block-users-privacy-class-suit>

(86)　Daniel B. Pasternak, “Illinois Employers Face A Recent Rash of Class Action Lawsuits Filed Under State Biometric Information Privacy Law,” 2017.11.27. The National Law Review website <https://www.natlawreview.com/article/illinois-employers-face-recent-rash-class-action-lawsuits-filed-under-state>

(87)　Kimberly R. McCoy, “Businesses Increasingly Subjected to Class Action Lawsuits Alleging Violations of Illinois Biometric Information Privacy Act,” 2017.11.16. Vinson & Elkins LLP website <https://www.velaw.com/Blogs/Tech-Blog/Businesses-Increasingly-Subjected-to-Class-Action-Lawsuits-Alleging-Violations-of-Illinois-Biometric-Information-Privacy-Act/>

(88)　Chris Burt, “BIPA lawsuit against United quashed and new suits filed as harm criteria is clarified,” 2018.8.2. Biometric Update.com website <https://www.biometricupdate.com/201808/bipa-lawsuit-against-united-quashed-and-new-suits-filed-as-harm-criteria-is-clarified>

(89)　Texas Statute on the Capture or Use of Biometric Identifier (81(R) HB 3186, Texas Business and Commerce Code - BUS & COM §503.001.) <https://capitol.texas.gov/BillLookup/History.aspx?LegSess=81R&Bill=HB3186>

(90)　John G. Browning, “The Battle Over Biometrics: A look at the law in Texas and two other states,” *Texas Bar Journal*, Vol.81 No.9, 2018.10, pp.674-675. <https://www.texasbar.com/AM/Template.cfm?ection=Content_Folders&ContentID=42128&Template=/CM/ContentDisplay.cfm>

(91)　2017 Wa. HB 1493, Chapter 19.375 RCW <https://app.leg.wa.gov/RCW/default.aspx?cite=19.375>

(92)　“Washington Becomes Third State to Enact Biometric Privacy Law,” 2017.6.1. Hunton Andrews Kurth Privacy & Information Security Law Blog website <https://www.huntonprivacyblog.com/2017/06/01/washington-becomes-third-state-enact-biometric-privacy-law/#page=1>

用しようとする場合の要件を定めている。商業目的での生体識別子の収集・利用を対象とし、事業者に事前説明と同意取得などを義務付けている。また、同法では、対象とする識別子について、「写真、ビデオ若しくはオーディオ録音、又はそれらから得られたデータ」を除外することが明示的に書かれている。そのため、SNS や写真ストレージウェブサイトがユーザーのデジタル写真に自動的にタグ付けするために用いる顔認識技術は本法律の適用対象外であると考えられている。

５　ニューヨーク州

ニューヨーク州では、生体情報の収集・保持・利用を規制する州法はないものの、法執行、学校安全、エンターテインメントといった多様な目的で顔認識技術が利用されており、それぞれが議論を呼んでいる。

2018 年 3 月、ニューヨークタイムズ紙が、関係者からの取材の結果、ニューヨーク市のマディソン・スクエア・ガーデンにおいてセキュリティと人物特定を目的として顔認識技術が利用されているのではないかと報じた[93]。これについてマディソン・スクエア・ガーデンでは、もともと顔認識技術自体は 2011 年から、FanCam と呼ばれるエンターテインメントを目的として、NBA（National Basketball Association）と NFL（National Football League）の試合で利用されてきた[94]。これは、高解像度のカメラで撮られた客席の写真をズームして自分を見つけ、タグ付けしてメールやソーシャルメディアなどでシェアするものである。

ニューヨーク市警（New York City Police Department: NYPD）は、2011 年、同市警等の膨大な犯罪データを分析し犯罪捜査を支援するリアルタイム犯罪センター（Real Time Crime Center: RTCC）の下に顔識別ユニットを設置した。顔識別ユニット内の 10 人の捜査員は、2018 年 4 月の時点で、容疑者の特定のために、監視カメラの画像等が捜査員から送られてきた場合に限り顔認識技術を利用しており、仮に（犯罪歴のある人の顔データベースである）マグショットと適合した場合でも、逮捕に必要な証拠には採用できず、捜査の手掛かりとされるだけだという[95]。同市警は、容疑者の特定だけではなく行方不明者の捜索にも顔認識技術を利用するため、犯罪歴の無い人の顔も含むニューヨーク州自動車局（Department of Motor Vehicles: DMV）の持つ運転免許証データベースも利用したいと考えていると報じられている[96]。

他方、DMV は 2010 年以降、顔認識ソフトウェアを利用して、運転免許証の申請時に、ID の窃盗や詐欺を調査しており、2016 年には顔認識システムが更新され、その正確性が増した。アンドリュー・クオモ（Andrew Cuomo）州知事は 2017 年 8 月、DMV の顔認識技術プログラムがこれまで 21,000 件以上の ID の窃盗や詐欺を特定し、そのうち 7,000 件はシステム更新後であることを明らかにした[97]。また、逮捕された人数は 4,000 人を上回るという。また、クオモ州知事は 2018 年 7 月 20 日、州公社が運営する橋やトンネルの料金所において、顔とナンバー

⑼3　Kevin Draper, “Madison Square Garden Has Used Face-Scanning Technology on Customers,” *New York Times*, 2018.3.13. <https://www.nytimes.com/2018/03/13/sports/facial-recognition-madison-square-garden.html>

⑼4　Jen Booton, “Report: MSG Adopts Facial Recognition At Arena Gates For Security,” 2018.3.14. SportTechie website <https://www.sporttechie.com/report-msg-adopts-facial-recognition-at-arena-gates-for-security/>

⑼5　Zolan Kanno-Youngs, “Facial Recognition Could Move Beyond Mug Shots,” *Wall Street Journal*, 2018.4.4.

⑼6　*ibid*.

⑼7　“Governor Cuomo Announces Major Facial Recognition Technology Milestone with 21,000 Fraud Cases Investigated,” 2017.8.21. New York State website <https://www.governor.ny.gov/news/governor-cuomo-announces-major-facial-recognition-technology-milestone-21000-fraud-cases>

プレートの自動認識をすでに行っていることを明らかにした。州当局によると、トライボロー橋で試行しており、クイーンズ・ミッドタウントンネルとブルックリン・バッテリートンネルにおいても新たに開始、さらに他の有料の橋や空港への道路などでもいずれ実施される予定である。ただし、セキュリティ上の理由から、開始時期、参照されるデータベースの種類、データへのアクセス権限の範囲については開示を拒否した[98]。

ニューヨーク州北部のロックポート市学区（Lockport City School District）が、生徒の学習機会を改善するためのインフラや技術への投資を増やす目的で設定された州教育省の予算を使って[99]、学校向けの顔認識技術を導入することを提案し、2015年夏からの試行において、様々なタイプの銃を認識できるかなどの検証が進められていた。その結果、400万ドルの予算のほとんどを顔認識システムに支出することを決め、2018年夏に300台のカメラが導入された[100]。州の内外から、そのセキュリティ上の効果への疑問と、生徒のプライバシーへの懸念が表明されている。市民団体の連合体である「ニューヨーク市民の自由連合」（New York Civil Liberties Union: NYCLU）はニューヨーク州教育省に書簡を送り反対した[101]。書簡では、予算の目的と合致していないことに加えて、2016年に開催された本件に関する公聴会が夏季休暇中であったため、パブリックコメントが0件であったことも指摘されている。さらに、問題点として4点が挙げられている。1点目は顔認識技術の正確性の問題で、特に有色人種や女性に関して正確性の低さが度々議論になっていること。2点目は生徒、教諭、スタッフのプライバシー権を侵害している点。3点目は得られた個人情報の管理方法について、特に法執行機関と共有されることへの懸念である。4点目は、学校が児童生徒を、保護する対象ではなく、脅威の1つとして扱っているというメッセージとなり、学校という教育の場の健全性をむしばむのではないかという懸念である。なお、2018年11月現在、ロックポート市学区が作成したプライバシーポリシーの草案が、ニューヨーク州教育省において審査中である[102]。

６　カリフォルニア州

カリフォルニアでは州全体での監視技術の規制改革が進んでいる。2018年6月28日に州議会で、「カリフォルニア消費者プライバシー法」が成立した[103]。2020年1月1日施行予定

98　Danielle Furfaro, Jennifer Bain and Ruth Brown, “Inside Cuomo's plan to have your face scanned at NYC toll plazas,” New York Post, 2018.7.20. <https://nypost.com/2018/07/20/inside-cuomos-plan-to-have-your-face-scanned-at-nyc-toll-plazas/>

99　プログラムの名称は「スマートスクール基金（法）」（Smart Schools Bond Act: SSBA）であり、総額20億ドルが各学区等に割り当てられることになっている。なお、このプログラムで各学区に割り当てられた予算を人件費に充てることはできないことが、顔認識システムが採用された一因という見方もある。Thomas J. Prohaska, “Lockport schools turn to state-of-the-art technology to beef up security,” 2018.5.20. The Buffalo News website <https://buffalonews.com/2018/05/20/lockport-schools-turn-to-state-of-the-art-technology-to-beef-up-security/>

100　Lockport City School District, “Smart Schools Investment Plan - 2016-17 Version (Original) - SSIP-1,” 2017.10.23, p.16. <http://p1232.nysed.gov/mgtserv/documents/LOCKPORTCITYSD.pdf>

101　New York Civil Liberties Union, [Letter to the Commissioner of New York State Education Department] 2018.6.18. <https://www.nyclu.org/sites/default/files/field_documents/june18_2018_nyclu_letter_re_lockport_city_school_district.pdf>

102　Connor Hoffman, “Lockport school officials review draft privacy policy,” *Lockport Union-Sun & Journal*, 2018.11.7. <https://www.lockportjournal.com/news/local_news/lockport-school-officials-review-draft-privacy-policy/article_8bd46eb0-8342-5b6c-a2d7-a80a62f5d7bd.html>

103　California Consumer Privacy Act of 2018 (AB-375 (2017-2018), Civil Code (CIV) Division 3, Part 4, TITLE 1.81.5.) <https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375>

である。生体情報は、同法の保護や規制の対象となる「個人情報」（personal information）[104]の1つとして、「個人を特定するために、それ単体又は他の特定データとの組合せで用いられる、DNAを含む、個人の生理学的、生物学的又は行動上の特徴」[105]と定義された。その例として、虹彩、網膜、指紋、顔、手、掌、静脈パターンの画像や声記録が挙げられている。消費者が、消費者の個人情報を収集する事業者に対して、収集した個人情報のカテゴリーや具体的内容（specific pieces）の公開を要求する権利を持つことが明記されるとともに、消費者の情報を収集する事業者が、個人情報取得時あるいはその前に、収集する個人情報の内容や目的を消費者に通知することが義務付けられた[106]。また、消費者から個人情報を収集した事業者に対して消費者が自らの情報を削除するよう要求する権利や、第三者に販売する際には消費者が個別に拒否（オプトアウト）できる権利が明記された[107]。

また、地方自治体レベルでも近年、様々な条例が成立している。バークレー市では2018年3月、市議会が全会一致で、「監視技術及びコミュニティ安全条例」[108]を可決した[109]。市の機関が監視技術を新たに利用する際に市議会の承認を得ることを義務付けた。その際に、新たに設置する監視技術がコミュニティへもたらす便益が費用を上回ること、意図した目的を達成した上で市民の自由や権利を最大限保護していること、同様の便益があり、市民の権利や自由への影響がより小さい実行可能な代替案が存在しないことを示さなければならない[110]。条例の対象となる「監視技術」は、「個人やグループに具体的に関連させた、又は、関連させうる音声、電子、視覚、位置、熱量、嗅覚、生体その他同様の情報を収集する」[111]様々なシステムであり、具体例として、顔認識ソフトウェア、身体装着カメラ、ナンバープレート自動読み取り装置、銃声検出マイクロフォン等が挙げられている。

デービス市でも市議会において2018年3月、「監視技術条例」[112]が可決され、監視技術を購入・使用する警察他の市の機関は、当該機器に、市民の自由への起こりうる侵害を上回る便益があることを示さなければならないとされた[113]。

オークランド市の市議会では、2018年5月15日、「監視及びコミュニティ安全条例」[114]が

---

[104] CIV §1798.140.(o)(1)(E)

[105] CIV §1798.140.(b) 原文は次のとおりである。“Biometric information” means an individual’s physiological, biological or behavioral characteristics, including an individual’s deoxyribonucleic acid (DNA), that can be used, singly or in combination with each other or with other identifying data, to establish individual identity.

[106] CIV §1798.100.(a), (b) なお、通知方法については特に指定されていない。

[107] CIV §1798.105.(a), §1798.120.(a)

[108] Surveillance Technology and Community Safety Ordinance (Ordinance No.7,592–N.S., Berkeley Municipal Code (BMC) Chapter 2.99)

[109] “3/27/2018; CLK - Ordinance; City Council; 7592; ; Surveillance Technology Use and Community Safety; Adding BMC Chapter 2.99,” City of Berkeley’s Records Online website <https://www.cityofberkeley.info/recordsonline/api/Document/AW5MrAQ1d7tLolsClZ5bBeGTtL%C3%898adqjxSS8KN5XxbXLKqpg9TXuIucnrZuW0qQPNG%C3%89hAeB%C3%81YXrYTrPOEeghDj0%3D/>

[110] BMC §2.99.060.

[111] BMC §2.99.020.1. 原文は次のとおりである。“Surveillance Technology” means an electronic device, system utilizing an electronic device, or similar technological tool used, designed, or primarily intended to collect audio, electronic, visual, location, thermal, olfactory, biometric, or similar information specifically associated with, or capable of being associated with, any individual or group.

[112] Surveillance Technology Ordinance (2018 Ordinance No.2527, Davis Municipal Code Article 26.07) Quality Code Publishing website <https://qcode.us/codes/davis/view.php?topic=26-26_07>

[113] Steve Milne, “Davis To Regulate Hi-Tech Surveillance Steve Milne,” 2018.3.21. Capital Public Radio website <http://www.capradio.org/111753>

[114] Surveillance and Community Safety Ordinance (Oakland Municipal Code Chapter 9.64) Municode Library website <https://library.municode.com/ca/oakland/codes/code_of_ordinances?nodeId=TIT9PUPEMOWE_CH9.64REACUSSUTE>

採択された[115]。条例では、市の機関が新しい監視技術について市議会に承認を求める際には、事前に、オークランドの市民主導のプライバシー助言委員会（Privacy Advisory Commission: PAC）に「監視影響報告書」（Surveillance Impacts Report）と「監視利用ポリシー」（Surveillance Use Policy）を提出することを義務付けている。PAC は市議会に対して、採択、修正、拒否を勧告する。監視影響報告書は、監視技術が市民の権利や自由に与える影響―特に監視技術が差別的な形で、又はアルゴリズムによるバイアスがある形で利用されていないかどうか―をチェックし、それらの影響を軽減できる技術的、手続的な方策を特定する。監視利用ポリシーは主に、監視技術により収集されるデータの扱いについて定めるものである。「監視技術」の定義はバークレー市のものとほぼ同じである。

Ⅱ　英国

英国は 1990 年代以降、監視カメラ大国になったが[116]、顔認識技術の利用はまだ始まったばかりである。1998 年に、ロンドン（ニューアム区）が、公共の場にある監視カメラ（CCTV）で顔認識技術を使った世界で初めての自治体になったとされる[117]。しかし、顔認識技術が注目を集め始めたのは、近年、法執行機関が、人が集まるイベントを対象にライブ映像を使った顔認識技術の利用の試行を始めてからである。顔認識技術の有効性とガバナンスに関して大きな議論が起こっている。1995 年の EU データ保護指令を受けて制定された「1998 年データ保護法」[118] には「生体データ」に関する明示的な規定はなかった。しかし、2016 年に制定された EU 一般データ保護規則（General Data Protection Regulation: GDPR）（第Ⅳ章参照）を受けて、GDPR 施行直前の 2018 年 5 月に「2018 年データ保護法」が成立した[119]。同法第 205 条は生体データ（biometric data）を定義するとともに、GDPR と同様に、扱いにより慎重を期し保護の対象となるべき特別な種類の個人データの１つとして位置付けている[120]。

１　法執行

(1) 生体データのガバナンス

内務省（Home Office）は、国境管理や犯罪防止、対テロ活動、警察活動を所管しており、それらにおいて生体認証技術、特に顔認識技術の利用を推進している。2010 年に成立したデービッド・キャメロン（David Cameron）政権以降、市民的自由やプライバシーへの影響を懸念する市民団体からの反対運動などを受け、規制を強化する方向に進んだ。2012 年に成立した「2012

