

Title	生体認証技術のELSIに関するグローバル動向：2020年4月～2022年11月
Author(s)	岸本, 充生
Citation	ELSI NOTE. 2022, 25, p. 1-74
Version Type	VoR
URL	https://doi.org/10.18910/89879
rights	
Note	

Osaka University Knowledge Archive : OUKA

<https://ir.library.osaka-u.ac.jp/>

Osaka University



大阪大学 社会技術共創研究センター
Research Center on Ethical, Legal and Social Issues

ELSI NOTE No.25

2022年12月27日

生体認証技術のELSIに 関するグローバル動向

2020年4月～2022年11月

Authors

岸本 充生

大阪大学 社会技術共創研究センター センター長 (2022年12月現在)

データビリティフロンティア機構 教授

目次

はじめに	3
1. 国内外の利活用の動向	4
1.1 国内の利活用の動向	4
1.2 Nature 誌による専門家アンケート	9
2. 米国の動向	10
2.1 連邦の動向	10
2.2 地方の動向	18
2.3 大手テック系企業の動向	22
2.4 Clearview AI 社関連の動向	25
2.5 その他の動向	27
3. 英国の動向	31
3.1 政府関係の動向	31
3.2 警察関係の動向	39
3.3 その他の動向	41
4. スコットランドの動向	44
5. カナダの動向	47
6. 欧州の動向	51
6.1 EU	51
6.2 フランス	55
6.3 イタリア	57
6.4 オランダ	58
6.5 スウェーデン	58
6.6 ギリシャ	58
6.7 ドイツ	59
7. オーストラリア・ニュージーランドの動向	59
7.1 オーストラリア	59
7.2 ニュージーランド	63
8. その他の国の動向	66
8.1 ブラジル	66
8.2 ウクライナ	67
8.3 ロシア	68
8.4 アフガニスタン	69
8.5 中国	69
8.6 インド	70
9. 国際機関の動向	70

はじめに

本 NOTE は、以下の 2 つのレポートの続編である。①は 2018 年 10 月頃までを対象としており、②は 2018 年 10 月から 2020 年 3 月を対象としている。

①国立国会図書館調査及び立法考査局「生体認証技術の動向と活用（平成 30 年度 科学技術に関する調査プロジェクト）」（2019 年 3 月）

<https://www.ndl.go.jp/jp/diet/publication/document/2019/index.html>

②岸本充生 2020: 「続・生体認証技術の動向と活用」、ELSI NOTE No.03. 大阪大学社会技術共創研究センター.

<https://elsi.osaka-u.ac.jp/research/351>

本 NOTE はこれらの続編として、2020 年 4 月から 2022 年 11 月のおよそ 2 年半を対象としている。インターネットからアクセスできるニュースを中心にまとめたものであり、内容については著者が独断でまとめたものである。また、すべてを網羅しているわけではないことに注意すべきであり、すべての項目はオリジナルの記事を確認できるようにリンクを貼ってあるので、詳細は各自で確認していただきたい。なお、ウェブアクセスは 2022 年 12 月 10 日に確認したものであり、その後、アクセス不可になる可能性はある。

1. 国内外の利活用の動向

1.1 国内の利活用の動向

●新駅「高輪ゲートウェイ駅」のオープンを記念したイベントで、（コロナで延期になっていたが）2020年7月、JR東日本が NEC と連携した「A DAY ～ちょっとミライのつながるセカイ～」と題するパビリオンを開催し、その中で、顔認証を用いた実験が行われた¹。担当の JR 東日本 MaaS・Suica 推進本部の深津智威氏は、「顔認証を活用した方式なら、IC カード自体を持たず、タッチ不要でご利用頂けるようになります。赤ちゃんを抱えたお母さんも、車いすの人もお年寄りも、荷物をたくさん抱えた外国人をはじめとした旅行者も、タッチレスで、より快適・便利に鉄道をご利用頂けるのでは、と思います。」とコメントしている²。また、チケット認証だけにとどまらず、MaaS との連携なども視野に入れているという。

●NEC は 2020 年 7 月 2 日、生体認証・映像分析技術とサーマルカメラを組み合わせた、新型コロナウイルス感染症をはじめとする感染症対策ソリューションの販売を開始すると発表した³。2020 年 8 月末から学校や企業、商業施設などに提供するという。

●2020 年 7 月 6 日、ダイドードリンコ株式会社は NEC の顔認証技術を活用して、日本初となる自動販売機で顔認証による購入が可能となる「顔認証決済自販機」の実証実験を 7 月 3 日より開始したことをプレスリリースした⁴。期間は 3 か月で、実験場所はダイドードリンコ（株）本社、大同薬品工業（株）関東工場、NEC 本社等。利用者は、スマートフォン等の端末を用いて事前に顔画像やクレジットカード情報、パスコードを登録することで、自販機で購入時に顔とパスコードの 2 要素認証により決済できる仕組み。

●厚生労働省のグレーゾーン解消制度に、申請事業者「宿泊施設事業者へチェックインシステムの提供を検討している企業」から、事業名「顔認証技術を活用したホテル無人チェックイン」として 2020 年 7 月 1 日に申請があり、同月 29 日付で医薬・生活衛生局生活衛生課から回答が寄せられた⁵。「玄関帳場又はフロント及び宿泊者名簿に関し、衛生等管理要領に定める要件を満た

¹ <https://gasket.bizright.co.jp/2020/07/31-13/>

² <https://wisdom.nec.com/ja/feature/smartcity/2020042801/index.html>

³ https://jpn.nec.com/press/202007/20200702_01.html

⁴ https://www.dydo.co.jp/corporate/news/2020/200706/pdf/20200706_02.pdf
https://jpn.nec.com/press/202007/20200706_02.html

⁵ https://www.mhlw.go.jp/shinsei_boshu/gray_zone/gray_zone.html 回答は
<https://www.mhlw.go.jp/content/000654354.pdf>

すものとみなして差し支えない。ただし、宿泊施設の所在地を管轄する自治体の条例等により規制が設けられている場合には、当該規制に従う必要がある。」と結論づけられた。

●三井不動産は、2020年8月7日に京都市の市営地下鉄五条駅近くに開業する新ホテルブランド「sequence（シークエンス）」で、顔認証による自動チェックインや客室解錠が可能となるシステムを導入した⁶。事前にアプリで登録する。

●カシマスタジアムで、2020年8月16日、約50人の報道陣を対象に、事前に顔写真を登録し、受付に設置された顔認証による入退館管理を行う生体認証導入に向けたテストが実施された⁷。これはスマートスタジアム計画の一環である。

●東芝インフラシステムズ株式会社は2020年8月17日付で、Osaka Metro 向けの次世代改札機実証実験システムについて、1台の改札機で顔・QRコード認証の両方式での運用が可能となり、マスク着用時の顔認証精度が向上したとのニュースリリースを公表した⁸。

●2020年9月13日、共同通信が「捜査に顔認証、全国の警察で」と報じた⁹。記事は短いもので、「全国の警察が今年3月から、犯行現場などの防犯カメラや、事件に関連する会員制交流サイト（SNS）などの顔画像を、過去に逮捕した容疑者の顔写真データベースと照合する「顔認証システム」の運用を始めたことが12日、警察庁への取材で分かった。」と報じた。

●NECは富山市から受託した「富山市 顔認証システム社会実験」を2020年10月1日から開始することを発表した¹⁰。「生体認証データを一つの共通IDとして利用し、富山市中心市街地と岩瀬地区の店舗30か所で顔認証決済やおもてなしサインエージ体験などのサービスを社会実験として順次試験的に導入」するとのことである。

●独立行政法人 国立高等専門学校機構 鹿児島工業高等専門学校と NEC は2020年10月8日、学校教育におけるデジタルトランスフォーメーション(DX)や地域振興等の活動を通じた新たな社会価値の創造を目的に包括連携協定を締結し、その中で、図書館と女子寮に NEC の顔認証システムを導入することになった¹¹。

⁶ <https://www.nikkei.com/article/DGXMZO62323880V00C20A8LKA000/>

⁷ <https://www.47news.jp/5151289.html>

⁸ <https://www.toshiba.co.jp/infrastructure/news/20200817.htm>

⁹ <https://jp.reuters.com/article/idJP2020091201001899>

¹⁰ https://jpn.nec.com/press/202010/20201001_02.html

¹¹ https://jpn.nec.com/press/202010/20201008_03.html

●2021年に延期になった東京オリンピックで、コロナ対策として、会場関係者以外に、観客に対しても顔認証技術の活用を検討していることが2020年10月21日、報じられた¹²。「競技会場への入場時などで観客の顔を記録し、体表面温度などを検知。画像情報をもとに会場内の防犯カメラで移動経路を記録しておくことで、後に感染が発覚した場合に濃厚接触の可能性のある人を推定し、早期に通知しやすくすることなどが検討されている。」