---

[115] “PAC Surveillance Technology Ordinance Approved by City Council,” City of Oakland website <https://www.oaklandca.gov/resources/pac-surveillance-technoloy-ordinance-approved-by-city-council>

[116] 例えば、2013 年時点で、英国全土に 600 万台の監視カメラがあると推計されている。Surveillance Camera Commissioner, *Annual Report 2016/17,* 2018.1, pp.12-13. <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/672286/CCS207_CCS0118716124-1_Annex_A_-_AR_2017-_web.pdf>

[117] Greig Watson, “Facial recognition: the death knell of anonymity?” 2014.8.26. BBC website <http://www.bbc.com/news/uk-england-28307929>

[118] Data Protection Act 1998 (1998 c. 29) legislation.gov.uk website <https://www.legislation.gov.uk/ukpga/1998/29>

[119] Data Protection Act 2018 (2018 c. 12) *idem* <http://www.legislation.gov.uk/ukpga/2018/12>

[120] “Special category data.” Information Commissioner's Office website <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/>

年自由保護法」[121]は、第1部が生体データの規制、第2部が監視（Surveillance）の規制を扱っている。前者では、「1984年警察及び刑事証拠法」（Police and Criminal Evidence Act 1984）を改正するという形で、採取された指紋とDNA型（DNA profiles）が破棄される条件（言い換えると、保持できる条件）が明記された。後者では、内務大臣に対して、監視カメラシステムの開発、使用、そして得られた画像等の情報の利用や加工などに関する行動規範（Code of Practice）を作成することが命じられた。また、内務大臣が生体認証データと監視それぞれにコミッショナーを指名することが定められ、「生体認証試料の保持と利用のためのコミッショナー」（通称「生体認証コミッショナー」（Biometrics Commissioner））と「監視カメラ・コミッショナー」（Surveillance Camera Commissioner: SCC）が置かれることになった。

生体認証コミッショナーの役割は、警察によるDNAサンプル、DNA型、指紋の保持と利用について第三者の立場で審査することであり、内務大臣に年次報告書を提出する。顔認識や声紋認識といった「第2世代の生体認証技術」は、2012年自由保護法の対象外であり、ガバナンス体制や法律の整備が遅れていることが年次報告書で指摘されている[122]。

監視カメラ・コミッショナーの役割は、監視カメラ行動規範（Surveillance Camera Code of Practice）[123]の遵守を関係機関に促すこと、行動規範が機能しているかどうかを審査すること、そして、行動規範を改訂すべきかどうか関係機関に助言することである[124]。監視カメラ行動規範は2013年6月に策定された。その中で、システム運用者が従うべき12の指針原則が示された。生体認証技術については、例えば、「原則2：監視カメラシステムを使用する際は、その目的が正当なものであり続けているか、定期的にレビューしながら、人々及び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ない」において、「顔認識を含む生体認証技術を利用する場合には必ず、目的を達成するに当たってそれらの利用が明らかに正当化され、目的に照らしてバランスの取れたものであり、妥当性が検証されている必要がある」としている。システム運用者が妥当性を検証する際には、監視カメラ・コミッショナーが適宜助言を行う。また、この原則2を達成するためには「データ保護影響評価」（Data Protection Impact Assessment: DPIA）[125]を実施する必要があることも指摘されている。データベースとの照合に触れた「原則12：照合目的で参照データベースと比較する監視カメラシステムを支援するために使用されるあらゆる情

---

[121] Protection of Freedoms Act 2012 (2012 c. 9) <http://www.legislation.gov.uk/ukpga/2012/9/contents/enacted>; 河島太朗「【イギリス】2012年自由保護法の制定」『外国の立法』No.253-2, 2012.11, pp.6-7. <http://dl.ndl.go.jp/view/download/digidepo_3948086_po_02530203.pdf?contentNo=1>

[122] *Commissioner for the Retention and Use of Biometric Material: Annual Report 2017*, Office of Biometrics Commissioner, 2018.3. <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/714054/CCS207_CCS0518559084-1_Biometrics_Commissioner_s_ARA_FINAL_WEB_version.pdf>

[123] 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>　2012年自由保護法第30条の手続規定に従い、議会の承認を受けた上で、同規範の効力発生等を定める命令も出されている。このため、単なるガイドラインではなく、政府関係機関に対しては遵守が義務付けられている。The Protection of Freedoms Act 2012 (Code of Practice for Surveillance Camera Systems and Specification of Relevant Authorities) Order 2013 legislation.gov.uk website <http://www.legislation.gov.uk/uksi/2013/1961/made>

[124] SCCの事務局は、内務省に雇用された4人のスタッフメンバーから成る。“Publication scheme - Surveillance Camera Commissioner.” GOV.UK website <https://www.gov.uk/government/organisations/surveillance-camera-commissioner/about/publication-scheme>

[125] 行動規範ではPIA（Privacy Impact Assessment）となっているが、GDPRに合わせて1998年データ保護法が改正され、現在の2018年データ保護法の下では、DPIAと名称が変わっている。なお、監視カメラ・コミッショナーは、2018年10月に、テンプレートを含む、監視カメラのDPIAに関するガイダンス文書を公表している。“Data protection impact assessments for surveillance cameras,” 2018.10.22. GOV.UK website <https://www.gov.uk/government/publications/data-protection-impact-assessments-for-surveillance-cameras>

報は正確かつ最新のものに保たれなければならない」では、顔認識技術の利用が例示されている。監視カメラ行動規範では、商用や住宅用の監視カメラは対象外であるため、それらについては、行動規範を自発的に採用してもらうことが期待されているだけであったが、監視カメラ・コミッショナーは、行動規範を遵守していることを第三者認証する制度を2015年11月に立ち上げた[126]。認証は1年間有効な部分認証と3年間有効な完全認証から成る。認証を受けた組織は、認証マークをウェブサイトに掲載することができる。

他方、1998年データ保護法に基づき、個人情報保護を監督する独立機関として設置された「情報コミッショナー」（Information Commissioner）も、2000年にCCTVに関する行動規範を策定しており、これは商用や住宅用も含めた全てのCCTVを対象としている。行動規範は、2008年、2015年に改訂され、さらに2017年にVer.1.2が出ている[127]。Ver.1.2では、技術の進展を反映して、ビデオテープに映像が記録される点だけでなく、「デジタル技術やポータブル技術を使った、より洗練された運用」に焦点が当てられ、第7節「CCTVシステム以外の監視技術」では、自動ナンバープレート認識システム（Automatic Number Plate Recognition: ANPR）、身体装着ビデオ（Body Worn Video: BWV）、無人航空システム（ドローン）、自動認識システム（顔認識技術）が取り上げられた。多くのケースにおいて、DPIA（PIA）を実施することが強く推奨されている。

このように、英国では、3人のコミッショナーが生体認証技術を監督していることになっている。しかし、2012年自由保護法の第1部の生体認証データの規制では、指紋とDNA型が対象となっており、第2部の監視の規制では、CCTVに加えて「他の監視カメラ技術」として、「得られた写真や他の情報の利用や加工」とは書かれているものの、顔認識技術そのものは明示的には書かれていないため、指紋とDNA型以外の生体認証技術、特に顔認識技術を誰が中心になって監督するのかが明確ではない。結果として、顔認識技術の利用に関しては、利用を推進する立場の内務省に加えて、生体認証コミッショナー、監視カメラ・コミッショナー、そして情報コミッショナーがそれぞれの立場から監督を担っているといえる[128]。

これらの法定機関以外にも、内務省は、勾留写真の扱いや顔認識技術の利用にも関連する法科学を所管する部門に対して、助言や指導を行う「法科学レギュレーター」（Forensic Science Regulator: FSR）を設置している。また、内務省は、生体認証技術に関して助言を行う政府外公共機関（Non-Departmental Public Body: NDPB）[129]として、「生体認証及び法科学倫理グループ」

126　英国認証機関認定審議会（United Kingdom Accreditation Service: UKAS）が認定した3つの 認証機関による。“Surveillance camera code of practice: third party certification scheme.” GOV.UK website <https://www.gov.uk/government/publications/surveillance-camera-code-of-practice-third-party-certification-scheme>

127　Information Commissioner's Office, *In the picture: A data protection code of practice for surveillance cameras and personal information*, Version 1.2, 2017.6.9. <https://ico.org.uk/media/1542/cctv-code-of-practice.pdf> なお、2018年データ保護法に対応した更新はまだ行われていないが、指針の内容の大部分が有効であることが注記されている。

128　なお、情報コミッショナーと監視カメラ・コミッショナーは「効果的な協力を確保する」ために覚書を結んでいる。lnformation Commissioner and Surveillance Camera Commissioner, “Memorandum of Understanding,” 2017.9.5. <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/640381/SCC_MOU_2017.pdf>

129　*The Cabinet Manual: A guide to laws, conventions and rules on the operation of government*, 1st ed., 2011.10, p.27. <http://www.cabinetoffice.gov.uk/sites/default/files/resources/cabinet-manual.pdf> 政府外公共機関は、「国の統治の過程において一定の役割を担う機関であるが、政府省庁又はその一部ではなく、程度の差はあれ大臣から距離を置き運営する」機関で、「通常、制定法上の機関のように、別個の法主体として設置され、公務員ではない職員を独自に雇用する」ものである。非省庁公的機関、非省公的組織などとも訳される。政府外公共機関は、エージェンシー（executive agency）とは異なる組織である。エージェンシーは、「特定の成果の達成に焦点を当てて明確に定義された組織」であって、「省庁の一部であり、公務員が職員を務める」ものである（国立国会図書館調査及び立法考査局『英国の内閣執務提要』（調査資料2012-4）2013, p.62. <http://dl.ndl.go.jp/info:ndljp/pid/8091534>）

（Biometrics and Forensics Ethics Group: BFEG）を設置している[130]。さらに、内務省は、後述するように、顔認識技術の監視と助言を行う委員会を新たに設置する方針を示している。

(2) 生体情報データベース

次に、警察活動で利用可能な生体情報データベースの現状をまとめる。

DNA 型のデータベースである全国 DNA データベース（National DNA Database: NDNAD）は内務省が管理している。NDNAD は 2 種類のデータベースを持っており、1 つは逮捕時に採取される逮捕者のもの、もう 1 つは犯行現場等から科学捜査班（Crime Scene Investigation: CSI）が採取したものである。2018 年 9 月末までに英国全体でおよそ 544 万人分の DNA 型が登録されている[131]。8 割が男性であり、年齢層別のデータも公開されている。2001 年 4 月から 2017 年 3 月までに、未解決事件に対して、犯行現場で採取された試料とデータベースの間でおよそ 64 万件の照合が行われた[132]。

指紋データベースである「全国自動指紋識別システム」（National Automated Fingerprints Identification System: NAFIS）の運用は 1999 年から始まり、2004 年に “IDENT1” となり、内務省が管理している。指紋はほとんどの場合、ライブスキャン（Livescan）と呼ばれる機器によって電子的に採取されている。データベースには 2 つのタイプの指紋が記録されている。1 つは個人から逮捕時に取得されたものであり、もう 1 つは犯行現場から科学捜査班（CSI）が採取したものである。2017 年 3 月末現在、およそ 790 万人の指紋が IDENT1 に登録されており、そのうち犯行現場から採取された指紋がおよそ 229 万件登録されている[133]。

英国にはもう 1 つ、「入国及び庇護生体認証システム」（Immigration and Asylum Biometric System: IABS）と呼ばれる指紋及び顔写真のデータベースが存在し、外国人が英国への入国や庇護を希望する際に採取される。IABS は、当該人物が ID を示す手段が他にない場合に限り、利用されている。職務質問した相手が ID を証明するものを何も持っていない場合、これまでは警察署まで同行してもらい、指紋採取していたため、数時間を要していた。携帯式[134]を導入することで大幅に時間節約となる。また、犯罪容疑者だけでなく、意識不明者、医療処置が必要な人、死者に対しても有効だと考えられている。

データベースに収録された DNA 型と指紋の保持期間は、2012 年自由保護法で定められている。DNA 型に関しては、「全国 DNA データベース戦略委員会」（National DNA Database Strategy

---

[130] 議長を含め 13 名で構成される。“Biometrics and Forensics Ethics Group Membership.” GOV.UK website <https://www.gov.uk/government/organisations/biometrics-and-forensics-ethics-group/about/membership> もともとは、2008 年に「全国 DNA データベース倫理グループ」（National DNA Database Ethics Group: NDNAD EG）として設置されたが、顔や指紋を含む全ての識別技術を対象にすべきであるとして 2017 年 7 月に改組された。“Biometrics and Forensics Ethics Group replaces the National DNA Database Ethics Group,” 2017.8.16. GOV.UK website <https://www.gov.uk/government/news/biometrics-and-forensics-ethics-group-replaces-the-national-dna-database-ethics-group>

[131] “DNA statistics as of 30th September 2018.” GOV.UK website <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/747846/NDNAD_website_statistics_Q2_18-19-2.ods> これは、英国全体での数値である。イングランドとウェールズに限定した DNA 型はおよそ 497 万人分である。

[132] National Police Chiefs' Council and Home Office, *National DNA Database Strategy Board Annual Report 2016/17*, 2018.7, p.5. <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/724596/040718_new_CCS0518718592_National_DNA_Database_Strategy_Board_AR_2016-17_updates_NEW.pdf>

[133] *ibid*., p.37.

[134] 内務省が、警察官が IDENT1 と IABS の両データベース（1200 万件）を 1 分以内で容易に検索できる携帯式の指紋採取システム（アプリ）を開発し、ウェストヨークシャー警察がこれを試行したことが 2018 年 2 月に報じられている。Matt Reynolds, “UK police are now using fingerprint scanners on the streets to identify people in less than a minute,” 2018.2.10. Wired website <https://www.wired.co.uk/article/uk-police-handheld-fingerprint-scanner-database-biometric-security>

Board）が、法律・運用・政策・倫理、及びプライバシーの観点から監督していたが[135]、2016年に公表された「法科学戦略」（Forensic Science Strategy）[136]において、指紋もカバーすることとされ、名称も「法科学情報データベース戦略委員会」（Forensic Information Databases Strategy Board: FINDS-SB）に変わった[137]。FINDS-SBは、警察が、DNA型と指紋について、それらの採取から、利用、保持、そして破棄に至るまでどのように行っているかを監督している。

警察が利用する顔写真のデータベースである「全国警察データベース」（Police National Database: PND）[138]には、イングランド、ウェールズ、北アイルランドで逮捕、勾留された人々の顔写真が含まれている[139]。PNDは2011年に正式に立ち上がり、2014年に内務省は顔検索機能（facial search functionality）をPNDに導入した。しかし、これは人による評価を必要としたため、顔認識（facial recognition）とは呼ばれなかった[140]。その後、PNDに含まれている勾留時の顔写真は、2016年7月時点で1900万件に上り（重複分を含む。）、このうち1600万件以上が顔認識ソフトウェアを使って検索可能な状態になっている[141]。

勾留時の顔写真にはその後有罪判決を受けた人だけでなく、起訴されなかった人々の顔写真も含まれていることが問題視されていたが、2012年6月、高等法院（High Court）は、ロンドン警視庁が逮捕した、チェルシー在住の60歳の女性（RMCと呼ばれた）と、ペッカム在住の12歳の少年（FJと呼ばれた）の勾留写真を、不起訴にもかかわらず保持していることについて人権侵害であると判示した[142]。これに対して、2017年2月、内務省は、顔写真の利用と保持

---

[135] 2012年自由保護法第24条による。

[136] Home Office, *Forensic Science Strategy: A national approach to forensic science delivery in the criminal justice system*, Cm 9217, 2016.3. <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/506652/54493_Cm_9217_Forensic_Science_Strategy_Accessible.pdf>

[137] Home Office, *Forensic Information Databases Service(FINDS): The Forensic Information Databases Strategy Board Policy for Access and Use of DNA Samples, DNA Profiles, Fingerprint Images, and Associated Data*, 2018.6.7, p.4. <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715318/FINDS-SB-P-002_-_Issue_1_-_FINDS_Strategy_Board_Policy_Access_and_Use_Po....pdf>

[138] 2002年に起きたケンブリッジ州ソーアムで起きた殺人事件を受けて行われた独立調査の結果、警察間での情報共有が不十分だったことが要因の1つであったと結論付けられたことが契機となった。Jennifer Scott, “NPIA launches Police National Database,” 2011.6.23. ITPRO website <https://www.itpro.co.uk/634408/npia-launches-police-national-database>