●渋谷の三書店で実施されている「渋谷書店万引対策共同プロジェクト」¹³は2020年12月1日、2019年7月30日から、2020年7月31日までの1年間の報告をニュースリリースした¹⁴。「プロジェクト開始前に、1件だけ1参加店への抗議があったが、それも開示と同時になくなり、以降アクシデント及び一切のトラブルは起きていない。」とのことである。「運用検証委員会」は4名の専門家からなる。2021年11月10日には開始後2か年のお知らせがニュースリリースされ、マスク着用客が増えたものの顔認識ソフトウェアの更新により以前と同程度の精度が保たれたという¹⁵。登録人数は44名で前年度より5名増加、事案件数は71件で前年度より18件増加したという。

●前橋市は、国土交通省が取り組む「令和2年度日本版MaaS推進・支援事業対象地域」として採択を受け、2020年12月21日から2021年3月12日まで、前橋版MaaS実証実験として『MaeMaaS』を実施した¹⁶。前橋市を含む前橋市新モビリティサービス推進協議会が「MaeMaaS」における各種の実証実験を進めている。その中で、自動運転バスと顔認証とマイナンバーカードを連携した実験が、2月15日から28日まで行われた¹⁷。日経新聞の報道によると、顔認識のためカメラ3台を車内に導入し、乗車時の本人確認に利用する1台を除く2台によって、車内の乗客の年代や性別を分析し、さらに、車内カメラの映像はデータ処理した後、翌日までに削除するとされている¹⁸。これらを受けて2021年10月1日から『MaeMaaS（前橋版MaaS）』は社会実装中である¹⁹。

¹² <https://www.nikkei.com/article/DGXMZO65291520R21C20A0CC1000/>

¹³ <https://www.manboukikou.jp/shibuyapjrj/>

¹⁴ <https://www.manboukikou.jp/shibuyapjrj/2020/12/02/1263/>

¹⁵ <https://www.manboukikou.jp/shibuyapjrj/2021/11/10/1278/>

¹⁶ <https://www.city.maebashi.gunma.jp/material/files/group/9/5MaaS.pdf>

¹⁷ <https://www.city.maebashi.gunma.jp/soshiki/seisaku/kotsuseisaku/gyomu/5/2/26546.html>

¹⁸ <https://www.nikkei.com/article/DGKKZO68567010X20C21A1L60000/>

¹⁹ <https://www.city.maebashi.gunma.jp/soshiki/seisaku/kotsuseisaku/gyomu/5/2/30314.html>

- 2021年1月20日、株式会社ビットキーと阪神電気鉄道株式会社は、阪神甲子園球場において、「顔認証による入場管理の実証実験」を、球場関係者約40名の入退場を対象として、2021年1月21日（木）から3月下旬まで実施することを発表した²⁰。
- 2021年1月26日、東大病院の研究者が、認知機能の低下した患者と健常者の顔写真を見分けることができるAIモデルを開発したこと発表した²¹。
- 神奈川中央交通株式会社は2021年2月1日、2021年2月9日から3月5日まで、横浜市内の公道で「中型自動運転バスの実証実験」を実施することを発表した²²。経済産業省・国土交通省の事業²³を受託した産業技術総合研究所によって選定され実施するものである。顔認証による自動決済を想定した仕組みは、ソフトバンク株式会社の子会社であるBOLDLY株式会社により提供されるシステムを用いて検証される²⁴。「乗車口と降車口付近に設置したカメラによって乗降時の乗客の画像を読み込み、位置情報と連携させることで各乗客の乗車区間を把握し、降車の際、降車口付近のモニターにその乗客の乗車区間を瞬時に表示する。同社は、将来的にこのシステムと決済システムを連携させ、乗車距離に応じた運賃の決済を顔認証により実現することを目指すとしている。」とのことである²⁵。顔の特徴量情報については、「顔の特徴点のデータから参加者の乗車バス停と降車バス停を照合し、乗車区間の把握に活用します。個人情報保護の観点から取得した顔の特徴点データは当日限りの利用とし外部サーバへの保存は行いません。」という扱いをすると書かれている²⁶。
- 2021年3月、読売新聞東京本社、読売巨人軍、東京ドームの3社は、「ジャイアンツ×東京ドーム デジタルトランスフォーメーション（DX）プロジェクト」の一環として、2021年シーズンを通して、顔認証技術を使って、物販の決済や入場管理などの技術実証を行うことを発表した²⁷。2022年2月24日には、オープン戦で、事前登録した顔画像により入場や決済ができ

²⁰ <https://www.hanshin.co.jp/company/press/detail/3067>

²¹ <https://www.h.u-tokyo.ac.jp/participants/research/saishinkenkyu/20210126.html>

²² <https://www.kanachu.co.jp/news/pdf01/somu/2021/02.01release.pdf>

²³ 「高度な自動走行・MaaS等の社会実装に向けた研究開発・実証事業：専用空間における自動走行などを活用した端末交通システムの社会実装に向けた実証顔認証システムによる運賃決済を想定した仕組みの検証」

²⁴ https://www.softbank.jp/drive/set/data/press/2021/shared/20210201_01.pdf 日本コンピュータビジョン株式会社が提供する顔認証ソフトウェア開発キットを活用して開発したシステムが用いられる。

²⁵ https://jidouten-lab.com/u_autonomous-taxi-face-solution

²⁶ <https://www.kanachu.co.jp/news/pdf01/somu/2021/02.01release.pdf>（3ページの1. 遵守事項の※1より）

²⁷ https://www.giants.jp/G/gnews/news_3915647.html 「今回の技術実証には、ご協力いただける

るサービス「facethru（フェイスルー）」を順次開始することを発表した²⁸。ベースとなる顔認証技術は引き続き、パナソニックの顔認証クラウドサービス「KPAS クラウド」を使用している。

●2021年3月25日、成田国際空港と東京国際空港ターミナルは、NECの生体認証「Bio-IDiom」を搭載した新しい搭乗手続き「Face Express」の実証実験を4月13日より開始し、7月から本格運用を開始することを発表した²⁹。これは一般的に「OneID」と呼ばれている仕組みである。成田国際空港のウェブサイトのQ&Aには「プライバシーについて教えてください」という項目があり、Face Expressに登録した顔画像及びその他個人を識別可能なデータは、24時間以内に自動消去されるという説明がある。また、顔認証による撮影を望まない客には、有人チェックインカウンターが用意されていることも説明されている³⁰。

●近畿大学とグローリー株式会社は2021年4月2日、近畿大学東大阪キャンパス内で顔認証による手ぶら決済サービス「BioPay（バイオペイ）」に関する実証実験を開始することを発表した³¹。

●Osaka Metroは2022年11月16日、12月1日から車いすを使用したお客さまを対象に、御堂筋線長居駅で顔認証改札機の実証実験を行うことを発表した³²。

●株式会社トライアルカンパニーは2022年11月19日、AIカメラによる24時間顔認証決済の「TRIAL GO 日佐店」に一般導入し、導入拡大に向けた実証実験を開始することを発表した³³。

方のみの顔データを利用します。無断でご来場者の方の顔データを取得することはありません。」とのことである。

²⁸ https://www.giants.jp/G/gnews/news_3916587.html

²⁹ <https://www.narita-airport.jp/jp/faceexpress/>

³⁰ <https://www.narita-airport.jp/jp/faceexpress/privacy/>

³¹ <https://newscast.jp/news/8034653>

³² https://subway.osakametro.co.jp/news/news_release/20221116_nagai_kaoninsho_kaisatsuki.php.

³³ <https://files.microcms-assets.io/assets/87d00534bf46460ea2837c178a963cd0/9394b668d65347f692fedaf830f0ab0d/%E3%80%90NEWS%20RELEASE%E3%80%9124%E6%99%82%E9%96%93%E9%A1%94%E8%AA%8D%E8%A8%BC%E6%B1%BA%E6%B8%88%E3%80%8CTRIALGO%E6%97%A5%E4%BD%90%E5%BA%97%E3%80%8D%E3%81%A7%E4%B8%80%E8%88%AC%E5%B0%8E%E5%85%A5%E9%96%8B%E5%A7%8B.pdf>

1.2 Nature 誌による専門家アンケート

●Nature 誌は 2020 年 2～3 月に、480 人の世界中の顔認識、コンピュータビジョン、AI 分野の研究者から、顔認識研究に関する倫理的課題に関する見解を e-mail で収集した結果を 2020 年 11 月に公表した³⁴。質問項目として、脆弱な人々への適用（例：ウイグル人）やセンシティブなパーソナルな特徴の推定（ジェンダー、性自認、年齢、人種等）などに関するものが挙げられた。