[139] “Police unlawfully retaining custody images, claims Norman Lamb,” 2018.2.6. BBC website <https://www.bbc.com/news/uk-politics-42961025> なお、イングランド及びウェールズにおいて警察が逮捕又は勾留する際に逮捕者の顔写真を撮影する法的根拠は、1984年警察及び刑事証拠法（Police and Criminal Evidence Act 1984 (1984 c.60) legislation.gov.uk website <https://www.legislation.gov.uk/ukpga/1984/60>）第64A条による。

[140] 2015年6月、レスターシャー警察がダービー（Derby）で開催された音楽フェスティバルに集まった9万人の顔を撮影し、地元警察のデータと照合したと報じられたが、これは誤報であり、当時、レスターシャー警察はPNDの顔検索機能を利用しておらず、またPNDの顔検索機能も上記のような利用方法は不可能であったとされる。Her Majesty's Inspectorate of Constabulary in Scotland, *Audit and Assurance Review of the use of the Facial Search functionality within the UK Police National Database (PND) by Police Scotland*, 2016.1, p.12. <https://www.hmics.scot/sites/default/files/publications/HMICS%20Audit%20and%20Assurance%20Review%20of%20the%20use%20of%20the%20Facial%20Search%20functionality%20within%20the%20UK%20Police%20National%20Database%20%28PND%29%20by%20Police%20Scotland_0.pdf>

[141] Home Office, *Review of the Use and Retention of Custody Images*, 2017.2, p.2. <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/594463/2017-02-23_Custody_Image_Review.pdf>

[142] RMCは、歩道を自転車で通行していたところを止めた地域支援担当官（Community Support Officer）に対する傷害の容疑について2007年に出頭し、逮捕され、DNA型、指紋、顔写真が採取された。その後、不起訴が決定されたが、ロンドン警視庁は彼女の記録を破棄しなかった。FJは、またいとこをレイプした容疑で2009年に逮捕されたが、第三者の目撃によって犯罪を確定できなかったために起訴されなかった。この事件で、ロンドン警視庁は、彼のDNA型や指紋、顔写真、逮捕記録を破棄しなかった。RMC and FJ v Commissioner of Police for the Metropolis and Secretary of State for the Home Department [2012], EWHC 1681 (Admin). <https://www.judiciary.uk/wp-content/uploads/JCO/Documents/Judgments/r-rmc-fj-metropolitan-police-commissioner-22062012.pdf>

の見直しを発表して、（逮捕はされたが）有罪と確定しなかった人々が全ての警察データベースから顔写真を削除されることを要求する権利を有するとして、要求に応じて、保持している無実の人々の顔写真を削除するように警察に命じた[143]。これに対して、プライバシー擁護団体等は、原則として歓迎しつつも、政府の対応が遅すぎたことに加えて、（DNA 型や指紋のように）わざわざ要求しなくても、データベースから自動的に削除されるようにすべきであると主張した[144]。しかし、PND では、写真と逮捕等の記録情報は連結されていないため、削除するためには写真を 1 件ずつ確認しなければならず、膨大な時間と費用がかかるとされる[145]。

なお、内務省は、PND と逮捕等の記録情報のデータベースである「全国警察コンピュータ」（Police National Computer: PNC）を統合した次世代システム「法執行データサービス」（Law Enforcement Data Service: LEDS）の 2020 年の導入を目指し、現在開発を進めている。内務省は、LEDS では、顔写真と逮捕者公訴等の記録情報が連結され、自動化された DNA 型や指紋と同じように、顔写真の効率的な削除も可能になると説明している[146]。

（3）生体認証戦略の公表と関連する動向

内務省は、当初計画されていた 2013 年末から大幅に遅れて、2018 年 6 月に「生体認証戦略」（Biometrics Strategy）を公表した[147]。生体認証戦略は、生体認証技術を「生物学的特性や行動データの計測と分析に基づいて人々を認識すること」[148] と定義し、利用方法を固定（fixing）、確認（verification）、識別（identification）の 3 通りに整理している。なお、固定は、生体情報を登録して経歴等の情報とひも付けることを指している。内務省の生体認証プログラムでは、DNA 型と指紋に加えて、顔写真もスコープ内に明記された。また、人々の信頼を維持するため、ガバナンス、プライバシー保護、倫理、監督と基準に関する内務省の取組方針を示している（表 4）。

---

[143] Home Office, *Review of the Use and Retention of Custody Images*, 2017.2, pp.5-6. <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/594463/2017-02-23_Custody_Image_Review.pdf>

[144] NGO 団体ビッグブラザーウォッチのレナーテ・サムソン（Renate Samson）氏のコメントによる。Alan Travis, “Police told to delete on request millions of images of innocent people,” *Guardian*, 2017.2.24. <https://www.theguardian.com/uk-news/2017/feb/24/police-told-to-delete-on-request-images-of-innocent-people>

[145] *ibid*.

[146] Home Office, *Biometrics Strategy: Better public services Maintaining public trust*, 2018.6, pp.11-12. <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/720850/Home_Office_Biometrics_Strategy_-_2018-06-28.pdf>; House of Commons Science and Technology Committee, *Biometrics strategy and forensic services: Government's Response to the Committee's Fifth Report*, Eighth Special Report of Session 2017–19, 2018 HC 1613, 2018.10.15, p.4. <https://publications.parliament.uk/pa/cm201719/cmselect/cmsctech/1613/1613.pdf>

[147] Home Office, *op.cit.*[141] 政府は 2013 年に「バイオメトリック及び法科学戦略」を同年末までに公表することを約束したが延期され、2015 年 3 月、さらには 2015 年末ということになり、その後、2 つに分離することになり、2016 年 3 月に「法科学戦略」だけが先行して公表された。House of Commons Science and Technology Committee, *Biometrics strategy and forensic services*, Fifth Report of Session 2017–19, 2018 HC 800, 2018.5.25, p.16. <https://publications.parliament.uk/pa/cm201719/cmselect/cmsctech/800/800.pdf>

[148] Home Office, *op.cit.*[146], p.5. 原文は次のとおりである。“the recognition of people based on measurement and analysis of their biological characteristics or behavioural data”

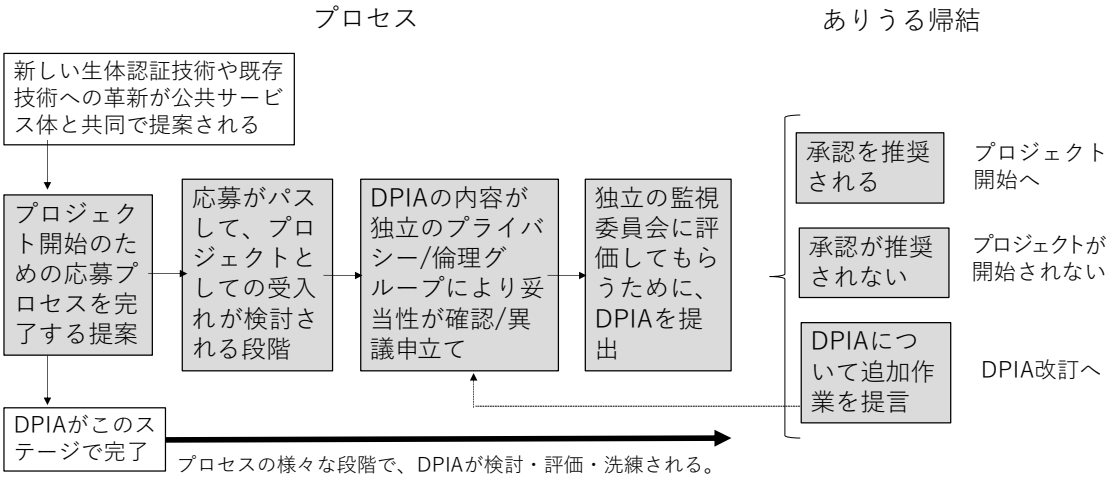
表４　「生体認証戦略」で示された信頼維持に向けた内務省の取組方針

・法執行機関による顔写真や顔認識技術の利用について監督と助言を行う委員会を新たに設置する。 ・新しい生体認証技術を導入し、又は既存生体認証技術の新しい応用を行おうとする場合は必ず、EU の一般データ保護規則（GDPR）と 2018 年データ保護法に基づくデータ保護影響評価（DPIA）を実施する。 ・生体認証及び法科学倫理グループ（BFEG）が、顔認識技術を含む新しい生体認証技術の応用に伴う倫理的な問題を検討する。 ・生体認証技術の監督について、生体認証コミッショナー、監視カメラ・コミッショナー、法科学レギュレーター、情報コミッショナーと協働する。 ・関係機関とも協議の上で、内務省とその所管機関を横断した生体認証技術のガバナンスと監督の見直しを 12 か月以内に行う。

（出典） Home Office, *Biometric Strategy: Better public services Maintaining public trust*, 2018.6, pp.13-18. <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/720850/Home_Office_Biometrics_Strategy_-_2018-06-28.pdf> を基に筆者作成。

内務省のデータ保護影響評価（DPIA）の実施プロセスは図１のように説明されている。

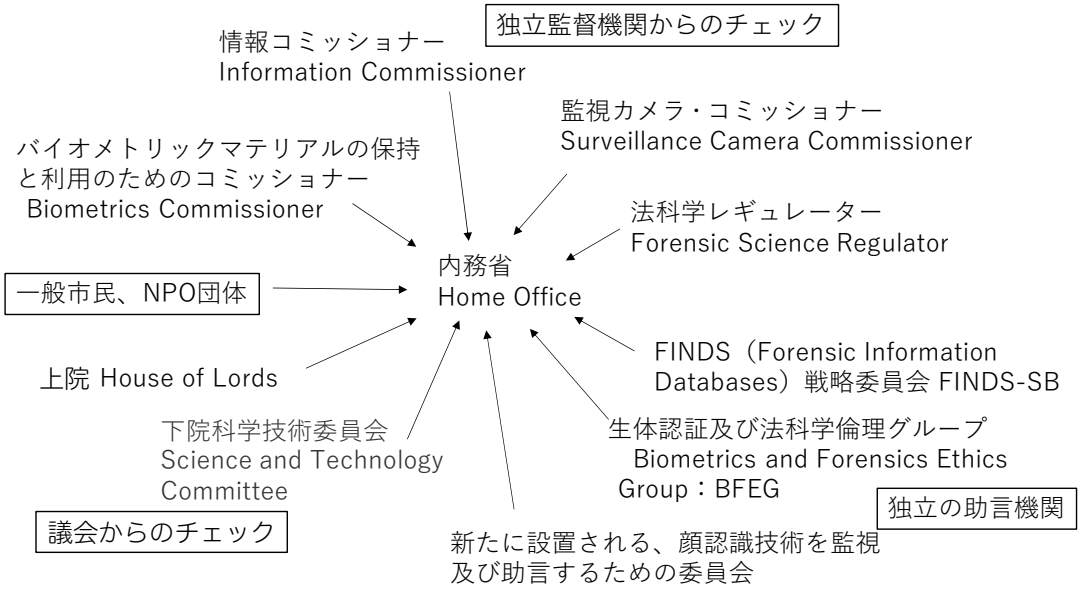
図１　新しい生体認証技術の導入や既存生体認証技術の新しい応用を行う際の内務省のプロセス



（出典） Home Office, *Biometric Strategy: Better public services Maintaining public trust*, 2018.6, p.16. (Figure 3) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/720850/Home_Office_Biometrics_Strategy_-_2018-06-28.pdf> を基に筆者作成。

生体認証戦略で示されているとおり、生体認証技術、特に近年、警察等の法執行機関で採用が進んでいる顔認識技術について、様々な組織が関わっているため、各組織の権限や責任が複雑化している（図2）。

図２　警察による生体認証技術の監督を巡るステークホルダー



（出典） Home Office, *Biometric Strategy: Better public services Maintaining public trust*, 2018.6, pp.21-27. <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/720850/Home_Office_Biometrics_Strategy_-_2018-06-28.pdf> 等を基に筆者作成。

ガバナンス上の複雑さや問題点について、2018年、議会で活発な議論が交わされた。2018年3月1日、貴族院（上院）において、緑の党のジェニー・ジョーンズ（Jenny Jones; Baroness Jones of Moulsecoomb）議員が、「セキュリティと警察活動：顔認識技術」について質問を行った[149]。議員の問題意識は、自動顔認識技術（Automated Facial Recognition: AFR）が、十分な法律、監督、政策がない状況で利用されていて、効果もなく、差別的になりうるという点にあり、政府に対して、自動顔認識技術の利用の中断と、有罪とされなかった人々の顔写真の消去を求めた。

また、庶民院（下院）の科学技術委員会は、「生体認証戦略と法科学サービス」をテーマに調査を行い、生体認証戦略に盛り込まれるべき事項を指摘するとともに、法科学サービス（forensics services）の現況をレビューした報告書を、生体認証戦略が公表される1か月前である2018年5月にとりまとめた[150]。報告書では、2016年3月に内務省が発表した法科学戦略の改訂も必要であることが指摘された。また、2012年自由保護法が規制対象とする生体情報は、指紋とDNA型だけであるが、顔写真など他のモダリティも含むようにする必要があることを指摘している。

---

[149] “Security and Policing: Facial Recognition Technology,” *House of Lords Hansard*, Vol.789, 2018.3.1. <https://hansard.parliament.uk/Lords/2018-03-01/debates/0AD45D64-63CB-458F-B9B1-A41B2887C051/SecurityAndPolicingFacialRecognitionTechnology>　これは「短時間討論のための質問」（Question for Short Debate）として行われたものであり、同議員の質問に対し、スーザン・ウィリアムズ（Susan Williams, Baroness Williams of Trafford）内務省閣外大臣（副大臣）が答弁した。なお、短時間討論のための質問制度については、次が詳しい。濱野雄太「イギリスの議会質問制度」『調査と情報―ISSUE BRIEF―』No.1028, 2018.12.6, p.11. <http://dl.ndl.go.jp/view/download/digidepo_11195783_po_IB1028.pdf?contentNo=1>

[150] House of Commons Science and Technology Committee, *op.cit.*[147]

また、情報コミッショナーのエリザベス・デンハム（Elizabeth Denham）氏は、2018年5月14日付のブログ記事において、「顔認識技術が合法的であるためには、警察は、公共空間での顔認識技術の利用が、対処しようとしている問題の解決に有効であり、当該問題に対処するために顔認識技術よりも侵襲度合いの少ない技術や方法が利用できないことを示す明確なエビデンスを示さなければならない」とし、さらに「もし私の懸念が適切に対処されなければ、私は、人々を適切に保護するために法的措置が必要だと考えるだろう」と述べた(151)。そして、12月には、情報コミッショナーが正式に調査を開始したことが報じられた(152)。

このほか、2018年には警察による自動顔認識技術の利用に対して書面による2件の反対声明が出され、いずれも利用が続く場合は高等法院への提訴の用意があるとした(153)。訴訟費用はクラウドファンディング・サイトで集められた。1件は、ウェールズの首都カーディフの市民によるもので、人権団体リバティ（Liberty）が支援している。2018年6月、サウスウェールズ警察の警察署長宛てに、兵器見本市への平穏な抗議や買い物中に自動顔認識システムにより追跡されたとする書面を提出している(154)。もう1件は、市民的自由やプライバシー保護の活動を行っているNGOビッグブラザーウォッチ（Big Brother Watch）と緑の党のジョーンズ上院議員によるもので、内務大臣とロンドン警視庁総監に、自動顔認識の利用を停止するように書面で求めている(155)。ロンドン警視庁とサウスウェールズ警察の動向については以下にまとめた。

２　ロンドン警視庁

ロンドン警視庁（Metropolitan Police Service: MPS）(156)は近年、顔認識ソフトウェアを利用した顔のスキャン（自動顔認識と呼ばれる）を試行している(157)。最初の試行は、2016年8月にノッティングヒル・カーニバルで実施された。1年後の同カーニバルでも同様に実施された。これに対して、2017年8月、生体認証コミッショナーは、①適切な事後評価とその公表が必須であること、②警察の顔写真データベースを統合し、正確性や有用性を評価すること、③法規制の枠組みや独立組織による監督が必要であること等を指摘したコメントを発表した(158)。

その後も、2017年11月にホワイトホールのセノタフ（戦没者記念碑）前で開催された「リメ

(151)　Elizabeth Denham, “Blog: facial recognition techology and law enforcement,” 2018.5.14. Information Commissioner’s Office website <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/05/blog-facial-recognition-technology/>

(152)　Natasha Bernal, “Britain's data commissioner launches investigation into UK use of facial recognition,” *Telegraph*, 2018.12.8. <https://www.telegraph.co.uk/technology/2018/12/03/britains-data-commissioner-launches-investigation-uk-use-facial/>