Q. 社会的弱者に対する研究についてのあなたの意見は？

Q. 研究コミュニティは、倫理的に疑問があるとされる研究について何をすべきか、あなたの意見は？

Q. センシティブなパーソナルな特徴によって顔を分類する研究についてのあなたの意見は？

Q. 人々の顔の大規模データセット（多くの場合インターネット上からスクレイプされる）を学習データとして利用する場合に研究者にはどのような許可が必要か？

Q. 顔認識技術の研究は、IRB（倫理審査委員会）やその他の倫理組織からの事前の承認を必要とすべきか？

Q. IRB は、この種の研究についての倫理的課題を判断するために十分な能力を備えていると思うか？

Q. 顔認識研究の倫理についての訓練を受けたか？

Q. 次のグループによる顔認識技術の利用についてどれくらい快適 (comfortable) か？－企業内研究者、大学内研究者、民間企業、警察、政府

Q. 顔認識技術が次のようなやり方で使われることに対してどれくらい快適 (comfortable) か？
－警察（犯罪後の容疑者調査）、空港、スマホ、会社、公共交通、学校（出席管理）、警察（公共空間での群衆監視）、学校（生徒の表情と行動）。会社（公共空間における歩行者の追跡）、労働、など。

Q. 政府や警察といった公的機関が顔認識技術を利用することをどう思うか？もし追加の規制が

³⁴ Richard Van Noorden (2020). What scientists really think about the ethics of facial recognition research, <https://www.nature.com/articles/d41586-020-03257-6> アンケート結果は、The ethical questions that haunt facial-recognition research, <https://www.nature.com/articles/d41586-020-03187-3>

必要だと思うならどんな？

Q. 出席や入退室管理といった、民間企業による顔認識技術の利用をどう思うか？もし追加の規制が必要だと思うならどんな？

2. 米国の動向

2.1 連邦の動向

●住宅・都市開発省（HUD）は、Ron Wyden 上院議員（民主党）へのレター（2020年5月26日付）で、120万家庭あるとされる公的住宅（public housing）で顔認識技術がどれくらい利用されているかについて情報を持ち合わせていないことを明らかにしたという³⁵。

●警察活動と人種差別の議論が過熱している中で、2020年6月25日、上院の民主党議員である Ed Markey (D-Mass.)と Jeff Merkley (D-Ore.)と下院の民主党議員である Pramila Jayapal (D-Wash.) と Ayanna Pressley (D-Mass.)が連邦議会に、議会が認可しない限り、連邦政府が顔認識技術や他の生体認証技術を監視目的に利用することを禁じる法案（Facial Recognition and Biometric Technology Moratorium Act）を（上下両院に同時に（bicameral））提案したことを発表した³⁶。

●米国商務省（Department of Commerce）の Bureau of Industry and Security (BIS)は連邦官報に2020年7月17日、「人権への懸念がある先進監視システムとその他の品目（‘Advanced Surveillance Systems and Other Items of Human Rights Concern.’）」と題する通知を掲載し、パブリックコメントを求めた³⁷。「顔認識ソフトウェアや他の生体認識技術」を含む10項目が挙げられた。BISは次の3つの観点からのコメントを求めている。

(1) Information (including performance criteria) that may distinguish purely or predominantly

³⁵ <https://www.cnet.com/news/us-government-doesnt-know-how-it-uses-facial-recognition-in-public-housing/>

³⁶ <https://www.markey.senate.gov/news/press-releases/senators-markey-and-merkley-and-reps-jayapal-pressley-to-introduce-legislation-to-ban-government-use-of-facial-recognition-other-biometric-technology>

³⁷ <https://www.federalregister.gov/documents/2020/07/17/2020-15416/advanced-surveillance-systems-and-other-items-of-human-rights-concern> 米国輸出管理改革法（Export Control Reform Act of 2018：ECRA）に基づき、BISが輸出管理規則（Export Administration Regulations：EAR）のもとで犯罪防止と検出（CC）目的で、商務省輸出規制品リスト（Commerce Control List：CCL）の品目リストを定めている。

- consumer or commercial applications from applications purely or predominantly for use by law enforcement or security services and/or used in mass surveillance, censorship, privacy violations or otherwise useful in committing human rights abuses; 商業用途と（プライバシーや人権侵害の可能性が高い）法執行や安全保障目的の区別方法
- (2) the impact of adding to, modifying, or removing items from the CCL on U.S. support of human rights throughout the world; 世界中の人権に対する米国の支援への影響
- (3) the impact that changes of controls would have upon the competitiveness of U.S. business and industry. 米国の産業界の競争力への影響

●2020年7月、政府アカウントビリティ局（GAO）は報告書「顔認識技術：商業利用に関するプライバシーと正確性の問題」を公表した³⁸。プライバシー面と正確性の側面を精査した結果、2013年の勧告³⁹を繰り返すこととなった、すなわち、議会に対して、連邦の消費者プライバシー枠組みを更新するように要請した。

●2020年9月、GAOから報告書「CBP（税関・国境警備局）とTSA（運輸保安庁）はプログラムを実施するための手順を進んでいるが、CBPはプライバシーとシステムパフォーマンスの問題に取り組むべきである」が公表された⁴⁰。CBPが進めている生体認証出入国プログラム（Biometric Entry-Exit Program）において、プライバシー通知に十分な情報を含むサインページを分かりやすいところに設置する、プライバシー監査を実施する、等の勧告を行った。TSAについてはパイロット・テストが限定的であったことから、TSAのプライバシー保護原則への準拠を完全に評価するのは時期尚早であるとした。

●2020年9月11日、国土安全保障省（DHS）が、市民権・移民サービス（U.S. Citizenship and Immigration Services : USCIS）による、生体情報の収集及び使用に関する提案ルール「米国市民権・移民サービスによる生体情報の収集と利用（“Collection and Use of Biometrics by U.S. Citizenship and Immigration Services”）」を官報に公表した⁴¹。これは生体情報の収集の対象を14歳未満の子どもにまで拡大し、また収集される生体情報の範囲を、現行の写真、指紋、署名から、掌紋、声紋、虹彩、顔画像、DNAなどへと大幅に拡大するものであった。10月13日まで

³⁸ <https://www.gao.gov/products/gao-20-522>

³⁹ <https://www.gao.gov/products/gao-13-663>

⁴⁰ <https://www.gao.gov/products/gao-20-568>

⁴¹ <https://www.federalregister.gov/documents/2020/09/11/2020-19145/collection-and-use-of-biometrics-by-us-citizenship-and-immigration-services>

パブリックコメントを求めた。この提案に対して、EFF（電子フロンティア財団）⁴²や EPIC（電子プライバシー情報センター）⁴³は反発している。また9月には、多数の団体がパブコメ期間の60日間への延長を請願していた。このパブリックコメント期間中である9月21日には、DHSのOffice of Inspector General（監査官室）が、2019年にCBPの下請け業者がサイバー攻撃を受け、18万人以上の旅行者の顔写真を漏洩させたとするサイバーセキュリティ事案に関する報告書を公表した⁴⁴。本提案ルールについての30日間のパブリックコメント期間が終了し、およそ5000件のコメントが集まった。WPF（世界プライバシー・フォーラム）は上記のパブリックコメントとして、米国DHSに対して、マルチステークホルダープロセスを導入して、子どもへの生体認証技術の利用に関する倫理ガイドラインの策定を要請したり、英国のBiometric Forensics Ethics Groupのような第三者助言サービスの利用を勧告したりした⁴⁵。

●国土安全保障省（DHS）のHomeland Security Advisory Council（HSAC）のバイオメトリクス小委員会（Biometrics Subcommittee）は、2020年4月の諮問に対する最終報告書を11月12日付で公表した⁴⁶。報告書では、DHSの各部門が生体認識ツールを利用する際にそれらを監督・協調する責任を持つ組織としてBiometrics Oversight and Coordination Council（BOCC）を設置することを含む勧告を10点公表した。EPICは報告書に対するコメントを公表している⁴⁷。

●国土安全保障省（DHS）は、入国者からの生体情報の収集に関する新ルールの最終案をOMBに提出したと12月16日、報じられた⁴⁸。規制監督機関であるOIRA（情報及び規制問題室）は2021年1月13日に、最終ルール（RIN: 1615-AC14）⁴⁹を、審査開始から1か月足らずで承認した⁵⁰。このルールでは、生体情報の収集件数が年間で、現行の390万件から600万件に増える見込

⁴² <https://www.eff.org/deeplinks/2020/09/tell-department-homeland-security-stop-collecting-dna-and-other-biometrics>

⁴³ <https://epic.org/2020/10/epic-urges-dhs-to-extend-comme.html>

⁴⁴ <https://www.oig.dhs.gov/sites/default/files/assets/2020-09/OIG-20-71-Sep20.pdf> 本件はGigazineにおいても日本語記事として報じられた。<https://gigazine.net/news/20200925-dhs-facial-recognition-photo-hack/>

⁴⁵ <https://www.worldprivacyforum.org/2020/10/wpf-advises-that-dhs-biometric-collection-proposal-needs-scientific-factual-ethical-and-human-rights-basis-urges-creation-of-transparent-multistakeholder-process-to-work-on-ethical-guidelines-rega/>

⁴⁶ <https://www.dhs.gov/publication/biometrics-subcommittee>

⁴⁷ <https://epic.org/apa/comments/EPIC-Comments-DHS-HSAC-Biometrics-Subcomm-Report.pdf>

⁴⁸ <https://www.biometricupdate.com/202012/dhs-submits-finalized-new-immigration-biometrics-collection-rule>

⁴⁹ <https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202010&RIN=1615-AC14>

⁵⁰ <https://www.reginfo.gov/public/do/eoDetails?rrid=131532>

みである⁵¹。政権末期に駆け込みで承認される、いわゆる「真夜中規制 (midnight regulations)」の1つとなる見込みであったが、DHS はトランプ政権終了時までに最終ルールを官報に掲載できなかった。バイデン新政権は、官報に公表されていないすべてのルールを撤回することを要請した。DHS は 2021 年 5 月 10 日付の官報 (FR) において本提案を公式に撤回した⁵²。パブリックコメントの大半が反対意見であるなど、批判の高まりを受けたものである。

●連邦取引委員会 (FTC) は、カリフォルニア州の写真アプリ (“Ever”) ⁵³の開発会社である Everalbum, Inc. の行為について調査し、写真ストレージアプリにおける顔認識技術の利用とアカウントを無効にしたユーザの写真とビデオの保持について消費者を欺いたとする申し立てを行った⁵⁴。同社は、2017 年 2 月に Ever アプリに新機能 (“Friends”) をデフォルト設定で導入し、顔認識技術を使ってユーザの写真进行分类し、タグ付けを行うようになったにもかかわらず、2018 年 7 月から 2019 年 4 月までの間、ユーザによって選択されない限り顔認識技術は使っていないと主張していた (ただし、2018 年 5 月からイリノイ、テキサス、ワシントン州と EU に住むユーザだけは顔認識技術を適用するかどうか選択できるようにした)。また、2017 年 9 月から 2019 年 8 月まで同社は、Ever ユーザの写真に誰でも利用可能なデータセットから得られた顔写真を合わせた数百万の顔写真を、顔認識技術の開発に使用しており、Ever アプリに利用し、さらには企業カスタマーに販売していた。また、少なくとも 2019 年 10 月まで、アカウントを無効にしたユーザの写真や動画を消去していなかった。

2021 年 1 月 11 日、連邦取引委員会 (FTC) は、Everalbum, Inc. が申し立てについて FTC と和解したことを発表した⁵⁵。提案された和解案では、Everalbum, Inc. は、写真や動画において顔認識技術を利用する前に、消費者の明示的な同意を得なくてはならないこと、及び、ユーザがアップロードした写真や動画を利用して開発したモデルやアルゴリズムを消去することが要請された。和解案は 2 月 24 日までパブリックコメントに付される。本件は、FTC が顔認識技術の誤使用に狙いを定めた初めてのケースとされる⁵⁶。これは、FTC にとって今後、顔認識技術の取締りの優

⁵¹ <https://news.bloomberglaw.com/daily-labor-report/final-rule-expanding-biometrics-for-immigrants-clears-review>

⁵² <https://www.govinfo.gov/content/pkg/FR-2021-05-10/pdf/2021-09671.pdf>

⁵³ Ever アプリは 2020 年 8 月 31 日に終了し、Paravision としてリブランドされた。
<https://www.paravision.ai/>

⁵⁴ https://www.ftc.gov/system/files/documents/cases/everalbum_complaint.pdf

⁵⁵ <https://jolt.law.harvard.edu/digest/everalbum-inc-in-first-facial-recognition-misuse-settlement-ftc-requires-destruction-of-algorithms-trained-on-deceptively-obtained-photos>

⁵⁶ <https://news.bloomberglaw.com/daily-labor-report/ftcs-first-settlement-on-facial-recognition-technology-yields-lessons>

先順位が高いことを示している。また、BIPA が、“biometric identifier“の定義から除外している「写真」も FTC はターゲットすることも明らかになった。FTC は 2021 年 5 月に和解を最終決定したことを発表した⁵⁷。Everalbum, Inc.は以下のような条項に従わなければならない。

- ユーザから収集した生体情報を利用して顔認識技術を訓練・開発・変更する前に、生体情報を収集したユーザに対して、「プライバシーポリシー」「利用規約」ページや他の類似文書とは別に、同社が生体情報を使用し、該当する範囲で共有するすべての目的を明確かつ明示的に開示し、彼らから肯定的かつ明示的な同意を得ること。
- この命令の発行日から 30 日以内に、この命令の発行日以前に Ever アカウントの停止を要求したユーザから同社が収集したすべての写真とビデオを削除または破棄し、偽証罪に問われる条件で宣誓して、すべての情報が削除または破棄されたことを確認する書面を FTC に提供すること。
- この命令の発行日から 90 日以内に、その日までに明示的な肯定的な同意をしていないユーザから収集した生体情報に由来するすべての画像を削除または破棄し、偽証罪に問われる条件で宣誓して、かかる情報がすべて削除または破棄されたことを確認する書面を FTC に提出すること。
- この命令の発行日から 90 日以内に、「影響を受ける成果物」（＝「Ever」モバイルアプリケーションのユーザから収集した生体情報を使用して開発されたモデルまたはアルゴリズムの全部または一部）を削除または破棄し、偽証罪に問われる条件で宣誓して、削除または破棄を確認する書面を FTC に提供すること。

●2021 年 2 月 16 日、多数の市民団体や個人が合同で、就任した直後のバイデン大統領宛てにレター⁵⁸を出して、連邦政府が顔認識技術（FRT）の利用について、次のような事項を要請した。顔認識技術は、黒人や有色人種（Black and Brown）の人々、LGBTQ の人々、女性、その他周辺化されたコミュニティに対して特に危険であることが指摘されている。

・バイアスがこれらのシステムに広がり、議会が、特定の状況において、プライバシー上の利益を保護し、危険で規制されない技術によって引き起こされる危害を防止する十分な安全策を

⁵⁷ <https://www.ftc.gov/news-events/news/press-releases/2021/05/ftc-finalizes-settlement-photo-app-developer-related-misuse-facial-recognition-technology>

⁵⁸ <https://www.washingtonpost.com/context/civil-rights-group-letter-to-president-biden-calling-for-facial-recognition-ban/ad27090b-7b93-4f44-9ca9-1793157666b6/>

もって、技術の利用を承認するよう行動しない限り、すべての連邦政府の FRT や他の形態の生体認証技術の利用についてモラトリアムを設けるように大統領府が素早く対応すること

・州および地方政府が連邦からの資金を使用して FRT を購入したり FRT にアクセスしたりするのを防ぐこと

・マーキー (Markey) 上院議員によって 2020 年 6 月に提案された「顔認識および生体認証技術モラトリアム法」を支持すること。この法案は、連邦モラトリアム法となり、これらの技術の連邦資金調達に追加の制限を課すことになる。

●政府アカウンタビリティ局 (GAO) が 2021 年 6 月、「DHS は生体識別管理システムを実装するために重要な実務を完全に施行する必要がある」と題する報告書を公表した⁵⁹。DHS はもともと Homeland Advanced Recognition Technology (HART) を 2021 年までに導入する計画であったが、予定よりも大きく遅れ、2021 年 12 月までに Increment 1 が実装され、残りの Increment の実装は 2022 年と 2024 年に予定されている。

●民主党の Markey 上院議員らは 2021 年 6 月 15 日、「顔認識および生体認証技術モラトリアム法案 (Facial Recognition and Biometric Technology Moratorium Act of 2021)」を再提案した⁶⁰。前の議会で廃案になっていたもので、法的な裏付けがない限り、連邦政府による顔認識技術を始めとする生体認証技術の利用を禁止するものである。

●米国下院法務委員会の犯罪・テロ・国土安全保障小委員会で 2021 年 7 月 13 日、公聴会「顔認識技術：法執行による利用を検討する」が開催された⁶¹。証人として下記の専門家が登壇した。

Dr. Cedric L. Alexander (ジョージア州デカルブ郡の元公安局長、21 世紀の警察に関するオバマ大統領タスクフォースの元メンバー)

Ms. Kara Frederick (ヘリテージ財団技術政策センター研究員)

Mr. Barry Friedman (ジェイコブ・D・フックスバーグ法学教授、ニューヨーク大学法学部警察プロジェクト部長)

Dr. Gretta L. Goodwin (政府アカウンタビリティ局 (GAO) の国土安全保障及び法務部門のディレクター)

⁵⁹ <https://www.gao.gov/products/gao-21-386>

⁶⁰ <https://www.markey.senate.gov/news/press-releases/senators-markey-merkley-lead-colleagues-on-legislation-to-ban-government-use-of-facial-recognition-other-biometric-technology>