(153)　Owen Bowcott, “Police face legal action over use of facial recognition cameras,” *Guardian*, 2018.6.14. <https://www.theguardian.com/technology/2018/jun/14/police-face-legal-action-over-use-of-facial-recognition-cameras>

(154)　Ed Bridges, “End lawless and dangerous police use of facial recognition technology,” crowdjustice website <https://www.crowdjustice.com/case/facial-recognition/>

(155)　Big Brother Watch, “Stop the Met Police using authoritarian facial recognition cameras,” crowdjustice website <https://www.crowdjustice.com/case/face-off/>

(156)　ロンドン警察が所管するシティ・オブ・ロンドン（シティともいう。）を除く、グレーター・ロンドン・オーソリティー（Greater London Authority: GLA. 大ロンドン庁ともいう。）内の警察実務を担当する機関である。

(157)　“Live Facial Recognition trial.” Metropolitan Police website <https://www.met.police.uk/live-facial-recognition-trial/> なお、NECのNeoFaceが採用されている。

(158)　Biometrics Commissioner, “Metropolitan Police’s use of Facial Recognition Technology at the Notting Hill Carnival, 2017,” 2017.8.23. GOV.UK website <https://www.gov.uk/government/news/metropolitan-polices-use-of-facial-recognition-technology-at-the-notting-hill-carnival-2017>

ンバランス・デー」（戦没者追悼記念式典）などで、自動顔認識の試行が続けられた[159]。

こうした動きに対し、グレーター・ロンドン・オーソリティー[160]を構成するロンドン議会のGLA監督委員会（GLA Oversight Committee）[161]は、ロンドン市長（Mayor of London）宛ての2017年11月14日の書簡[162]と2018年2月7日の書簡[163]において、ロンドン警視庁の顔認識技術の利用について、「明確な法規制枠組みが確立され、また市長公安室（Mayor's Office for Policing And Crime: MOPAC）[164]が意味のあるコンサルテーションを完了するまで、この技術の利用を一時停止することを検討すること」を要請した。一番の懸念は、市民は顔認識技術が試行されていることを知らない、すなわち市民の同意が得られていない点にあるとされた。そこで、2014年に市長により設置された独立組織である「ロンドン警察活動倫理パネル」（London Policing Ethics Panel: LPEP）[165]が、法執行における顔認識技術の利用を含むデジタル警察活動の社会への影響をレビューすることになった。

ビッグブラザーウォッチは、2018年5月、情報公開請求で入手したロンドン警視庁とサウスウェールズ警察（後述）の顔認識技術の利用記録を分析した報告書を公表した[166]。同報告書は、ロンドン警視庁の2016年から2017年の3回の試行で、自動顔認識システムが発した104件の警告のうち、警戒リストと正しく照合できていたものはわずか2件であり、98%が偽陽性（false-positive）であるとした[167]。また、適合できたもののうち1件は警戒リストに誤登録されていたもので、もう1件はメンタルヘルス上の理由で登録されていた人物であった。いずれも指名手配犯ではなく、自動顔認識システムを用いた逮捕はなかった。一方、ロンドン警視庁は、新聞の取材に対し、自動顔認識システムが警告を発した後、警察官が再確認する手順であるため、これらの102件全てが必ずしも「偽陽性」だとは考えていないとした上で、システムが警告を発しなかった写真は即座に削除し、「偽陽性」だった写真も30日以内に削除していると説明している[168]。

159　*op.cit.*157　なお、自動顔認識の評価のため、様々な公共空間で計10回の試行を実施する予定とされている。

160　GLAは、32のロンドン特別区とシティ・オブ・ロンドンの33の（基礎）自治体を含んだ2層目の（広域）自治体である。GLAの位置付け、構成等については、次が詳しい。自治体国際化協会「英国の地方自治（概要版）2017年改訂版」2018.5, pp.9-18. <http://www.jlgc.org.uk/jp/wp-content/uploads/2015/12/2017_LON.pdf>

161　"GLA Oversight Committee." Greater London Authority website <https://www.london.gov.uk/about-us/london-assembly/london-assembly-committees/gla-oversight-committee>

162　Chair of the GLA Oversight Committee, A Letter to the Mayor of London, 2017.11.14. <https://www.london.gov.uk/sites/default/files/personal_data_in_the_gla_group_-_letter_from_chair_to_mayor.pdf>

163　Chair of the GLA Oversight Committee, A Letter to the Mayor of London, 2018.2.7. <https://www.london.gov.uk/sites/default/files/letter_to_mayor-use_of_personal_data_in_the_gla_group_-_feb_7_2018.pdf>

164　MOPACは、「2011年警察改革及び社会責任法」（Police Reform and Social Responsibility Act 2011 (2011 c.13)）に基づき、2012年に設置された機関であり、ロンドン市長がそのトップを務める（第3条）。ロンドン警視庁の戦略、年次予算を策定するほか、幹部職員を任命し、監督する権限を有する。河島太朗「【イギリス】2011年警察改革及び社会責任法の制定」『外国の立法』No.249-2, 2011.11, pp.8-9. <http://dl.ndl.go.jp/view/download/digidepo_3382127_po_02490204.pdf?contentNo=1>

165　ボリス・ジョンソン（Boris Johnson）前市長により2014年に設置された。同市長在任中の2014年から2016年まで（第1期）は、車両検問、ボディカメラ、職務質問について検討を行い、報告書をまとめた。2017年から現在まで（第2期）は、医療倫理の専門家であるスザンヌ・シェール氏（Suzanne Shale）が議長を務め、そのほか3名のメンバーで構成されている。"Membership - Appointed 2017." London Policing Ethics Panel website <http://www.policingethicspanel.london/the-panel.html>

166　Big Brother Watch, *Face Off: The lawless growth of facial recognition in UK policing*, 2018.5. <https://bigbrotherwatch.org.uk/wp-content/uploads/2018/05/Face-Off-final-digital-1.pdf>

167　*ibid*., pp.3, 25.

168　Jon Sharman, "Metropolitan Police's facial recognition technology 98% inaccurate, figures show," *Independent*, 2018.5.13. <https://www.independent.co.uk/news/uk/home-news/met-police-facial-recognition-success-south-wales-trial-home-office-false-positive-a8345036.html>

LPEPは、自動顔認識の利用に伴う倫理的問題について、2017年12月以降、7回の会合を開催し、2018年7月に中間報告書をとりまとめた[169]。中間報告書は、公共空間を対象にリアルタイムで利用される顔認識技術を指す「ライブ映像の顔認識」（Live Facial Recognition: LFR）という表現を用いている[170]。そして、「ロンドン警視庁によるLFRの現在の試行は、試行が健全な状態で継続されるにあたって、対処される必要のある倫理的問題を引き起こしているか」に焦点を当てている。中間報告書は、鍵は「信頼」（trust）にあるとした上で、LFRに対する懸念が、自由に対するLFRの潜在的な脅威と、現行のLFRの不完全さに起因するバイアスによるものであるとし、5つのLFRの課題を挙げている（表5）。

表5　ロンドン警察活動倫理パネル（LPEP）中間報告が指摘したライブ映像の顔認識（LFR）の課題

課題1：技術試行に市民を巻き込むこと	
	一連の試行が、フィールド研究であるのか、警察の活動であるのかが曖昧である。前者ならば通常の研究倫理（参加者への同意、同意を必要としない場合はその正当性等）が、後者ならば警察活動に要求される原則（アカウンタビリティ、合法性、必要性、比例性など）が必要となる。イベントスペースで試行が実行される場合は、前者の場合は参加を拒否するものにはカメラを避けて入退場する自由が与えられるべきであり、後者の場合は全員スキャンされるべきである。
課題2：不正確な識別という問題	
	正確性について、試行には2つの目的があるとする。1つは人混みの中でどれだけ正確に顔認識できるかという技術的な正確性の問題で、もう1つは警察活動において人間によって実施される際に顔認識システムがどれだけうまく機能するかという問題である。顔認識システムが警戒リストと一致したと判定しても、実際に介入に進むに値する信頼性があるかどうかを判断するのは警察官である。最初の3回の試行で104件の一致が発生し、そのうち8件を警察官はもっともらしいと評価した。そのうち6件は人違いであったことが判明し、2件において正しく特定していた。人違いであった6件は、警察官に呼び止められ、IDを要求されただけで、それ以上の介入はなかった。
課題3：警戒リストの構成とデータ保護	
	勾留写真データベースの利用の合法性については裁判にもなっていて議論のあるところであり、ほとんどの写真はこのデータベースに由来し、一部は他の情報源からも来ている。警察の試行については、プライバシー影響評価が事前に実施されており、試行において得られる個人データの利用についての原則を定めている。録画は30日間保持されて消去される。録画された映像から静止画である写真が引き出されることはないとされる。
課題4：公然の監視と内密の監視	
	現在のLFRはこれまでのところは公然の監視であるが、2000年調査権限規制法（Regulation of Investigatory Powers Act 2000）を通して実施される活動のように、LFRが内密の監視として利用される可能性がある。その際は、現在実施されている他の内密の活動と同レベルの厳格な審査が必要になる。
課題5：限定された試行が無制限の適用になる可能性	
	現在の試行が社会にとって受入可能だとしても、「滑りやすい坂」（slippery slope）の危険性が指摘されている。理由としては2点挙げられていて、1つ目が、LFRのガバナンスに関するもので、LFRは生体認証、監視カメラ、情報の3コミッショナーのどれにも厳密には当てはまらない対象であり、2つ目が、技術の性能が更に進んだ場合にどう対応するかである。

（出典）London Policing Ethics Panel, *Interim Report on Live Facial Recognition*, 2018.7, pp.8-15. <http://www.policingethicspanel.london/uploads/4/4/0/7/44076193/lpep_report_-_live_facial_recognition.pdf> を基に筆者作成。

[169] London Policing Ethics Panel, *Interim Report on Live Facial Recognition*, 2018.7. <http://www.policingethicspanel.london/uploads/4/4/0/7/44076193/lpep_report_-_live_facial_recognition.pdf>

[170] *ibid.*, p.4. これは、AFRが、公共空間でリアルタイムに行われる自動化された身元確認（identity checks）を必ずしも含まない関連技術も含む広い概念とされることによる。

以上の課題を指摘した上で、LPEP は、「倫理的ガバナンスを促進し、市民の参画を増し、人々の信頼を維持するため」、次の 13 点を勧告した（表 6）。

表６　ロンドン警察活動倫理パネル（LPEP）中間報告における勧告の概要

情報のコミュニケーションに関する勧告	
	1.　試行の内容はウェブページで誰でも容易に確認できるようにすべき。
試行についての法規制枠組みに関する勧告	
	2.　試行をこれ以上進める前に、ロンドン警視庁は当該技術利用の法的根拠に関する見解を公表すべき。
	3.　ライブ映像の顔認識（LFR）の適切な監督（oversight）のために必要な基本原則を明らかにするため、関連するコミッショナーとの対話を継続すべき。
	4.　内務省の生体認証及び法科学倫理グループ（BFEG）の LFR に関する作業部会の見解が公表された際、それを考慮すべき。
試行が有する科学的及び社会的価値に関する勧告	
	5.　残りの試行の実施のために監督グループを設置し、学術研究者も参加させるべき。
	6.　ロンドン警視庁内に設置された LFR の将来の展開に関心を持つガバナンスグループを LPEP も支援する。
	7.　ロンドン警視庁は市民に対して、試行が何を解決しようとしているのか、そしてなぜ人々の参加が必要なのかを伝えるべき。
	8.　混乱を防ぐために（偽陽性などの）全ての用語の定義を明確にすべき。
	9.　試行の場所は、特定のコミュニティに対するバイアスだと思われないように、また、新しい知見ができるだけ多く得られるように選定すべき。
	10.　不必要な重複を避けるために他の警察と試行の設計や事後評価を共有すべき。
試行への市民参加が期待することに関する勧告	
	11.　スキャンされることを拒否すること自体が容疑の根拠とみなされることはないことを明記すべき。
	12.　データ保護の原則がどのように適用されているか知ってもらうために、LFR 試行について作成されたプライバシー影響文書を公表すべき。
LFR を展開するという将来の決定に関する勧告	
	13.　ロンドン警視庁は、試行を継続するための条件として、市民参加の方法も含めて、将来の意思決定をどのように行うかを提示すべき。

（出典）London Policing Ethics Panel, *Interim Report on Live Facial Recognition,* 2018.7, pp.16-19. <http://www.policingethicspanel.london/uploads/4/4/0/7/44076193/lpep_report_-_live_facial_recognition.pdf> を基に筆者作成。

最終報告書では、① LFR に利用する顔写真の情報源や利用方法（特に民間における LFR 利用と連携する場合）、②結社の自由や抗議活動に対する萎縮効果、③公共の秩序を維持するための警察活動以外の分野における LFR 技術の将来の利用を取り上げるとしている[171]。

ロンドン警視庁のウェブサイトでは、顔認識技術の利用に関する市民の懸念を聞き取り、議論するパブリックコンサルテーションを予定していることや、重要なステークホルダーが参加する「助言コンサルテーショングループ」（Advisory Consultation Group: ACG）を立ち上げたことが説明されている[172]。2018 年 7 月には、LFR の利用について、2018 年データ保護法で義務付

[171]　*ibid.,* p.19.　なお、LPEP は、アンケート調査等も実施した上で、2018 年内に最終報告書をとりまとめる予定であったが（*ibid.,* p.4.）、2019 年 1 月 25 日現在、公表に至っていない。

[172]　*op.cit.*[157]

けられたDPIAを公表した[173]。そこでは、LRFのリスクとして、例えば、LFR装置の不正確な機能、偽陽性時の不当な介入、間違った人の呼び止め、誤認逮捕、写真の保持期間の不遵守等のほか、「人々の間で誤った情報が拡散してLFRに関する信頼が失われること」を挙げ、その対策として、ステークホルダー参加戦略、メディア戦略、リスクマネジメント戦略の策定を示している。また、ロンドン警視庁によるLFRの試行にあたって、2018年データ保護法のほか、2012年自由保護法や1998年人権法[174]との関係を概説した文書も公表している[175]。

3　サウスウェールズ警察

サウスウェールズ警察[176]はAFRの利用において英国で最も先を進んでおり、スポーツイベント、ショッピングセンター、コンサートなどで広範囲に試行している。サウスウェールズ警察によるAFRの利用形態は、「識別」（Identify）と「検索」（Locate）の2種類がある。前者は監視カメラから静止画像で得られた顔写真を、およそ50万件の勾留写真と比較するもの、後者はライブ映像と照合するものである。最初の試行は2017年6月にカーディフで開催されたUEFA（Union of European Football Associations. 欧州サッカー連盟）チャンピオンズリーグ決勝（レアル・マドリード対ユベントス）で、およそ17万人の観客に対して、AFRの検索が利用された。その際に、指名手配犯であった34歳の男性の逮捕につながった[177]。サウスウェールズ警察は、AFRの利用についてPIAを実施しており、2018年2月12日付けで、4.0版の草稿が公表されている[178]。

2018年5月4日、サウスウェールズ警察は、9か月間でAFR識別によって2,000を超える正しい一致があり、450人以上を逮捕したことを公表した[179]。同時に、「偽陽性」の警告であるにもかかわらず介入があり逮捕に至った例（誤認逮捕）はなく、市民からの苦情も来ていないとした。また、大きなイベントに適用されるAFR検索の「成績」も公表された（表1）。最初のケースであるUEFAチャンピオンズリーグ決勝では、2,470件の一致（警告）のうち2,297件（92%）が誤検出（偽陽性）、すなわち正しい警告が173件（8%）であったことが明らかにされた[180]。

照合の結果、一致したとする警告があると、オペレーターはまず、無視するか、介入チームを派遣するかを「直感」で決める。派遣された場合は警察官が当人と会話し、伝統的な警察活動手法（通称は対話）により、正誤を見極める。もし誤った一致であったなら、警察官は当

173　*Metropolitan Police Service Privacy Impact Assessment*, 2018.7.25. Metropolitan Police website <https://www.met.police.uk/SysSiteAssets/media/downloads/met/advice/lfr/metropolitan-police-service-privacy-impact-assessment-lfr.pdf>

174　Human Rights Act 1998 (1998 c.42) legislation.gov.uk website <https://www.legislation.gov.uk/ukpga/1998/42>

175　*Live Facial Recognition, (LFR) MPS Legal Mandate*, 2018.7.23. Metropolitan Police website <https://www.met.police.uk/SysSiteAssets/media/downloads/met/advice/lfr/live-facial-recognition-lfr-mps-legal-mandate.pdf>

176　サウスウェールズ警察は、ウェールズの首都カーディフを含む地域を管轄する。

177　なお、これとは別に、サウスウェールズ警察において、2017年5月末、自動顔認識を用いた逮捕者が出ている。これは、自動顔認識を用いた英国初の逮捕例とされている。“Police make first arrest using facial recognition technology,” 2017.6.8. itv news website <http://www.itv.com/news/wales/2017-06-08/police-make-first-arrest-using-facial-recognition-technology/>

178　*DRAFT South Wales Police Privacy Impact Assessment*, Version 4.0, 2018.2.12. South Wales Police website <https://swplive.blob.core.windows.net/wordpress-uploads/2018/04/PIA-draft-V4-002.pdf>　なお、1998年データ保護法に基づくものとなっている。

179　“Welsh police wrongly identify thousands as potential criminals,” *Guardian*, 2018.5.5. <https://www.theguardian.com/uk-news/2018/may/05/welsh-police-wrongly-identify-thousands-as-potential-criminals>

180　“Facial recognition helps South Wales Police become smarter, creating a safer and connected community.” South Wales Police website <http://afr.south-wales.police.uk/>

人に対して経緯を説明し、「公正な処理の通知」（Fair Processing Notice）を提示しながら、装置を見せる。UEFA チャンピオンズリーグ決勝で高い偽陽性率が出てしまった原因としては、①UEFA やインターポールなどから提供された監視リストの顔写真の品質が低かったこと、②当時のアルゴリズムは正確性が低かったこと、③初めての大規模な利用であったことが挙げられている。また、プライバシーへの懸念についてもよく認識しており、情報コミッショナーや内務省の生体認証プログラム、監視カメラ・コミッショナー、生体認証コミッショナー等の関係機関と協議しているとされている。

表7　イベントごとの正しい照合と誤った照合

イベント	日付	正	誤
UEFA チャンピオンズリーグ（サッカー）	2017/6/3	173	2,297
エルビス・フェスティバル	2017/9/23	11	7
Operation Fulcrum（集中捜査）	2017/10/18	9	11
アンソニー・ジョシュアのボクシングの試合	2017/10/28	5	46
ウェールズ対オーストラリア（ラグビー）	2017/11/11	5	33
ウェールズ対ジョージア（ラグビー）	2017/11/18	3	3
ウェールズ対ニュージーランド（ラグビー）	2017/11/25	3	9
ウェールズ対南アフリカ（ラグビー）	2017/12/2	5	18
カサビアン（コンサート）	2017/12/4	4	2
リアム・ギャラガー（コンサート）	2017/12/12	6	0
Operation Fulcrum（集中捜査）	2017/12/22	8	2
Operation Malecite（集中捜査）	2017/12/23	3	0
ハリー王子の訪問	2018/1/18	0	0
ウェールズ対スコットランド（サッカー）	2018/2/3	6	7
ステレオフォニックス（コンサート）	2018/3/7	0	5
ウェールズ対イタリア（ラグビー）	2018/3/11	0	23
ウェールズ対フランス（ラグビー）	2018/3/17	2	11
DPTRE（防衛産業の国際展示会）	2018/3/27	1	0
BBC の音楽フェスティバル	2018/5/27	2	10
ボルボのヨットレース	2018/5/28	0	4
ビヨンセとジェイ Z（コンサート）	2018/6/6	0	1
ローリング・ストーンズ（コンサート）	2018/6/15	1	7
エド・シーラン（コンサート）	2018/6/21	8	10

（出典）“Facial recognition helps South Wales Police become smarter, creating a safer and connected community.” South Wales Police website <http://afr.south-wales.police.uk/>; Big Brother Watch, *Face Off: The lawless growth of facial recognition in UK policing*, 2018.5, pp.28-29. <https://bigbrotherwatch.org.uk/wp-content/uploads/2018/05/Face-Off-final-digital-1.pdf> 等を基に筆者作成。

4　スコットランド

スコットランドでは、顔認識技術に関するルールがほとんど何もない状態から、急ピッチでガバナンスの体制を整えつつあることが特徴である。

スコットランドには、法執行機関による指紋や DNA 型といった生体情報の保持を規制する法律[181]はあったが、顔写真の保持や利用を監督する法律は存在しなかった。また、生体認証

[181]　「スコットランド刑事手続法」（Criminal Procedure (Scotland) Act 1995 (1995 c. 46)）legislation.gov.uk website <https://www.legislation.gov.uk/ukpga/1995/46>

技術の警察活動での利用に関する独立した組織による監督の仕組みもなかった。これは、2012年自由保護法が成立し、独立した生体認証コミッショナーが置かれ、監視カメラ行動規範を策定しているイングランドやウェールズとは対照的であるとみなされた。スコットランド警察による顔写真データベースと顔認識技術の採用に対する規制や監督の欠如については、情報公開請求によりスコットランド警察の実態を明らかにした自由民主党の議員から、2015年に指摘されていた[182]。

2016年1月、「スコットランド警察監察局」（Her Majesty's Inspectorate of Constabulary in Scotland: HMICS）が報告書「スコットランド警察による全国警察データベースの顔検索機能の利用についての監査及び保証審査」を公表した[183]。顔認識（facial recognition）ではなく、顔検索（facial search）を用いているのは、データベースが必ずしもデジタル化されたものばかりではないからである。HMICSは、報告書の中で、スコットランド政府に4つの勧告を行った（表8）。

表８　スコットランド警察監察局（HMICS）の勧告

1	警察による顔写真の保持と利用に関連した立法を検討すべき。
2	倫理的問題の検討や監督を担う独立したコミッショナーの設置を検討すべき。
3	スコットランド警察は、検索要求理由を適切に記録できるようにするため、内部の全国警察データベース（PND）検索要求フォームを改正すべき。
4	法的拘束力のある行動規範（Code of Practice）を策定する可能性を協議すべき。

（出典）Her Majesty's Inspectorate of Constabulary in Scotland, *Audit and Assurance Review of the use of the Facial Search functionality within the UK Police National Database (PND) by Police Scotland*, 2016.1, p.9. <https://www.hmics.scot/sites/default/files/publications/HMICS%20Audit%20and%20Assurance%20Review%20of%20the%20use%20of%20the%20Facial%20Search%20functionality%20within%20the%20UK%20Police%20National%20Database%20%28PND%29%20by%20Police%20Scotland_0.pdf> を基に筆者作成。

HMICSの勧告事項、すなわち、警察活動における生体認証データの取得、利用、保持の在り方を検討するため、2017年6月、スコットランド政府は、「スコットランドにおける生体認証データの利用に関する独立助言グループ」（Independent Advisory Group on the Use of Biometric Data in Scotland: IAG）を設置した[184]。IAGは、2017年6月から2018年1月まで8回の会合を開き、生体認証に関心のある広範囲の組織や個人（プライバシーや人権擁護団体、研究機関などを含む）への聞き取りを行った。その中で、子どもや若者の生体認証データの保持や利用に関して検討するサブグループも設置された。そして、IAGは、2018年3月に公表した報告書[185]の中で、スコットランド政府に9つの勧告を行った（表9）。

182　Magnus Gardham, "Controversial face recognition software is being used by Police Scotland, the force confirms," *Herald*, 2015.5.26. <https://www.heraldscotland.com/news/13215304.controversial-face-recognition-software-is-being-used-by-police-scotland-the-force-confirms/>

183　Her Majesty's Inspectorate of Constabulary in Scotland, *op.cit.*(140)

184　"Use of Biometric Data and Technologies," Scottish Government website <http://www.gov.scot/About/Review/biometric-data>

185　"Independent Advisory Group on the Use of Biometric Data in Scotland," 2018.3. Scottish Government website <https://www.gov.scot/binaries/content/documents/govscot/publications/report/2018/03/report-independent-advisory-group-use-biometric-data-scotland/documents/00533063-pdf/00533063-pdf/govscot%3Adocument>

表9　スコットランドにおける生体認証データの利用に関する独立助言グループ（IAG）の勧告

1	人々の理解と信頼を改善するために、国民的な議論が必要である。
2	生体情報の取得・保持・利用・廃棄をカバーする行動規範が必要である。
3	行動規範は詳細なコンサルテーションの対象とすべきである。
4	12 ～ 17 歳の子どもについては別に方針を定める必要がある。
5	スコットランド刑事訴訟法（Criminal Procedure (Scotland) Act 1995）の生体情報の保持ルールを見直すべき。
6	保持期間が過ぎた生体情報は削除されるべき。
7	適切な保持期間についてはパブリックコンサルテーションすべき。
8	独立のスコットランド生体認証コミッショナーを設置すべき。
9	倫理助言グループを設置すべき。

（出典）“Use of Biometric Data: Report of the Independent Advisory Group,” 2018.3.22. Scottish Government website <https://www.gov.scot/publications/report-independent-advisory-group-use-biometric-data-scotland/> を基に筆者作成。

報告書の公表に合わせて、スコットランド政府は、勧告に対する回答を公表し[186]、9 つの勧告を全て受け入れた。ただし、行政機関の肥大化の防止の観点から、スコットランド議会との調整が必要とされたため、生体認証コミッショナーの設置（勧告 8）については、「原則として受諾」とされた。

スコットランド政府は、IAG の勧告のうち、法的拘束力のある行動規範と生体認証コミッショナーの設置について、HMICS の支援の下、政府案を作成してパブリックコンサルテーションを実施した[187]。法的拘束力のある行動規範については、どんな生体認証データ及び技術を、また誰を対象とすべきか意見が求められた。生体認証コミッショナーの設置については、必要か否か、そして必要な場合はその役割、任命方法、責任範囲などの意見が求められた。パブリックコンサルテーションは 2018 年 7 月 13 日から 10 月 1 日まで実施され、その間に 4 度、ステークホルダーを集めたイベントも開催された。寄せられた意見は合計 89 件であった。行動規範の策定には 83% が、生体認証コミッショナーの設置には 89% が賛同した。

2018 年 9 月に発表されたスコットランド政府の年度計画 2018-19 年では、2019 年の提出予定法案の 1 つに、「生体認証データ法案」（Biometric Data Bill）が挙げられている[188]。同法案では、IAG の勧告とパブリックコンサルテーションの結果を踏まえ、①刑事司法制度における指紋、DNA、顔写真を含む生体認証データの取得、保持、廃棄に関わる法的拘束力のある行動規範を定めること、また、②行動規範を監視し、ベストプラクティスを促進するとともに、スコットランド市民に新しい技術を周知する任務を負う、生体認証技術に関する議会コミッショナーを設置することを盛り込むとされている。

---

[186] Scottish Government, “Scottish Government’s Response to the Report by the Independent Advisory Group on the Use of Biometric Data,” 2018.3. <https://www2.gov.scot/Resource/0053/00533027.pdf>

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

[188] Scottish Government, *Delivering for today, investing for tomorrow: the Government's programme for Scotland 2018-2019,* 2018.9.4. <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>

Ⅲ　オーストラリア

オーストラリアでは近年、国全体で、パスポートや運転免許証まで含めて各種生体情報を共有する方向で制度改正が進みつつあり、他方で、地方自治体や市民団体からはプライバシーへの懸念が表明されている。

１　法執行のための生体認証

オーストラリア連邦犯罪情報委員会（Australian Criminal Intelligence Commission: ACIC）[189]が、国家犯罪捜査DNAデータベース（National Criminal Investigation DNA Database: NCIDD）と国家自動指紋識別システム（National Automated Fingerprint Identification System: NAFIS）という２つの生体認証サービスを提供している。

国全体のDNAデータベースであるNCIDDは、国内の全ての警察組織が24時間365日使える形で2001年に稼働を開始した[190]。当初は、クリムトラック（CrimTrac）所管であり、2016年に後継組織であるACICの管轄となった。120万件以上のDNA型が収録されている[191]。これらは犯行現場、有罪判決を受けた人、容疑者、任意捜査の対象者、行方不明者の持ち物や身元不明死者から得られたものである。犯罪現場から採取されたDNAサンプルはデータベースと照合される。2018年９月には、血縁関係の照合（kinship matching）や家族検索（familial searching）といった機能が追加された[192]。これらはレイプや殺人といった重い犯罪に適用され、他に手段がない際に利用されるとされている。

指紋と掌紋のデータベースであるNAFISは、国内の全ての警察組織が24時間365日使える形で2001年に稼働を開始し、犯罪捜査だけでなく、移民プログラムを支援するために内務省（Department of Home Affairs）にも利用されている[193]。警察は、逮捕時や犯罪現場からほとんどリアルタイムで指紋データをアップロードしたり検索したりすることができる。クリムトラックは、NAFISを、連邦、地域、州の警察データベースに保持されている670万の指紋に1200万の顔写真を加えた統合生体認証データベースである「生体認証識別サービス」（Biometric Identification Service: BIS）に更新することを決定し、2017年から運用可能になる予定であった。しかし、プロジェクトの進行が遅れ、費用もかさんだことから、ACICは2018年６月、BISプロジェクトの中止を発表した[194]。

オーストラリアでの顔認識技術の利用は、地方政府から始まった[195]。例えば、ニュー・サ

189　オーストラリア犯罪委員会（Australian Crime Commission）と、国内の法執行機関の間での生体情報を含む情報共有サービスを担当していたクリムトラック（CrimTrac）が合併して2016年７月に発足した。

190　オーストラリアの法執行機関によるDNAの利用については、次を参照した。Marcus Smith and Monique Mann, “Recent developments in DNA Evidence,” *Trends & issues in crime and criminal justice*, No.506, 2015.11. <https://aic.gov.au/publications/tandi/tandi506>

191　“National Criminal Investigation DNA Database.” Australian Criminal Intelligence Commission website <https://www.acic.gov.au/our-services/biometric-and-forensic-services/national-criminal-investigation-dna-database>

192　“Law enforcement to match DNA profiles across borders,” 2018.9.29. Minister for Home Affairs (The Hon Peter Dutton MP) website <https://minister.homeaffairs.gov.au/peterdutton/Pages/dna-profiles-across-borders.aspx>

193　“National Automated Fingerprint Identification System.” Australian Criminal Intelligence Commission website <https://www.acic.gov.au/our-services/biometric-matching/national-automated-fingerprint-identification-system>

194　“Biometric Identification Services project to close,” 2018.6.15. *idem* <https://www.acic.gov.au/media-centre/media-releases-and-statements/biometric-identification-services-project-close>

195　本段落の記述は、次の資料による。Monique Mann and Marcus Smith, “Automated Facial Recognition Technology: recent developments and approaches to oversight,” *University of New South Wales Law Journal*, Vol.40 No.1, 2017, pp.125-126. <http://www.unswlawjournal.unsw.edu.au/wp-content/uploads/2017/09/40-1-11.pdf>

ウス・ウェールズ（New South Wales: NSW）州政府は2009年、道路交通（運転免許）規則を改正し、ID不正を防止することを目的として、個人が運転免許証などの許可証の発行や更新を求める際にID確認のために自動顔認証技術が利用できるようにした。その後、NSW州政府も含む各州政府等は法改正を行い、運転免許証の顔写真データベースを連邦機関と共有できるようにした。

２　顔マッチングサービスの試み

オーストラリア全体では、2015年9月、連邦政府と州政府が顔写真データベースを共有して自動顔認識技術が使える「国家顔生体認証マッチング能力」（National Facial Biometric Matching Capability: NFBMC）と呼ばれるシステムが2016年半ばに連邦政府により運用可能となることが発表された[196]。具体的には、一対一で比較し同一性を判定する「顔確認サービス」（Face Verification Service:FVS）が2016年11月に運用可能となり、一対多の検索により人物を特定する「顔識別サービス」（Face Identification Service: FIS）が、州や特別地域との交渉次第であるが、2017年中に運用可能となるとの見通しが示された。この時点では、CCTVを始めとする他の監視システムとの連携はとられていない[197]。2016年11月16日に、FVSの第1フェーズが開始されたことが報じられた[198]。連邦レベルでは、外務貿易省（DFAT）と連邦警察（AFP）が、当時の移民国境警備省（DIBP）（2017年の行政機構再編により、現在は内務省。）が保持する入国時の顔写真記録と照合することが可能となった。次のフェーズでは、パスポート写真、ビザの写真、運転免許証などが追加される予定である。そのためには、運転免許証を所管する州や特別地域政府との合意が必要であった。他方、顔識別サービス（FIS）の準備は後述するように遅れた。