⁶¹ <https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4635>

Ms. Jennifer E. Laurin (テキサス大学オースティン校ロースクールのライト C.モロー教授)

Mr. Bertram Lee Jr. (メディアおよび技術政策顧問、公民権および人権に関するリーダーシップ会議)

Mr. Brett Tolman (Right on Crime の事務局長)

Mr. Robert Williams (ミシガン州ファーミントンヒルズ)

●政府アカウントビリティ局 (GAO) は 2021 年 8 月、「顔認識技術：連邦政府機関による利用の現状と計画 (Facial Recognition Technology: Current and Planned Uses by Federal Agencies)」(GAO-21-526) と題する報告書を公表した⁶²。24 の連邦政府機関を対象に調査が行われ、16 の機関が顔認識技術を使用しており、例えば、職員がこの技術を使って連邦政府のスマートフォンをロック解除できるようにしている等と回答した。犯罪捜査の手がかりを得るために使用していると回答したのは 6 組織、建物や施設への出入りを管理するなどの物理的なセキュリティに利用していると回答したのは 5 組織、10 組織が利用を拡大する予定と回答した。

●国土安全保障省 (DHS) の科学技術局 (Science and Technology Directorate : S&T) は 2021 年 11 月 5 日付の官報 (FR) で、「新興技術の人々の認知 (Public Perceptions of Emerging Technology)」と題する情報収集要請 (ICR) の通知を掲載した⁶³。具体的には、顔認識を含む AI の適用のリスクとベネフィットに関して人々がどのように受け止めているかを理解することを目的としている。コメント締め切りは 12 月 6 日である。

●国内国歳入庁 (IRS) は、納税者がオンラインでアカウントを作成する際にサードパーティ (である ID.me 社) の顔認識技術を使って、セルフイーを提出するかビデオチャットを使ってエージェントと接続することを要求していたが、プライバシー、データセキュリティ、インターネットにアクセスできない人々の存在などを懸念するプライバシー擁護団体や市民からの反発を受けて、2022 年 2 月 7 日、納税者がオンラインでアカウントを作成する際に顔認識技術を使って認証することを近いうちにやめることを表明した⁶⁴。代わりに、顔認識技術を使わない認証プロセスの開発も急いで進めることを表明した。同日には、Wyden 上院議員 (民主党) らが IRS 委員長の

⁶² <https://www.gao.gov/products/gao-21-526>

⁶³ <https://www.federalregister.gov/documents/2021/11/05/2021-24247/public-perceptions-of-emerging-technology>

⁶⁴ <https://www.irs.gov/newsroom/irs-announces-transition-away-from-use-of-third-party-verification-involving-facial-recognition> ニュース報道記事はこちら
<https://www1.cbn.com/cbnnews/us/2022/february/irs-drops-facial-recognition-requirement-for-tax-access-after-critics-cite-privacy-issues>

Chuck Rettig 氏に対してレターを送付し、顔認識技術の利用をやめるように要請した⁶⁵。その中で、顔認識技術が脆弱な人々に対してバイアスを持つことに加えて、政府の基盤インフラを民間部門にアウトソースすることへの警戒についても触れられた。また、同日、Lieu 氏ら 4 人の民主党議員も Rettig 氏宛にレターを送付し、顔認識技術の利用をやめるよう要請した⁶⁶。1 つは、2019 年に起きた下請企業によるデータ漏洩事件を引用しつつ、生体情報データベースがサイバー攻撃の対象になりうる点が挙げられた。次に、顔認識技術の正確性やバイアスへの懸念、さらに、ID.me 社との契約プロセスや ID.me 社自体の透明性への懸念が表明されている。

これに対して、IRS と納税者らはこれまで、本人の申請前に他人になりすまして税金の還付を請求する ID 詐欺に悩まされ続けてきており、同様のことはコロナ救済給付金でも発生していた。これらへの対策として ID.me 社と契約したという背景がある。そのため、顔認識システムの導入をやめることのコストは結局、納税者が負担し続けることになること、ワシントンポスト紙に掲載されたオピニオン記事は主張している⁶⁷。

●2022 年 2 月 9 日、Markey 上院議員（民主党）らは、いくつかの連邦省庁（DHS、DOJ、DOD、DOI、HHS）に対して、Clearview AI 社のものを含む顔認識技術の利用をやめるように要請するレターを送付した⁶⁸。市民の自由やプライバシー権への重大な脅威となること、さらに、黒人、有色人種、移民のコミュニティへの脅威となることが強調された。

●2022 年 2 月 15 日、Wyden 上院議員らは労働省に対して、失業保険やその他の重要な政府サービスへのアクセスのために顔認識技術の利用を要求すべきではないとするレターを送付した⁶⁹。半数以上の州が ID.me のサービスを利用しており、これらを GSA（一般調達庁）の Login.gov を含む別のやり方に替えるように要請した。

●バイデン大統領は、2022 年 5 月 22 日、「国民の信頼と安全を向上させるため、効果的でアカウントブルな警察活動および刑事司法の実践を推進するための大統領令」を公布した⁷⁰。Sec. 13

⁶⁵ <https://twitter.com/RonWyden/status/1490715667468890112>

⁶⁶ <https://eshoo.house.gov/sites/eshoo.house.gov/files/LettertotheIRSonFacialRecognition2.4.22.pdf>

⁶⁷ <https://www.washingtonpost.com/opinions/2022/02/18/irs-facial-recognition-technology-safe/>

⁶⁸ https://www.markey.senate.gov/news/press-releases/senators-markey-and-merkle-and-reps-jayapal_pressley-urge-federal-agencies-to-end-use-of-clearview-ai-facial-recognition-technology

⁶⁹ <https://twitter.com/RonWyden/status/1493708084371415040>

⁷⁰ <https://www.whitehouse.gov/briefing-room/presidential-actions/2022/05/25/executive-order-on-advancing-effective-accountable-policing-and-criminal-justice-practices-to-enhance-public-trust-and-public-safety/>

では、「身体装着型カメラおよび高度な法執行技術の適切な使用を確保する。」とされ、身体装着カメラの利用ポリシーを策定するとともに、顔認識技術についても、本大統領令の公布日から180日以内に、司法長官は、全米科学アカデミー（NAS）に対し、その国家研究会議を通じて、以下の契約を締結するよう要請した。

(i) 顔認識技術、生体情報を用いる他の技術、および予測アルゴリズムについて、特に法執行機関による当該技術およびアルゴリズムの使用に焦点を当て、当該技術およびアルゴリズムの使用方法、ならびに当該技術およびアルゴリズムまたはその使用方法によって生じるプライバシー、市民権、自由、正確性、または格差の影響の評価を含む研究を実施し、また。(ii) 調査結果を詳述した報告書、および法執行機関による顔認識技術、生体情報を用いる他の技術、および予測アルゴリズムの使用または制限に関するあらゆる勧告を公表すること。

ここで得られた研究成果は、法執行機関（Law Enforcement Agencies: LEA）における実務に必要な変更を加えるために使用される。

●2022年6月29日、下院の科学・宇宙・技術委員会の行政調査及び監視小委員会(Subcommittee on Oversight and Investigations)は「生体計測技術（バイオメトリクス）時代のプライバシー」と題する公聴会を開催した⁷¹。証言を行ったのは次の3人であった。

- Ms. Candice Wright (GAO の Science, Technology Assessment, and Analytics 部門の Director)
- Dr. Charles H. Romine (NIST の Information Technology Laboratory の Director)
- Dr. Arun Ross (ミシガン州立大学コンピューターサイエンス学部の教授、NSF 識別技術研究センターの Site Director)

2.2 地方の動向

●メリーランド州では、コロナ禍において、労働関係のいくつかの法律が成立し、2020年10月1日に施行される。その中で、House Bill 1202 (Labor and Employment - Use of Facial Recognition Services - Prohibition)⁷²では、企業に対して、採用候補者 (Job candidates) をイ

⁷¹ <https://science.house.gov/hearings/privacy-in-the-age-of-biometrics>

⁷² <https://legiscan.com/MD/text/HB1202/2020>

ンタビューする際に同意なしに顔認識技術を用いることを禁じた⁷³。

●ニューヨーク市議会は2020年6月18日、「監視技術に関する公的な監視（Public Oversight of Surveillance Technology：POST）法」を可決した⁷⁴。NYPDによって使用される監視技術の公的な監視を可能にする。具体的には、警察に対して、監視技術の利用を説明する文書を公表し、パブリックコメントを受け、「監視の影響と利用ポリシー（“surveillance impact and use policy”）」を公表することを要求している。ニューヨーク市長のDe Blasio氏は7月16日、Black Lives Matter 関係のセレモニーの中で、POST法に署名した⁷⁵。