連邦政府と州・特別地域政府間の問題を協議する場である政府間協議会（Council of Australian Governments: COAG）[199]は、2017年10月5日に首都キャンベラで開催されたテロ対策のCOAG特別会合[200]で、NFBMCの確立に合意し、「ID照合サービスに関する政府間合意」（Intergovernmental Agreement on Identity Matching Services）に署名した[201]。ID照合サービスは、文書確認サービス（Document Verification Service）、顔照合サービス（Face Matching Service）、IDデータ共有サービス（Identity Data Sharing Service）から成る。このうち、顔照合サービスは、顔確認サー

196　Adam Moinar, “Your face is part of Australia’s ‘national security weapon’: should you be concerned?” 2015.9.14. The Conversation website <https://theconversation.com/your-face-is-part-of-australias-national-security-weapon-should-you-be-concerned-47364> 司法省（Attorney-General’s Department: AGD）は、NFBMCの枠組みについて詳細が決まっていない段階で、PIAをコンサルティング会社に委託した。2015年8月に公表された報告書では、オーストラリアの1988年プライバシー法や、そこに含まれている13項目からなる「オーストラリア・プライバシー原則」（APP）と整合的であると考えられ、重大なリスクやプライバシー問題は発見されなかったと記述された。Information Integrity Solutions Pty Ltd., *National Facial Biometric Matching Capability: Privacy Impact Assessment – Interoperability Hub*, 2015.8. Australian Gobernment Department of Home Affairs website <https://www.homeaffairs.gov.au/criminal-justice/files/privacy-impact-assessment-national-facial-biometric-matching-capability.PDF>

197　Mann and Smith, *op.cit.*[195], p.127.

198　Alie Coyne, “Australia's new facial verification system goes live,” 2016.11.16. itnews website <https://www.itnews.com.au/news/australias-new-facial-verification-system-goes-live-441484>

199　COAGの参加機関は、連邦政府に加えて、6つの州と2つの特別地域である。

200　“Special Meeting of the Council of Australian Governments on Counter-Terrorism Communiqué,” 2017.10.5. Council of Australian Governments website <https://www.coag.gov.au/meeting-outcomes/special-meeting-council-australian-governments-counter-terrorism-communique>

201　*Intergovernmental Agreement on Identity Matching Services*, 2017.10.5. *idem* <https://www.coag.gov.au/sites/default/files/agreements/iga-identity-matching-services.pdf>　なお、署名日同日に発効した。

ビス、顔識別サービス、顔認識解析供給サービス、1個人1ライセンスサービスの4つからなる。これにより、法執行機関がパスポート、ビザ、市民権、運転免許証の顔写真を同時に利用することが可能になった。CCTVの映像には適用されないが、空港のカメラには適用される。運転免許証が加わることで国民の80％をカバーできる[202]。逆に、犯罪者やテロリストは運転免許証やパスポートを持たないことで事実上「オプトアウト」できてしまうという指摘もある[203]。

2018年2月7日、ピーター・ダットン（Peter Dutton）内務大臣が、COAG合意に基づいて、「2018年ID照合法案」[204]を連邦議会に提出した。同法律案では、ID照合サービスを運用するために、5種類のID照合サービスを対象に、ID情報を収集、利用、公表する権限を内務省に与えるとともに、各ID照合サービスの定義規定を設け、内務省に、新しいサービスの利用に関する年次報告書を発表することを義務付けることも盛り込んでいる。また、「2018年パスポート改正法案（ID照合サービス）」[205]も提出された。同法律案は、ID照合サービスに利用する目的で、渡航文書の個人情報を提供する権限を外務大臣に与えることを盛り込んでいる。

連邦議会のインテリジェンス及びセキュリティに関する両院合同委員会（Parliamentary Joint Committee on Intelligence and Security）が両法案の審査を開始し、5月にメルボルンで、8月にキャンベラで公聴会が開催された[206]。1つの論点は、ID照合サービスの利用時に、令状（warrant）を必要とするか否かである。内務省は4月に様々な懸念に回答する文書を公表し[207]、その中で、政府間合意においても事前の令状の要求は含まれておらず、内務省としても、そのような要求は法執行その他の機関のサービス利用に大きな影響を与えるため、支持しないと主張している。5月の公聴会では、オーストラリア人権委員会（Australian Human Rights Commission）とオーストラリア弁護士連合会（Law Council of Australia）、そして内務省が意見陳述した。オーストラリア人権委員会は、事前に令状を必要とすることを含む9か所の法案修正を勧告し、オーストラリア弁護士連合会は、もともと合意された目的を超えて軽微な犯罪にも用いられる懸念を表明して、生体情報の監視を専門とする規制機関を新設することを提案した[208]。

州レベルでも、例えば、2018年3月、ビクトリア州の情報コミッショナー局（Office of the Victorian Information Commissioner: OVIC）が、両院合同委員会に意見書を提出し、2つの法律案について原則として支持するとしつつも、ガバナンスとプライバシーに対する懸念を伝えている[209]。その後、ビクトリア州政府が両院合同委員会に提出した意見書では、ガバナンス体制の整備が

[202] Rebecca Trigger, “Experts sound alarm as biometric data from drivers’ licences added to government database,” *Newdaily*, 2018.1.15. <https://thenewdaily.com.au/news/national/2018/01/15/biometric-data-drivers-licences-government-database/>

[203] なお、ガーディアン紙は、2017年11月25日、情報公開請求で入手した文書から、将来的にFVSを手数料を取って民間企業の利用を可能とする方向で、司法省が大手通信会社と議論していることが明らかになったと報道した。Elise Thomas, “Coalition could allow firms to buy access to facial recognition data,” *Guardian*, 2017.11.26. <https://www.theguardian.com/technology/2017/nov/26/government-could-allow-firms-to-buy-access-to-facial-recognition-data>

[204] Identity-matching Services Bill 2018. Parliament of Australia website <https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6031>

[205] Australian Passports Amendment (Identity-matching Services) Bill 2018. *idem* <https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6030>

[206] “Public Hearings.” *idem* <https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/IMSBill/Public_Hearings>

[207] Submissions received by the Committee, *idem* <https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/IMSBill/Submissions> リストの中の12番がこれにあたる。

[208] Paul Karp, “Dutton's home affairs department argues against restrictions on facial recognition,” *Guardian*, 2018.5.3. <https://www.theguardian.com/world/2018/may/03/duttons-home-affairs-department-argues-against-restrictions-on-facial-recognition>

[209] Justin Hendry, “Privacy bodies take aim at facial recognition laws,” 2018.3.28. itnews website <https://www.itnews.com.au/news/privacy-bodies-take-aim-at-facial-recognition-laws-487841>

不十分であることに加え、民間セクターや地方自治体に拡大される際のリスク、法律案の対象が元の政府間合意（IGA）よりも拡大している点などを問題として挙げている。また、オーストラリア首都特別地域（ACT）も、提案された法案がACTのプライバシー及び人権法と矛盾してしまうとして、 ビクトリア州の提出文書に賛同した[210]。これら2つの法律案は、2018年末時点でまだ審議中である。

３　声紋認証

連邦税務局（Australian Tax Office: ATO）は、早くて簡単な個人認証手段として、声紋（voiceprints）認証を用いている[211]。2018年2月、ATOが340万人のオーストラリア人の声紋を収集済みであることが報じられた[212]。登録は任意で、一度登録すると、電話をした市民は、自分が誰であるかを証明するために、「オーストラリアでは私の声が私を特定します」（In Australia my voice identifies me）というフレーズを繰り返すことで個人認証が可能となる。登録されているデータとの一致率がスコアで表示される[213]。データは暗号化され、ファイアウォールで遮断された安全なデータベースに保管されている。登録した声紋を消去したい場合はいつでも可能である。声紋認証は2016年に導入され、その結果、手続き時間が48秒短縮されたという。ATOのプライバシーポリシーには、「将来的に政府全体の声紋データベースになるであろう声紋データベースを保持している」と明記されている[214]。

同じ技術は、福祉省（Department of Human Services）傘下で、連邦政府の社会保障給付事務等を行う「センターリンク」（Centrelink）でも利用されている[215]。利用は任意で、ATOと同様、「オーストラリアでは私の声が私を特定します」というフレーズが使われている。

４　空港による生体認証

2015年、移民国境警備省（DIBP. 現在は内務省）は「シームレスな旅客イニシアティブ」（seamless traveller initiative）を発表し、スマートゲート（SmartGates）を含む新技術を採用し、2020年までに国際線乗客の90％が、生体認証が採用された自動化ラインで手続できることを目指すと宣言した[216]。2017年3月に、クイーンズランド州のブリスベン空港は、ニュージーランド航空、SITA（国際航空通信共同体）と組んで、 オーストラリアで最初の顔認識技術を使った搭乗の試行を開始した[217]。「SITAスマートパス」技術では、最初に、生体情報（顔画像）が単一のIDトークン

⑵⑽　Finbar O'Mallon, "Federal facial recognition bill clashes with ACT law," *Canberra Times*, 2018.5.13. <https://www.canberratimes.com.au/politics/act/federal-facial-recognition-bill-clashes-with-act-law-20180510-p4zel1.html>

⑵⑾　"Voice authentication." Australian Tax Office website <https://www.ato.gov.au/General/Online-services/Voice-authentication/>

⑵⑿　George Nott, "The ATO now holds the voiceprints of one in seven Australians," 2018.2.15. Computerworld website <https://www.computerworld.com.au/article/633461/ato-now-holds-voiceprint-one-seven-australians/>

⑵⒀　声紋認証技術を提供しているのは、Nuance社であり、音声が録音されたものか、ライブで話しているのかを区別できるとのことである。

⑵⒁　"ATO Privacy Policy." Australian Taxation Office website <https://www.ato.gov.au/about-ato/commitments-and-reporting/in-detail/privacy-and-information-gathering/privacy-policy/>

⑵⒂　"Create a voiceprint," Department of Human Services website <https://www.humanservices.gov.au/individuals/enablers/create-voiceprint/29576>

⑵⒃　"Benefits for consumers, travellers and industry from red tape cuts and new technology," 2015.5.12. Minister for Home Affairs (The Hon Peter Dutton MP) website <https://minister.homeaffairs.gov.au/peterdutton/2015/Pages/benefits-for-consumers-travellers-industry.aspx>

⑵⒄　"Brisbane Airport leads with smart biometrics from check-in to boarding," 2017.3.9. SITA website <https://www.sita.aero/pressroom/news-releases/brisbane-airport-leads-with-smart-biometrics-from-check-in-to-boarding>

として登録され、チェックイン、荷物の預入れ、セキュリティチェック、国境管理、搭乗といった各段階で、乗客は、搭乗券もパスポートも見せずに、顔認識技術を用いて正しい乗客が正しい航空機に搭乗していることが確認される[218]。

シドニー空港は、搭乗券とパスポートを提示する回数をできるだけ減らすことを目指して、あらかじめ選ばれたカンタス航空の国際線の旅客に対して、顔認識技術を用いた「カウチソファからゲートまで」（couch-to-gate）生体認証システムの試行プロジェクトを2018年6月21日から12月11日まで実施した[219]。このプロジェクトは、IATA（国際航空運送協会）の“One Identity”コンセプトとも連携し、単一のトークンを使って、旅程の各段階で乗客のIDを認証する。乗客が4か所の重要なステップ（チェックイン、荷物の預入れ、ラウンジ、搭乗）を本人の顔の確認だけで通過することが試みられる。将来的には到着の場面でも利用される予定である。試行段階でおよそ2万人の顔写真を収集し、照合性能を評価した結果、他人誤受入率（FAR）は4,000人に1人（すなわち0.025%）未満であったことを明らかにした[220]。

ブリスベン空港でも、カンタス航空とSITAとともに、いくつかの国際線において、顔認識の試行を、2018年9月23日から12月11日まで実施した。カンタスの顔認証アプリをダウンロードすることにより、自宅からもパスポートを用いて登録することができ、空港の出国エリアにある顔認証キオスクからも登録できる。

また、キャンベラ空港では、2017年11月、Vision-Box社の顔認識技術を使ったスマートゲートが最初に設置された空港となった。最初は、パスポートを挿入する「コンタクト」モードのみで実施された。到着する乗客に対する試行が実施され、2,200人が参加した。これは、パスポートのチップ内の顔写真ではなく、航空会社のシステムにあらかじめ蓄えられた顔写真と照合するもので、入国の際に搭乗口でパスポートを提示する手間を省く。

Ⅳ　EU

EUでは、厳格な個人情報保護法制のため、英国や米国のように法執行機関や商業施設での生体認証技術の利用は盛んではないが、非正規の移民の流入という事態を受けて、国民ID制度と国境管理における生体認証技術の利用に関する議論が盛んであるという特徴がある。

1　個人情報保護

1995年データ保護指令[221]では、第2条(a)項において、個人データは「識別された、または識別されうる自然人に関するあらゆる情報」と定義され、さらに「識別されうる人は、特に、ID番号か、その身体的、精神的（中略）同一性に固有な1つ以上の指標を参照することで、直接的または間接的に識別されうる者をいう」とされた。データ保護指令第29条に基づいて設置された作業部会（以下「WP29」）は、2003年8月1日に、生体認証技術の利用に伴うプライ

218　“SITA Smart Path™: Delivers whole journey identity management.” *idem* <https://www.sita.aero/solutions-and-services/solutions/sita-smart-path>

219　“Facial recognition.” QANTAS website <https://www.qantas.com/au/en/travel-info/travel-advice/facial-recognition.html>

220　Justin Hendry, “Home Affairs 'face on the move' biometrics trial scores 94 percent,” 2018.7.11. itnews website <https://www.itnews.com.au/news/home-affairs-face-on-the-move-biometrics-trial-scores-94-percent-497710>

221　Directive 95/46/EC *OJ* L 281, 1995,11.23, pp. 31–50. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=EN>

バシー問題についての意見書を公表し、データ保護指令の上記条文に従えば、「生体認証の手段や、それらのテンプレート形態でのデジタル変換されたものは、ほとんどの場合、個人データである」とし、生体データ（biometric data）を個人データであると明言した[222]。WP29 から 2007 年に発表された「個人データに関する意見」では、具体的なケースを挙げながら個人データの定義について深掘りをしている中で、生体データが「技術的に計測するために使用するパターンが実際にはある程度の蓋然性を含むものだとしても、特定の個人に固有かつ計測可能である生物学的特性、身体的特徴、生体の特質や繰り返される行動」と定義された[223]。

そして、生体認証技術の発展や価格の劇的な低下、そして身元詐称（なりすまし犯罪）の脅威などを踏まえて、WP29 は 2012 年にも意見を公表している[224]。各種用語の定義に続いて、第 3 章では法的な側面が分析され、第 4 章では新しい技術トレンドについて、静脈パターン、指紋、顔認識、声紋認識、DNA、署名が取り上げられた。第 5 章では、生体認証システムが社会に実装されるにあたり、欧州市民のプライバシーや基本的人権を保護するために、プライバシー・バイ・デザイン概念の採用と PIA の実施に加え、技術的な対策リストや組織的対応の必要性が勧告されている。同じ年には、WP29 から「オンライン及びモバイルサービスにおける顔認識に関する意見」も公表されている[225]。

2018 年 5 月 25 日、欧州一般データ保護規則（GDPR）[226] が施行された。第 4 条（定義）において、「生体データ」（biometric data）が「自然人の身体的、生理的又は行動的な特性に関連する特別な技術的取扱いから得られる個人データであって、顔画像や指紋データのように、当該自然人を一意に識別できるようにするもの、又は、その識別を確認するものを意味する」とされた。さらに、第 9 条（特別な種類の個人データ）の第 1 項では、（本人の同意等、第 2 項に列挙された条件を満たさない場合は）「人種的若しくは民族的な出自、政治的な意見、宗教上若しくは思想上の信条、又は、労働組合への加入を明らかにする個人データの取扱い、並びに、遺伝子データ、自然人を一意に識別することを目的とする生体データ、健康に関するデータ、又は、自然人の性生活若しくは性的指向に関するデータの取扱いは、禁止される」とされた。また、第 4 項では「加盟国は、遺伝子データ、生体データ又は健康に関するデータの取扱いに関し、その制限を含め、付加的な条件を維持又は導入することができる」とも定められており、より厳しいルールの導入を加盟各国に認めた形になっている。プライバシー影響評価（PIA）は、GDPR では「データ保護影響評価」（DPIA）として、第 35 条に定められている。DPIA が必要なケースとして第 1 項では「取扱いの性質、範囲、過程及び目的を考慮に入れた上で、特に新

[222] ARTICLE 29 Data Protection Working Party, *Working document on biometrics*, 12168/02/EN WP80, 2003.8.1, p.5. <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp80_en.pdf>

[223] ARTICLE 29 Data Protection Working Party, *Opinion 4/2007 on the concept of personal data*, 01248/07/EN WP 136, 2007.6.20, p.8. <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf>

[224] ARTICLE 29 Data Protection Working Party, *Opinion 3/2012 on developments in biometric technologies*, 00720/12/EN WP193, 2012.4.27. <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf>

[225] ARTICLE 29 Data Protection Working Party, *Opinion 02/2012 on facial recognition in online and mobile services*, 00727/12/EN WP 192, 2012.3.22. <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp192_en.pdf>

[226] 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>

たな技術を用いるような種類の取扱いが、自然人の権利及び自由に対する高いリスクを発生させるおそれがある場合」とされ、DPIAが特に求められるケースとして挙げられている第3項(a)項「プロファイリングを含め、自動的な取扱いに基づくものであり、かつ、それに基づく判断が自然人に関して法的効果を発生させ、又は、自然人に対して同様の重大な影響を及ぼす、自然人に関する人格的側面（personal aspects）の体系的かつ広範囲な評価（evaluation）の場合」は、生体データの解析に該当すると考えられる。また、同(c)項の「公衆がアクセス可能な場所の、システムによる監視が大規模に行われる場合」は、監視カメラによる顔や歩容情報の取得に該当すると考えられる。DPIAガイドラインは、2017年、「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とともに採択された[227]。

2　IDカード

WP29は、2003年に公表した生体認証技術に関する作業文書を受けて、EU市民のパスポート等の身分証明への生体識別子や生体データの利用に関して首尾一貫したアプローチを検討する作業を開始した。2005年9月30日には、加盟国が発給するIC旅券、他の旅行関係文書、IDカードのセキュリティと生体認証技術の基準に関する意見を発表し、生体的特徴を利用する際に生じうる倫理的、法的、及び技術的問題が数多く挙げられた[228]。

欧州委員会は2018年4月17日、犯罪者やテロリストの行動を制限するための対策パッケージを発表した[229]。その中で、彼らによって利用される偽造文書を取り締まるために、EU市民のIDカードを利用している加盟国に対して、2指の指紋と顔の写真のデジタル写真を含むことを義務付ける規則案を欧州議会と欧州連合理事会に提出した[230]。ただし、12歳未満の子どもは免除される。準拠していないカードは5年で使えなくなる。2018年春時点で、オーストリアとスウェーデンなどいくつかの国では任意であるが、英国、アイルランド、デンマークを除く全ての加盟国でIDカードが発行されている[231]。現在、8000万人ほどが、機械で読み取ったり、生体情報の識別子を含んだりできないIDカードを所持していると見積もられている。EUでは、2009年以来、パスポートに生体データを含むよう義務付けているが、多くの国でこのルールの施行には時間がかかっている。欧州委員会の規制案に対して、欧州データ保護監督官（EDPS）は8月、規制案は、影響を受ける人数の多さと取扱いに慎重を期すべきデータとして特別な保護を要するという性質を考慮すると、2種類の生体データを利用する必要性を必

---

[227] 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, 2017.4.4. (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）」<https://www.ppc.go.jp/files/pdf/dpia_guideline.pdf>

[228] Article 29 Data Protection Working Party, *Opinion 3/2005 on Implementing the Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States*, 1710/05/EN-rev WP 112, 2005.9.13. <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2005/wp112_en.pdf>

[229] "Security Union: Commission presents new measures to deny terrorists and criminals the means and space to act," 2018.4.17. European Commission website <https://ec.europa.eu/home-affairs/news/security-union-commission-presents-new-measures-deny-terrorists-criminals-means-space-act_en>

[230] COM(2018) 212 final - 2018/0104 (COD) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018PC0212>; <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018PC0639&from=EN>

[231] Philip Blenkinsop and Samantha Koester, "EU Commission proposes making fingerprints mandatory in ID cards," *Reuters*, 2018.4.17. <https://www.reuters.com/article/us-eu-security/eu-commission-proposes-making-fingerprints-mandatory-in-id-cards-idUSKBN1HO23A>

ずしも正当化できていないとする意見を公表した[232]。また、適用年齢も 14 歳以上とすべきとした。欧州議会からの要請に基づき、欧州基本権機関（FRA）も 9 月、ID カードや居住許可証に生体データを含めることの基本的権利への影響に関して意見を公表した[233]。そこでは、チップに含まれた生体データは国のデータベースには保持されないようにすべきことや、2 種類の生体データが本当に必要なのか再評価する必要があることなど、6 点の意見が表明された。

３　国境管理

欧州基本権機関は、2018 年 3 月、EU 全体の IT システムにおける生体認証技術の利用に関する報告書を発表した[234]。EU が国境管理のために持つ 3 つの既存の大規模 IT システム及び 3 つの新規の大規模 IT システムとそれらの相互運用が、指紋採取の際の同意の取り方や個人の尊厳の尊重といった観点から、移民や庇護申請者、子どもの基本的権利に与える正負の影響を、欧州 6 か国での多数のインタビューやアンケートを基に調査した結果が掲載されている。

既存の 3 つの IT システムとは Eurodac（欧州指紋データベース）、VIS（査証情報システム）、SIS II（シェンゲン情報システム）で、新規の 3 つの IT システムとは、EES（出入国システム）、ETIAS（欧州旅行情報及び認証システム）、ECRIS-TCN（欧州第三国（EU 非加盟国）国民（無国籍者を含む）の犯罪記録情報システム）である。これらを表 10 にまとめた。一番右側の列が、各システムが収集している生体識別子である。グレーの網掛け部分は 2018 年春に計画提案段階のものである。これまでは指紋しか用いられていなかったが、顔写真など、多様な生体識別子の利用が計画されていることが分かる。

⑵32　European Data Protection Supervisor, *EDPS Opinion 7/2018 on the Proposal for a Regulation strengthening the security of identity cards of Union citizens and other documents*, 2018.8.10. <https://edps.europa.eu/sites/edp/files/publication/18-08-10_opinion_eid_en_0.pdf>

⑵33　European Union Agency for Fundamental Rights, *Fundamental rights implications of storing biometric data in identity documents and residence cards: Opinion of the European Union Agency for Fundamental Rights*, 2018.9.5. <https://fra.europa.eu/en/opinion/2018/biometric-id>

⑵34　European Union Agency for Fundamental Rights, *Under watchful eyes: biometrics, EU IT-systems and fundamental rights*, 2018.3. <https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-biometrics-fundamental-rights-eu_en.pdf>

表１０　既存及び新規の EU の大規模 IT システムと生体識別子の利用

ITシステム	主要目的	対象	法規制	生体識別子
Eurodac 欧州指紋データベース	国際的保護の申請者の審査責任国の決定 非正規状態の移民や2次移動の制御を支援	国際的保護の申請者や受益者 非正規状態での移民	Regulation (EU) No. 603/2013 (Eurodac Regulation) COM(2016) 272 final (Eurodac proposal)	指紋（16歳以上）、顔写真
VIS 査証情報システム	ビザ申請に関するデータ交換促進	ビザ申請者	Regulation 767/2008/EC (VIS Regulation)	指紋（12歳以上）
SIS Ⅱ警察 シェンゲン情報システム	安全の確保	行方不明者/指名手配犯	Council Decision 2007/533/JHA (SIS II Decision) COM(2016) 883 final (SIS II police proposal)	指紋、掌紋、顔写真、DNA型
SIS Ⅱ国境	入国や滞在を拒否する目的での警告	非正規状態での移民	Regulation 1987/2006 (SIS II Regulation) COM(2016) 882 final (SIS II borders proposal)	指紋、掌紋、顔写真
SIS Ⅱ帰国	帰国決定の第三国国民への警告	非正規状態での移民	COM(2016) 881 final (SIS II return proposal)	指紋、掌紋、顔写真
EES 出入国システム	第三国国民の滞在期間計算と不法滞在の発見	短期滞在者	Regulation (EU) 2017/2226 (EES Regulation)	指紋、顔写真（ともに12歳以上）
ETIAS 欧州旅行情報及び認証システム	ビザなし旅行者のリスク評価	ビザなし旅行者	COM(2016) 731 final (ETIAS proposal)	－
ECRIS-TCN 欧州第三国国民の犯罪記録情報システム	情報共有	犯罪記録のある第三国国民	COM(2017) 344 final (ECRIS-TCN proposal)	指紋、顔写真
相互運用可能性-共通IDリポジトリ	上記全ての相互運用枠組み確立	上記システムが対象とする第三国国民	COM(2017) 793 final (Borders and visa interoperability proposal) COM(2017) 794 final (Police cooperation, asylum and migration interoperability proposal)	指紋、顔写真、DNA型

（注）　グレーの網掛け部分は、2018 年 3 月時点で計画段階のものを示す。

（出典）European Union Agency for Fundamental Rights, *Under watchful eyes: biometrics, EU IT-systems and fundamental rights*, 2018.3, p.23. (Table 1) <https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-biometrics-fundamental-rights-eu_en.pdf> を基に筆者作成。

これらの中で、Eurodac に関する動向は以下のようである[235]。Eurodac は 2003 年に設置され、現在は 2013 年の規則[236]に基づき運用されているが、欧州委員会、欧州連合理事会及び欧州議会は、同規則の改正に向けた検討を進めている[237]。2016 年 5 月に欧州委員会が提出した規則の改正案では、① Eurodac の目的として、非正規に滞在している第三国の国民の特定を加えること、②取得する生体データに、顔写真を加えること、③生体データの取得を強制する年齢下限を 14 歳から 6 歳に引き下げることが盛り込まれた。

2016 年 12 月、FRA は、欧州議会からの要請を受けて、規則改正の影響に関する意見を公表した[238]。その中で、子どもについては、①生体データを取得する際に、優しく、かつ、気を配ったやり方であるだけでなく、ジェンダーにも気を配ったやり方で実施すべきとし、②自由を奪ったり、身体的及び心理的な力を行使したりするなど、強制的な生体データの取得は避けるべきとされた。また、年齢制限の引下げをめぐっては、人身取引の犠牲となった子どもの保護、行方不明や誘拐からの保護など、子どもの保護の目的に限り、正当化されるとした。

2017 年 5 月、欧州議会の「市民の自由・司法・内務委員会」（Committee on Civil Liberties, Justice and Home Affairs: LIBE）は、強制取得の年齢制限の引下げについて、子どもたちが両親と再会することが容易になること等を理由に、賛成 35、反対 10、棄権 8 で可決した[239]。これに対して、2018 年 2 月、国連難民高等弁務官事務所（UNHCR）等の国連機関とセーブ・ザ・チルドレン（Save the Children）を始めとする市民団体が、「児童の権利に関する条約」の第 3 条を踏まえ、強制取得の対象から子どもを除外するよう求める共同声明を発表した[240]。

その後、欧州議会と欧州連合理事会は、2018 年 6 月 19 日、規則の改正案をめぐって、①庇護申請者と非正規移民に対しては、指紋に加えて、パスポート写真と英数字（氏名、ID、旅券番号）を含めたより多くのデータを収集すること、②行方不明の子どもを追跡し、家族のつながりを回復するために、指紋や顔写真の取得年齢を、14 歳から 6 歳に引き下げることなどに合意した[241]。ただし、子どもからの強制取得は原則として行わないとされた。なお、規則の改正案は、2018 年末時点で、検討が続けられている。

---

[235] 本段落の記述は、次の資料による。“Identification of applicants (EURODAC).” European Commission website <https://ec.europa.eu/home-affairs/what-we-do/policies/asylum/identification-of-applicants_en>

[236] Regulation (EU) 603/2013, *OJ* L180, 2013.6.29, pp.1–30. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013R0603&from=EN>

[237] COM/2016/0272 final - 2016/0132 (COD) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016PC0272>; <https://eur-lex.europa.eu/procedure/EN/2016_132>

[238] European Union Agency for Fundamental Rights, *The impact of the proposal for a revised Eurodac Regulation on fundamental rights*, 2016.12.22. <http://fra.europa.eu/en/opinion/2017/impact-proposal-revised-eurodac-regulation-fundamental-rights>

[239] “European Parliament: Civil Liberties Committee position on recast Eurodac Regulation,” 2017.6.12. Statewatch website <http://www.statewatch.org/news/2017/jun/ep-eurodac-report.htm>

[240] UNICEF et al., *JOINT STATEMENT: Coercion of children to obtain fingerprints and facial images is never acceptable*, 2018.3.2. <https://www.unicef.org/eca/press-releases/joint-statement-coercion-children-obtain-fingerprints-and-facial-images-never>「児童の権利に関する条約」（平成 6 年条約第 2 号）の第 3 条第 1 号は、「児童に関するすべての措置をとるに当たっては、公的若しくは私的な社会福祉施設、裁判所、行政当局又は立法機関のいずれによって行われるものであっても、児童の最善の利益が主として考慮されるものとする。」と定めている。なお、「児童の権利に関する条約」は、「子どもの権利条約」とも称される。

[241] “Asylum: deal to update EU fingerprinting database,” 2018.6.19. European Parliament website <http://www.europarl.europa.eu/news/en/press-room/20180618IPR06025/asylum-deal-to-update-eu-fingerprinting-database>

Ⅴ　インド

インドでは、世界最大規模の国民IDシステムに生体データを追加する試みが始まっている。また、行方不明者の捜索にも顔認識技術が活用されている。

1　個人認証

インドでは10億人を超える全国民に12桁の固有のID番号を付与する「Aadhaar」（アーダール）[242]と呼ばれるプロジェクトが2009年に開始された。人口統計及び生体情報（指紋や虹彩）に基づいていることが特徴であり、世界最大の生体情報IDシステムである。データは、インド固有識別番号庁（Unique Identification Authority of India: UIDAI）が収集している。2016年には「アーダール法」[243]が制定され、法的な裏付けがなされた。アーダールへの登録は、義務ではなく任意であるものの、銀行取引や携帯電話の契約など、アーダールの身分証明カードが必要なサービスが増え続けており、登録なしの生活は困難になってきていた[244]。

UIDAIは、2018年1月、アーダールの生体認証の「追加的なオプション」として、指紋や虹彩やワンタイムパスワード（One-time Password: OTP）[245]との組合せで顔認証を使えるようにすると発表し、当初は7月1日からとしていたが、2度延期され、9月15日から開始された。顔認証を導入した理由は、高齢化や労働によって指紋が擦り切れて認証できなくなった人々のためであるという[246]。

しかし、プライバシーやセキュリティの問題が度々指摘され、プライバシー権の侵害を訴える訴訟が起こされた。インドの憲法にはプライバシー権は明文化されていなかったが、インド最高裁判所は2017年8月、プライバシー権は憲法で保障される権利であると認める判断を下した。しかし、アーダール自体には直接言及はなく、アーダールの合憲性については審理が続いていた。2018年9月、インド最高裁判所は、アーダールはプライバシーに対する基本権に違反しておらず憲法違反ではないとすると同時に、民間主体が取引時にアーダールを要求することを認めていたアーダール法第57条は憲法違反であり無効であると判示した[247]。このため、銀行口座を開設したり、携帯電話を購入したりする際に、また学校入学時に[248]アーダールの提示を義務付けることはできなくなる。

---

[242] Aadhaarは、ヒンディー語で「基礎」（foundation / base）という意味である。「アドハー」と表記されている場合が多いが、ヒンディー語での発音は「アーダール」に近いため、本稿では「アーダール」とする。

[243] Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (2016 No.18) <https://uidai.gov.in/images/targeted_delivery_of_financial_and_other_subsidies_benefits_and_services_13072016.pdf>

[244] サンディ・オン「インド13億人を監視するカード」2017.10.4. ニューズウィーク日本版ウェブサイト <https://www.newsweekjapan.jp/stories/world/2017/10/13-12.php>

[245] 時限付きのパスワードのことであり、アーダールでは有効期間は30分程度である。ウェブサイトにアーダール番号を入力すると、登録している携帯電話番号に送られてくる。"'Aadhaar OTP Is Never Sent On Email': What UIDAI Says On Aadhaar Authentication," 2018.1.4. NDTV Profit website <https://www.ndtv.com/business/aadhaar-otp-is-never-sent-on-email-what-uidai-says-on-aadhaar-authentication-1795602>

[246] Mahendra K Singh, "Now, face recognition to authenticate Aadhaar, but with biometrics or OTP," *Times of India*, 2018.1.16. <https://timesofindia.indiatimes.com/india/now-face-recognition-to-authenticate-aadhaar-but-with-biometrics-or-otp/articleshow/62515557.cms>; Deepika S, "Fingerprints, Iris Scan, and Now Facial Recognition: All your Qs on Aadhaar's new rule answered," 2018.9.15. oneindia website <https://www.oneindia.com/india/fingerprints-iris-scan-and-now-facial-recognition-all-your-qs-on-aadhaars-new-rule-answered-2776261.html>