●NYCLU（ニューヨーク市民自由連合）は2020年6月22日、ニューヨーク州の教育省が、ロックポート市学区の顔認識セキュリティシステムを承認したことが、生徒のデータ保護法に違反しているとして提訴した⁷⁶。このセキュリティシステムは、ロックポート市学区が管理するデータベースに写真が保存されている一部の人物だけを識別することになっており、レベル2および3の性犯罪者、停職中の教師のような無許可の学校職員、その他、法執行機関が信頼できる脅威をもたらすと判断した成人の訪問者が含まれている⁷⁷。

●ボストン市議会は2020年6月24日、全会一致で、警察を含む市政府が顔認識技術を利用することを禁じる条例を可決した⁷⁸。条例名は「ボストンにおける顔監視（face surveillance）を禁止する条例」となった。もともとは「顔認識（facial recognition）」であった。顔監視の定義は「個人の顔の物理的特徴に基づき、個人の識別もしくは認証、または個人に関する情報の取得を支援する自動化または半自動化されたプロセス」とされている⁷⁹。

●ニューヨーク州議会は2020年7月22日、学校における生体認証技術の利用を2022年7月1日まで禁止するモラトリアム法案（A06787）を可決した⁸⁰。教育委員長（commissioner of

⁷³ <https://www.natlawreview.com/article/maryland-employers-get-ready-host-new-employment-laws>

⁷⁴ <https://epic.org/2020/06/new-york-city-passes-new-surve.html> 2017年3月に最初に提案された。

⁷⁵ <https://queenseagle.com/all/new-city-law-compels-nypd-to-explain-surveillance-tools-and-strategies>

⁷⁶ <https://news.wbfo.org/post/nyclu-suing-state-education-department-over-lockport-schools-facial-recognition-technology> 提訴の関連資料は <https://www.nyclu.org/en/cases/shultz-et-al-v-new-york-state-education-department>

⁷⁷ <https://www.wbfo.org/education/2020-06-24/facial-recognition-in-lockport-schools-best-technology-in-the-world-or-not-proven-to-work>

⁷⁸ <https://www.boston.com/news/local-news/2020/06/24/boston-face-recognition-technology-ban>

⁷⁹ <https://www.boston.gov/sites/default/files/file/2021/02/Boston-City-Council-face-surveillance-ban.pdf>

⁸⁰ <https://www.wgrz.com/article/news/education/new-york-state-pauses-use-of-facial-recognition-systems-in-schools/71-2bcf5d7d-c683-4679-932b-718f3538acab>

education) に対して、生体認証技術の利用に関する研究を実施し、学校における生体認証技術の利用を 2022 年 7 月 1 日まで（あるいは、委員長が購入や利用を認可するまで）禁止することを指示する。これを受けて NYCLU（ACLU のニューヨーク支部）は歓迎する旨の声明を出した⁸¹。

●2020 年 9 月 9 日、ポートランド市長と市議会は満場一致で 2 つの条例を可決した⁸²。1 つ目の条例は、市の組織が顔認識技術を利用したり入手したりすることを禁じるもので即日、施行された。もう 1 つは民間企業が公共空間において顔認識技術を利用することを禁じる条例で、2021 年 1 月 1 日に施行される予定である。民間企業の利用も禁止するものは初めてである。

●ニューヨーク州のクオモ知事は 2020 年 12 月 22 日、ニューヨーク州内の公立・私立の小中学校での顔認識技術を含む生体認識技術の購入や利用をいかなる目的であれ禁止する法案に署名した⁸³。禁止措置は少なくとも 2022 年 7 月まで続き、ニューヨーク州の教育省の研究が完了し、ガイドラインを整備するなどして、顔認識技術を学校において利用することが適切であることが見出せるまで続く。

●マサチューセッツ州で 2020 年 12 月 31 日、ベイカー知事が“An Act Relative to Justice, Equity and Accountability in Law Enforcement in the Commonwealth,”⁸⁴ という法律に署名した⁸⁵。法執行機関が顔認識検索を実施する際には、緊急時を除き、裁判所の命令を必須とすることを明記した。2021 年 7 月に施行される。

●アムネスティ・インターナショナルは 2021 年 6 月 3 日、ニューヨーク市における監視の状況に関する調査結果を発表した⁸⁶。ニューヨーク市警察（NYPD）が、顔認識技術を用いた 15,280 台の監視カメラによって人々が追跡する能力を持っていることを明らかにした。この調査には世界中から数千人のボランティアが参加し、マンハッタン（3,590 台）、ブルックリン（8,220 台）、ブロンクス（3,470 台）の交差点にある 15,280 台の監視カメラにタグが付けられ、この 3 区を

⁸¹ <https://www.nyclu.org/en/press-releases/nyclu-statement-facial-recognition-schools-moratorium>

⁸² <https://www.portland.gov/bps/news/2020/9/9/city-council-approves-ordinances-banning-use-facial-recognition-technologies-city>

⁸³ <https://www.forbes.com/sites/rachelsandler/2020/12/22/new-york-issues-first-in-nation-moratorium-on-facial-recognition-in-schools/?sh=6b42e732484b>

⁸⁴ <https://malegislature.gov/Bills/191/S2963>

⁸⁵ <https://www.mass.gov/news/governor-baker-signs-police-reform-legislation>

⁸⁶ <https://www.amnesty.org/en/latest/news/2021/06/scale-new-york-police-facial-recognition-revealed/>

合わせると、ニューヨーク市の交差点の約半分（47％）を占める。

●メイン州議会は2021年6月30日、公的機関による顔認識技術の利用を広範囲に禁止する法律⁸⁷を制定した。6月16日と17日にそれぞれ下院と上院において全会一致で承認されたため、ミルズ州知事の署名なしで成立した。10月1日に施行される。これまでで「全米で最も厳しい」と評価されている⁸⁸。州政府、郡政府、市政府のすべてのレベルにおいてこの技術の使用を禁止している。また、法執行機関が顔認識技術を使用できる例外的なケースを狭く限定している。

●ニューヨーク市では「生体識別子情報法（Biometric Identifier Information Law）」⁸⁹が2021年7月9日に施行された。顧客の生体識別子情報を収集、保持、変換、保管、共有する事業者は、その旨を、商業施設のすべての入口付近に、平易で簡単な言葉で、はっきりと目立つ標識を配置して開示することが義務付けられた。また、価値のあるものと引き換えに販売、貸出、取引、共有すること、またはその他の方法で生体識別子情報の取引から利益を得ることは違法とされた。

●ニューヨーク自由人権協会（New York Civil Liberties Union：NYCLU）が2020年6月に、ニューヨーク州教育省に対して、ロックポート市学区（Lockport City School District）が顔認識技術の付いたカメラによる監視システムを運用することを差し止めるよう求めた裁判で、2021年8月31日、判事は、2020年末に当時のクオモ知事が学校での顔認識技術の利用を一時的に停止（モラトリアム）させる州法に署名したことから、訴えの利益がなくなったとの判断をくだした⁹⁰。モラトリアムは州の教育省がプライバシー問題に関する研究を完了させるか、2022年7月1日の遅い方までとなっている。

●2022年1月18日、サンフランシスコ市のブリード（Breed）市長は、警察が監視カメラをリアルタイムでモニターできる状況を拡大するようサンフランシスコ市民に求める投票法案を提出したと報じられた⁹¹。投票は6月7日に予定されていた。1点目は、警察がライブ映像にアクセスできる「重要イベント（critical events）」のリストに、組織的な小売店窃盗、略奪、暴動などの特定の財産犯罪を追加することである。現行法では、市による監視技術の使用を制限する2019年の条例に基づいて、死亡または重傷の危険を伴う緊急事態のみが、監督委員会（Board of

⁸⁷ <http://www.mainelegislature.org/legis/bills/getPDF.asp?paper=HP1174&item=2&snum=130>

⁸⁸ <https://slate.com/technology/2021/07/maine-facial-recognition-government-use-law.html>

⁸⁹ <https://codelibrary.amlegal.com/codes/newyorkcity/latest/NYCAAdmin/0-0-0-42626>

⁹⁰ https://buffalonews.com/news/local/education/parents-lawsuit-over-lockport-facial-recognition-system-ends/article_4092d242-0cd2-11ec-8cf3-cf3c616d941f.html

⁹¹ <https://www.govtech.com/public-safety/sf-proposes-to-broaden-polices-use-of-surveillance-cameras>

Supervisors) の承認プロセスを回避できるとしている。2 点目は「治安危機エリア (public safety crisis areas) 」での警察カメラの使用を認めるものであり、市内に設置された民間の防犯カメラも含まれる。ところが、3 月 7 日、ブリード市長は、上記の投票法案を撤回し、代わりに、同様の目標を達成する他の方法について、監督委員会で対話を続けることを選択したと報じられた⁹²。

●テキサス州の司法長官は 2022 年 2 月 14 日、Meta 社 (旧 Facebook) が州内の住民の生体識別子を同意なしに 10 年に渡って違法に収集・商業化していたとして、「生体識別子の取得または使用に関する法律 (Capture or Use of Biometric Identifier Act : CUBI) 」と 3 つの州法に基づき、Meta 社を提訴したと発表した⁹³。Meta 社はすでに 2021 年 11 月に Facebook での当該機能を停止すると発表している。Capture or Use of Biometric Identifier Act はイリノイ州の BIPA と異なり、消費者に訴える権利を付与する私的権利は規定されていないが、司法長官に訴訟を起こす権限が与えられている。BIPA による集団訴訟が注目を集めやすいが、テキサス州での動きは、バイオメトリクスに関する法律を持たない州でも追及が可能であることを意味することになり、全米に広がっていく可能性がある⁹⁴。

2.3 大手テック系企業の動向

●2020 年 6 月、警察官によるジョージ・フロイド氏殺害により拡大した Black Lives Matter 運動を受けて、大手テック企業三社がそれぞれ警察への顔認識技術の提供を止めると発表した。まず、IBM は 6 月 8 日、自社ブログで、CEO である Arvind Krishna 氏が同日付で議会 (5 人の議員)宛てに出したレターを公表し、議会とともに進めるテーマとして三つの政策分野、すなわち警察改革、技術の責任ある利用、スキルと教育機会の拡大を挙げた⁹⁵。責任ある技術政策として、汎用の IBM 顔認識や解析ソフトウェア製品の提供を行わないとした。Amazon は 6 月 10 日、自社ブログにおいて、Amazon の顔認識技術 (製品名 Rekognition) の警察による利用に対して 1 年間の猶予期間 (モラトリアム) を実施することを発表した⁹⁶。対象は警察であり、他の用途で利用することは妨げないとした。議会が、顔認識技術の倫理的な利用を監督することのできる、

⁹² <https://www.sfchronicle.com/sf/article/S-F-police-surveillance-battle-Mayor-Breed-16972657.php>

⁹³ <https://www.reuters.com/technology/texas-sues-meta-over-facebooks-facial-recognition-practices-report-2022-02-14/>

⁹⁴ <https://news.bloomberglaw.com/privacy-and-data-security/metax-texas-facial-recognition-suit-shows-enforcement-headache>

⁹⁵ <https://www.ibm.com/policy/facial-recognition-sunset-racial-justice-reforms/>

⁹⁶ <https://www.aboutamazon.com/news/policy-news-views/we-are-implementing-a-one-year-moratorium-on-police-use-of-rekognition>

より強い規制を策定することを提唱してきており、このモラトリアム中に実現することを希望するとした。Microsoft の Smith 社長は 6 月 11 日、Washington Post Live において、人権が組み込まれた (“grounded in human rights”) 連邦法ができるまで、顔認識技術を米国内の警察部門には販売しないことを明言した⁹⁷。

●Amazon、Google の親会社である Alphabet、と Microsoft が、同意なしに顔写真を学習データとして利用したとして、イリノイ州の BIPA 違反として、2020 年 7 月 14 日に 2 人の市民 (Steven Vance 氏と Tim Janecyk 氏) によって提訴された⁹⁸。問題となっている顔写真は、IBM の Diversity in Faces データベースに含まれていたものである。このデータベースは、皮膚の色、性別、年齢などのバランスをとって正確性や公平性を担保したことが売りであった。

これに続き、同月、同データベースを顔認識技術の訓練用に利用した (その中にイリノイ州在住の人たちが含まれていて、BIPA で定められた本人の明示的な同意を得ていない) ことが BIPA (生体情報プライバシー法) 違反であるとして、集団訴訟 (クラスアクション) が提訴された⁹⁹。

●Amazon 社は 2021 年 5 月 18 日、2020 年 6 月に開始した、顔認識技術の警察利用に関するモラトリアムを継続することを発表した¹⁰⁰。

●米 Facebook と眼鏡大手の仏エシロール・ルクソティカは 2021 年 9 月 9 日、写真の撮影や音楽の再生などが可能な「スマートグラス」を米国などで発売した¹⁰¹。フレームに 500 万画素の小型カメラを 2 つ組み込み、マイクやスピーカー、操作のタッチセンサーも内蔵している。

●Meta 社 (Facebook 社が 10 月 28 日に社名を変更) は 2021 年 11 月 2 日、Facebook 上での顔認識システムの利用を中止することを発表した¹⁰²。顔認識にオプトインした利用者 (アクティブユーザの 3 分の 1 以上) も、写真や動画においてもはや自動的に認識されることはないという。また、10 億人以上の顔認識テンプレートを削除する予定であることも表明した。このため、

⁹⁷ https://www.washingtonpost.com/video/washington-post-live/microsoft-president-brad-smith-says-the-company-will-not-sell-its-facial-recognition-technology/2020/06/11/f6ccd46e-a8e6-42f5-82d2-61323f0368d0_video.html

⁹⁸ <https://www.cnet.com/news/amazon-google-and-microsoft-sued-over-photos-in-facial-recognition-database/>

⁹⁹ <https://www.cpomagazine.com/data-privacy/illinois-class-action-lawsuit-alleges-facial-recognition-databases-violate-biometric-privacy-law-could-cost-tech-giants-5000-per-incident/>

¹⁰⁰ <https://www.reuters.com/technology/exclusive-amazon-extends-moratorium-police-use-facial-recognition-software-2021-05-18/>

¹⁰¹ <https://www.nikkei.com/article/DGXZQOGN09F0Z0Z00C21A9000000/>

¹⁰² <https://about.fb.com/news/2021/11/update-on-use-of-face-recognition/>

目の不自由な人向けの技術である Automatic Alt Text (AAT) が使えなくなる。ただし、個人認証等の有用な用途はあるので顔認識技術の研究は社内で継続するとしている。また、最後に次のように結んでいる。「すべての新しい技術は、利益と懸念の両方をもたらす可能性があり、私たちはその適切なバランスを見つけないと思っています。顔認識の場合、社会における長期的な役割については、オープンな場で、最も影響を受ける人々の間で議論する必要があります。私たちは、この議論に参加し、この議論をリードしている市民社会団体や規制当局と協力していきます。」

Facebook における顔認識技術の利用の中止については 1 年前から、AI 部門のエンジニアや製品マネージャーらの小さなチームが議論を始めており、社内の様々な部門で顔認識技術を利用している同僚と議論した結果を、2021 年 6 月に、CTO らに、顔認識技術の利用中止の利害得失がまとめられた 50 ページの文書として示されたという¹⁰³。

●Microsoft 社は 2022 年 6 月 21 日、AI システムの構築方法を導くためのフレームワークである「責任ある AI 基準 (“Responsible AI Standard”）」を公開するとともに、顔認識技術に関して「既存顧客に対する移行期間を経て、これらのサービスへのアクセスを管理されたカスタマーとパートナーに限定し、ユースケースをあらかじめ定義された許容範囲に絞り込み、サービスに組み込まれた技術的コントロールを活用する予定」と表明した¹⁰⁴。さらに、感情認識機能については技術提供を原則行わないことも明らかにした。

「感情の状態を例にとると、人の顔をスキャンして、その表情や動作から感情の状態を推測するような技術には、オープンエンドの API アクセスを提供しないことにしている。社内外の専門家は、「感情」の定義に関する科学的コンセンサスの欠如、ユースケース、地域、人口統計にまたがる推論の一般化に関する課題、およびこの種の機能に関するプライバシー上の懸念の高まりを強調している。また、顔解析や他の AI 技術を用いたものであっても、人の感情の状態を推測することを目的としたすべての AI システムを慎重に分析する必要があると判断した。」

●Instagram は 2022 年 6 月 23 日、「インスタグラムが、ネット上で子どもの年齢を判定する新アイデアを発表」と題するブログにおいて、子どもの年齢を確認する方法として、自撮り動画から年齢を確認する技術も利用できるようになることが報告された¹⁰⁵。オンライン年齢認証を専門に行う Yoti 社と提携し、人々のプライバシーを保護するための取り組みも行っているという。

¹⁰³ <https://www.washingtonpost.com/technology/2021/11/05/facebook-facial-recognition/>

¹⁰⁴ <https://blogs.microsoft.com/on-the-issues/2022/06/21/microsofts-framework-for-building-ai-systems-responsibly/>

¹⁰⁵ <https://about.instagram.com/blog/announcements/new-ways-to-verify-age-on-instagram>

まず米国でテストが開始される。具体的には、誰かが Instagram で生年月日を 18 歳未満から 18 歳以上に編集しようとした場合、年齢を確認することが要求されるが、1) 身分証明書 (ID) をアップロードする、2) ビデオで自撮りする、3) 共通の友人に年齢を確認するよう頼む、という 3 つのオプションが利用可能となる。年齢推定を行ったのちは、画像は削除されるという。