[247] *Justice K.S. Puttaswamy (Ret'd) v. Union of India*, 2018.9.26. (W.P.(C) No.-000494-000494 / 2012) Supreme Court of India website <https://www.supremecourtofindia.nic.in/supremecourt/2012/35071/35071_2012_Judgement_26-Sep-2018.pdf>

[248] "Aadhaar not mandatory for admission in schools: Supreme Court," 2018.9.26. India Today website <https://www.indiatoday.in/india/story/aadhaar-not-compulsory-for-school-admissions-board-exams-supreme-court-verdict-1349557-2018-09-26>

２　行方不明者の捜索

女性子ども省（Ministry of Women and Child Development）によると、インドでは 2012 年から 2017 年の間に 24 万 2938 人の子どもが行方不明になっている。同省は、行方不明の子どもを検索するためのウェブサイトを作成している[249]。インドの NGO「バチパン・バッチャオ・アンドーラン」（BBA）[250] は、20 万人の行方不明の子どもたちと、子ども保護施設に住むおよそ 9 万人を人手で照合するのは困難であり、顔認識技術を活用することを 2 年間訴え続けていたところ、デリー高等裁判所の命令により、ニューデリー警察が、顔認識ソフトウェアの試行を 2018 年 4 月に 5 日間実施した[251]。およそ 45,000 人の子どもに対して顔認識技術が利用された結果、2,930 人の子どもを特定し、家族と再会させることができたという[252]。

Ⅵ　国際機関

国際連合（国連）や NGO では、人道支援、選挙管理、公衆衛生といった様々な目的で、生体認証技術の利用が検討されてきた。いくつかの国連機関は、途上国政府と協力して、積極的に生体認証技術を活用しているが、いくつかの NGO は利用に懐疑的な立場をとっている。

１　個人認証

国連の「持続可能な開発目標」（Sustainable Development Goals: SDGs）は 17 の目標と 169 のターゲットからなる。目標 16「持続可能な開発のための平和で包摂的な社会を促進し、すべての人々に司法へのアクセスを提供し、あらゆるレベルにおいて効果的で説明責任のある包摂的な制度を構築する」の 9 番目のターゲット 16.9 は「2030 年までに、すべての人々に出生登録を含む法的な身分証明（legal identity）を提供する」[253] である。全てのアフリカ諸国の個人に法的な身分証明を付与することを目指す “ID4Africa”（アイディーフォーアフリカ）という運動体は、毎年異なる国で年次大会を開催しており、発足した 2015 年はタンザニア、2016 年にはルワンダ、 2017 年にはナミビア、そして 2018 年にはナイジェリアで開催された[254]。9 月 16 日を「国際 ID デー（International Identity Day）に指定すべく、署名活動を開始した[255]。

２　テロ対策

2016 年 12 月の「安全保障理事会決議第 2322 号」[256] は、加盟国に、外国人テロ戦闘員（Foreign

[249] National Tracking System for Missing and Vulnerable Children (Ministry of Women and Child Development) website <http://trackthemissingchild.gov.in/trackchild/index.php>

[250] ヒンディー語で「子ども時代を救え運動」という意味である。本部事務所は首都ニューデリーにある。

[251] Vidya Raja, “Delhi Police Reunites 2930 Missing Children With Families in Just 5 Days! Here’s How,” 2018.4.23. The Better India website <https://www.thebetterindia.com/138862/face-recognition-software-helps-find-missing-children-in-delhi/>

[252] Anthony Cuthbertson, “Indian Police Trace 3,000 Missing Children in just Four Days Using Facial Recognition Technology,” *Independent*, 2018.4.24. <https://www.independent.co.uk/life-style/gadgets-and-tech/news/india-police-missing-children-facial-recognition-tech-trace-find-reunite-a8320406.html>

[253] 「我々の世界を変革する：持続可能な開発のための 2030 アジェンダ（仮訳）」外務省ウェブサイト <https://www.mofa.go.jp/mofaj/gaiko/oda/sdgs/pdf/000101402.pdf>

[254] ID4Africa website <http://www.id4africa.com/>

[255] 9 月 16 日は、SDGs のターゲットの番号である 16.9 に由来する。Chris Burt, “Drive for official UN International Identity Day launched at ID4Africa,” 2018.4.24. Biometric Update.com website <https://www.biometricupdate.com/201804/drive-for-official-un-international-identity-day-launched-at-id4africa>

[256] United Nations Security Council, *Resolution 2322 (2016)*, 2016.12.12. S/RES/2322 (2016) <https://undocs.org/en/S/RES/2322(2016)>

Terrorist Fighters: FTFs）や他の個人テロリスト、テロ組織について、生体情報を含む情報の共有を求めている。また、2017 年 12 月の「安全保障理事会決議第 2396 号」[257] では、FTFs を含むテロリストを、国内法及び国際人権法を遵守しつつ、責任を持って、かつ、適切に特定するために、加盟国が、指紋、写真、顔認識及びその他の関連する生体識別データを含む、生体データを収集するシステムを開発し、特定の手段とすることを義務付けた。また、国際刑事警察機構（International Criminal Police Organization: ICPO. いわゆるインターポール）等の国際機関とのデータ共有も推奨されている。

これらの決議を受けて、国連の生体認証プロジェクトが、「国連安全保障理事会テロ対策委員会事務局」（Counter-Terrorism Committee Executive Directorate: CTED）により、インターポール、国連薬物・犯罪事務所（UNODC）、国際民間航空機関（ICAO）、UNHCR などの対テロ実施タスクフォース（Counter-Terrorism Implementation Task Force : CTITF）参加組織とともに実施されている。国連事務総長は 2018 年 6 月 28 ～ 29 日に、加盟国のテロ対策機関のトップによる初のハイレベル会合を開催した[258]。会合の全体テーマは「進化するテロの脅威と戦うための国際協調を強化する」であった。そのサイドイベントの 1 つとして、6 月 29 日に、国連テロ対策局（Office of Counter-Terrorism: UNOCT）[259]、国連安全保障理事会テロ対策委員会事務局、オーストラリア国連代表部、NPO である生体認証研究所（Biometrics Institute）によるイベント「テロ対策における生体認証技術の責任ある利用と共有のための推奨される実践」が開催され[260]、それに合わせて同タイトルの報告書も発表された[261]。報告書は、国連テロ対策局に置かれた国連テロ対策センター（UN Counter-Terrorism Centre: UNCCT）の支援により、CTITF[262] のテロ対策に関連する国境管理と法執行に関する作業グループ（Working Group on Border Management and Law Enforcement Related to Counter-Terrorism）により作成されたもので、安全保障理事会決議第 2322 号（2016）及び第 2396 号（2017）が加盟国に求めるテロ対策、特に、外国人テロ戦闘員（FTFs）を含むテロリストを同定するための生体認証技術の利用に焦点を当てたものである。第 2 節では「ガバナンスと規制」と題し、国際法、人権法、倫理、データ保護の要件、プライバシー権等の観点から生体認証技術のガバナンスや規制の要件を論じ、システムのリスク管理等が扱われている。国連の加盟各国に推奨される活動として以下の 5 点が挙げられた[263]。

---

[257] United Nations Security Council, *Resolution 2396 (2017)*, 2017.12.21. S/RES/2396 (2017) <https://undocs.org/en/S/RES/2396(2017)>

[258] “High-level Conference on Counter-Terrorism, High-level Conference of Heads of Counter-Terrorism Agencies of Member States, 28 - 29 June 2018,” United Nations website <http://www.un.org/en/counterterrorism/hlc/index.shtml>

[259] 2001 年 9 月 11 日の同時多発テロを受けた安全保障理事会決議 1373 により、Counter-Terrorism Commiittee (CTC) が設置され、その後 CTITF や UNCCT が設置されたが、両者は、2017 年 6 月 15 日の国連総会決議 71/291 の採択を通して、Department of Political Affairs 内から、新設された Office of Counter-Terrorism に移った。“United Nations Office of Counter-Terrorism: About.” *idem* <http://www.un.org/en/counterterrorism/overview.shtml>

[260] “High-level Conference of Heads of Counter Terrorism Agencies: side event: United Nations Compendium of Recommended Practices for the Resposible Use & Sharing of Biometrics in Counter-Terrorism.” *idem* <https://www.un.org/sc/ctc/news/event/high-level-conference-heads-counter-terrorism-agencies-side-event-united-nations-compendium-recommended-practices-responsible-use-sharing-biometrics-counter-terrorism/>

[261] United Nations Office of Counter-Terrorism et al., *United Nations Compendium of recommended practices for the responsible use and sharing of biometrics in counter-terrorism*, 2018. <https://www.un.org/sc/ctc/wp-content/uploads/2018/06/Compendium-biometrics-final-version-LATEST_18_JUNE_2018_optimized.pdf>

[262] CTITF は、UNCCT の下で 38 の組織からなる。

[263] United Nations Office of Counter-Terrorism et al., *op.cit.*[261], pp.51-52.

・ 対テロ生体認証技術の使用に当たっては、手続的安全措置や効果的な監視を含む人権に基づくアプローチを採用すべきである。これには、関連するプライバシー法制の実施と、違反があった場合の効果的な救済措置の提供を監督するために、既存の適切な独立監督機関の権限を拡大するか、新規に設立することを含む。これはまた、対テロ目的での生体認証の利用に関する全ての国家政策や意思決定に有益な情報を与える倫理審査プロセスによって補完されるべきである。
・ 国際的なテロ行為や関連する犯罪に対して生体認証技術を適用する場合は、全ての個人のプライバシーに対する基本的権利と、生体データを含む個人データの法に基づく保護を遵守しなければならない。
・ 生体認証システムは、人為ミスや様々な形の意図的な攻撃に脆弱である。国は、今起きている、又はこれから起きる脅威を軽減するために、生体認証の適用に関する全体プロセスの定期的なリスク評価を実施することが推奨される。
・ 国は、全ての生体認証システムを国際技術基準に準拠した形で運用し、国際的な科学的水準に合致した法科学と品質管理プロセスの正式な認定を受けることが推奨される。これは、効果的な生体情報処理の強力な基礎を提供するだけでなく、生体データを共有することを望む国際的なパートナーを安心させることになる。
・ 生体認証システムを調達する際は、現在及び将来的にどのようなリソースが必要であるかを示した長期的な戦略計画が必要である。そのため、以下の事項を検討すべきである。
  － システムを購入し、試行するための初期設備投資
  － スタッフの雇用とシステムの維持管理、セキュリティや更新のための持続可能な支出
  － システムの存続期間全体に必要な予算、データベースの容量、処理能力
  － 国内あるいは国際的なネットワークへの接続や相互運用の可能性、互換可能性
  － セキュリティ、使用者のアクセスとユーザビリティ、処理量、処理スピードの観点と、対テロ生体認証システムの重要な運用上の要求のバランスをとること

３　人道援助

国際人道支援においては、UNHCR と世界食糧計画（World Food Programme: WFP）が生体認証技術の利用を積極的に進めている。他方、20 の NGO 組織の連合体であるオックスファム（Oxfam）など、慎重な態度をとっているアクターも少なくない。

UNHCR は 2003 年前後から、指紋と虹彩を含む生体認証ツールの採用を試み始めた。2010 年 12 月には、「難民の登録と照合における生体認証に関する方針」（Policy on Biometrics in Refugee Registration and Verification）を作成し、2013 年以来、新しいグローバルな「生体認証 ID 管理システム」（Biometric Identity Management System: BIMS）を開発している[264]。マラウイでの初期のパイロットテストでは 1 万 7 千人の難民が参加した。2015 年 1 月、タイで実施した最終フィールドテストを経て、2 月、BIMS を完成させた。BIMS は、指紋と虹彩の両方をカバーする。

また、UNHCR は、WFP とともに、生体情報の登録システムを運営し、難民保護から食料援助や有権者登録にも活用している。食料援助の場面では、食料を受け取りに来た全ての人の

[264] UNHCR, *Biometric Identity Management System.* <http://www.unhcr.org/550c304c9.pdf>

指紋を、UNHCRの難民登録データベースと照合し、照合できた人に食料が配られる。生体認証プロジェクトは詐欺や横流しを防止し、届けたい対象に確実に援助が届くことに貢献しているという[265]。

2018年3月には、ウガンダ政府とUNHCRは、生体認証（指紋と虹彩）を使って100万人以上の難民の本人確認を行うプログラムを立ち上げた。400人以上のスタッフが、WFPとUNHCRによって設置された68以上のサイトを移動し、当初予定の2018年9月末を少し過ぎたが、10月24日に無事に完了した[266]。目標とされた約140万人の難民の中から、約110万人（75%）の難民が確認され、生体認証登録された。

他方、オックスファムは、2015年、人道支援や開発のためのプログラムにおける生体認証技術の利用に関して、自主的な2年間のモラトリアム期間を設けることを決めた。モラトリアムの終了が近づく中、オックスファムは、そのプログラムにおいて生体認証技術が将来的にどのように位置付けられるかに関して、アドバイスと勧告を求めて、社会変革組織を支援している国際NPOであるThe Engine Roomに研究委託した。研究は2017年12月から2018年3月まで実施され、関係者へのインタビューなどに基づき、報告書が2018年4月に公表された[267]。生体認証技術が国際人道援助において近年注目されている背景と、生体認証技術を国際人道援助に利用することの便益とリスクが次のように整理された。

---

[265] World Food Programme, *WFP Innovative Food Assistance Instruments: The Biometrics Project, Kenya*. <https://documents.wfp.org/stellent/groups/public/documents/resources/wfp271054.pdf>

[266] "OPM and UNHCR complete countrywide biometric refugee verification exercise," 2018.10.30. Reliefweb website <https://reliefweb.int/report/uganda/opm-and-unhcr-complete-countrywide-biometric-refugee-verification-exercise>

[267] The Engine Room and Oxfam, *Biometrics in the Humanitarian Sector*, 2018.3. <https://oxfamilibrary.openrepository.com/bitstream/handle/10546/620454/rr-biometrics-humanitarian-sector-050418-en.pdf>

表１１　生体認証技術に関するオックスファムの研究報告書（概要）

背景	・国際援助者側から、援助が目的とした人々にきちんと届いているかどうか確認するために生体認証技術を採用してほしいという圧力が高まっている。 ・現金ベースの介入への選好が高まっていることから、銀行口座を作るための個人認証が必要となってくる。 ・国連安全保障理事会やFATF（金融活動作業部会）勧告により、マネーロンダリングやテロ資金防止のために、金融機関により厳しい本人確認が求められる。 ・途上国は個人データ保護に関する規制が緩いために、新規技術の実験場として利用されがちである。
便益	B1：援助が必要な人を特定できる（identifiability and traceability） B2：不正と重複を減らすことができる（accuracy and integrity） B3：登録と特定を簡素化できる（simplicity and efficacy）
リスク	R1：間違った適合や偽装される可能性（reliability） R2：他者に利用されたり、意図しない目的で利用されたりする可能性（reusability） R3：生体データの窃盗、喪失、悪用のリスク（security） R4：データ漏洩が起こった際や間違った噂が広がることによる評判リスク（reputation） R5：何らかの理由で拒否した場合に起こる排除の可能性（societal impacts）

（出典） The Engine Room and Oxfam, *Biometrics in the Humanitarian Sector*, 2018.3. <https://oxfamilibrary.openrepository.com/bitstream/handle/10546/620454/rr-biometrics-humanitarian-sector-050418-en.pdf> を基に筆者作成。

特にR2やR3は深刻であり、多くの難民は迫害を逃れてきた経験を持つため、登録した生体データが逆に迫害者側に渡ってしまうと、当人を危険にさらすことにつながりかねず、プログラムが意図したことと正反対の結果を招くおそれがある。このことは、ロヒンギャ難民のケースで顕在化している[268]。報告書は、「人道的組織にとって、大量の変えることのできない生体データを保持することの潜在的リスクは（中略）ほとんど全てのケースで潜在的な便益を大きく上回る」と結論付けている。また、多くの場合、生体認証以外のシステムが利用可能であるとも述べている[269]。

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）

[268] Elise Thomas, “Tagged, tracked and in danger: how the Rohingya got caught in the UN’s risky biometric database,” 2018.3.12. Wired website <https://www.wired.co.uk/article/united-nations-refugees-biometric-database-rohingya-myanmar-bangladesh>

[269] The Engine Room and Oxfam, *op.cit.*[267], p.12.