このアイデアに対しては、もともと Instagram などのソーシャルメディアによる子どもたちへの害を懸念している議員らからは、子どもたちのプライバシーリスクの懸念の声が上がっている¹⁰⁶。Meta 社の広報担当者 Stephanie Otway 氏は声明の中で、この技術は「個人的に誰かを認識することはない」し、画像は年齢推定以外の目的には使用されないと述べた。Instagram は、13 歳未満の子どもを対象とした“Instagram Kids”体験を計画していたが、Blackburn 上院議員と Blumenthal 上院議員が率いる上院小委員会の公聴会に 2021 年 12 月に出席する前に、批判が高まったため開発を一時停止した。両氏は 2022 年 2 月に Kids Online Safety Act を提案した。

2.4 Clearview AI 社関連の動向

●2021 年 1 月 6 日に発生した、トランプ大統領の支持者らが国会議事堂を襲撃した事件をめぐって、米国の警察当局が Clearview AI 社の顔認識ソフトを用いて容疑者特定を行っていることが報じられた¹⁰⁷。Clearview AI 社の CEO である Hoan Ton-That 氏によると、事件の翌日には米国の法執行機関による利用が通常よりも 26% 増加したと言った。

●Clearview AI 社は 2021 年 8 月 18 日、法執行、政府、法律、金融サービス、国家安全保障などの分野で活躍する人物からなる諮問委員会 (Advisory Board) を設置したことを発表した¹⁰⁸。主なメンバーは、Raymond Kelly 氏 (元ニューヨーク市警察本部長)、Richard Clarke 氏 (元国家安全保障会議の高官)、Rudy Washington 氏 (元ニューヨーク市副市長) などである。

●Clearview AI 社は 2022 年 3 月 25 日、顔認識プラットフォームの最新版である Clearview 2.0 のリリースを発表した¹⁰⁹。200 億以上の一般公開された顔画像のデータベース、世界で最も正確な顔認識アルゴリズムの一つ、法執行機関の調査をより良くサポートするために設計されたコン

¹⁰⁶ <https://m.washingtontimes.com/news/2022/jun/24/instagram-testing-facial-scanning-tech-kids-verify/>

¹⁰⁷ <https://www.sankei.com/economy/news/210110/ecn2101100001-n1.html>
<https://www.nytimes.com/live/2021/01/09/us/trump-biden#facial-recognition-clearview-capitol>

¹⁰⁸ <https://www.verdict.co.uk/clearview-ai-facial-recognition-technology/>

¹⁰⁹ <https://www.clearview.ai/clearview-ai-releases-2-version-of-industry-leading-facial-recognition-platform-for-law-enforce>

プライアンスと管理ツールの強化などを特徴としている。2022年1月には、顔認識アルゴリズムについて米国特許を取得した¹¹⁰。また、最近の米国国立標準技術研究所（NIST）の顔認識ベンダーテスト（FRVT）ではすべてのカテゴリーで米国1位、世界トップ10にランクインしたという。

●Clearview AI社CEOはロイター通信からのインタビューにおいて、同社の顔認識ソフトウェアの販売を、主に警察向けから企業向けに拡大していると語った¹¹¹。その中で、学校向けに接客管理システムを販売する米企業とも契約していることを明らかにした。この発表は、テキサス州ユバルディの小学校で銃乱射事件が発生した5月24日とほぼ同時期に行われた。

●ACLU（アメリカ市民自由連合）らが2020年5月にClearview AI社がBIPAに違反しているとして起こした訴訟について、Clearview AI社は、2022年5月9日に裁判所に提出された法的和解案により、同社がBIPAを遵守することに同意した。和解の内容は以下のとおりである¹¹²。

- Clearview AI社は、その膨大な顔認識データベースへの有料・無料アクセスを、BIPAに含まれる狭い例外を除き、全国の民間団体（民間企業および個人を含む）に永久に禁止される。

- Clearview AI社は、イリノイ州の州政府または地方政府機関（法執行機関を含む）に対し、5年間、同社のデータベースへのアクセスを許可することを禁止される。つまり、イリノイ州内では、Clearview AI社はその間、政府契約者に対するBIPAの例外措置を利用することができない。

- Clearview AI社は、イリノイ州内の民間企業に対してデータベースへのアクセスを許可することを5年間禁止される。これは、クリアビューがBIPAの特定の種類のビジネスへの販売を許可する例外措置を、その期間中は利用できないことを意味する。

- Clearview AI社は、同社のウェブサイトにオプトアウト要求フォームを設置し、イリノイ州の住民が写真をアップロードしてフォームに記入すれば、Clearview AI社の法執行機関のユーザを含め、Clearview AI社の検索結果に自分の顔写真が表示されないようにする。同社はまた、オプトアウトの仕組みを宣伝するインターネット広告の費用として5万ドルを拠出する。Clearview AI社は、このオプトアウト・プロセスの一環としてアップロードされた写真を、オプトアウト・

¹¹⁰ <https://www.clearview.ai/press-release-clearview-ais-revolutionary-facial-recognition-platform-awarded-us-patent>

¹¹¹ <https://www.reuters.com/technology/clearview-ais-facial-recognition-tool-coming-apps-schools-2022-05-24/>

¹¹² <https://www.aclu.org/press-releases/big-win-settlement-ensures-clearview-ai-complies-with-groundbreaking-illinois>

プログラムの効果以外のいかなる目的にも使用することを禁じられる。

- Clearview AI 社は、雇用主に知られることなく、また雇用主の承認を得ることなく、個々の警察官に無料トライアルアカウントを提供するやり方を廃止する。

- 今後 5 年間、Clearview AI 社は、イリノイ州で撮影された、またはイリノイ州からアップロードされた写真を除外するための現在の措置を継続する。

2.5 その他の動向

●2020 年 4 月 14 日、World Privacy Forum が、米国の学校における生徒の個人データの取扱いを扱った報告書「同意なしで：米国の学校における生徒の directory information の実態とプライバシーへの影響」を公表した¹¹³。この中で、生徒の生体データの問題も取り上げられた。米国では「家族教育権とプライバシー法（Family Educational Rights and Privacy Act：FERPA）」が 1974 年に策定され、子供の教育記録に関して保護者が一定の権利が確保されている。しかし、同法には、“directory information”¹¹⁴については、保護者や生徒の事前同意なしに公表することができるという免除規定がある。これらはオプトアウトの権利により保護されているにもかかわらず、そのことが学校のウェブサイト等に分かりやすく掲載されていないなど、十分に活用されていないことが分かった。また、“directory information”がデータブローカーに渡るケースも見られた。また、顔認識アルゴリズムのための教師データとして学校サイトから子供の顔画像をスクレイプしている例が見られた。勧告の 1 つは、顔認識技術や生体認証システムの教師データとして、事前同意なしに生徒の写真を利用することを禁止し、イヤーブックの製作者は情報を販売したり共有したりせず、顔認識の利用にはそれに特化した同意を必要とするべきであるとした。

●2020 年 5 月初旬に、ペンシルベニアの Harrisburg 大学の研究グループが、個人レベルで犯罪行動に向かいやすいかどうかを 80%の精度で予測できる自動顔認識ソフトウェアを開発したとするプレスリリース¹¹⁵を公表し、研究成果はシリーズ本に収録される予定であった¹¹⁶。しかし、技術的な事項に加え、人を見ただ目で犯罪者扱いするという点に倫理面からの批判が殺到し¹¹⁷、大

¹¹³ <https://www.worldprivacyforum.org/2020/04/without-consent/>

¹¹⁴ これには、生徒氏名、住所、写真、ジェンダー、保護者の住所、生年月日、出生地、など広範な情報が含まれる。

¹¹⁵ <http://archive.is/N1HVe>（アーカイブ化されている）

¹¹⁶ <https://www.biometricupdate.com/202005/biometric-software-that-allegedly-predicts-criminals-based-on-their-face-sparks-industry-controversy>

¹¹⁷ <https://www.linkedin.com/feed/update/urn:li:activity:6663620384715227136/>

学は、本人たちの要求によるという形で、先のプレスリリースを削除し、出版もとりやめることをアナウンスした。これを機に、研究者らが Coalition for Critical Technology のもとに集結し、6月22日付で、Springer社の編集委員会にレター¹¹⁸を書き、犯罪行動を予測できるとするすべての研究の公表を延期するように依頼した¹¹⁹。

●[報告書]2020年5月29日付で、Erik Learned-Miller氏（マサチューセッツ大学アマースト校）らは報告書「野に放たれた顔認識技術：連邦機関の設置を要求する」を公表した¹²⁰。FDA（食品医薬品局）が医薬品や医療機器を規制するように、顔認識技術を監督する連邦規制機関を設置することを提案した。顔認識技術の製造業者は、意図する利用が安全で効果的であることを自ら示す必要があり、専門家パネルが技術そのものとともに、社会的リスクを検討したうえで、承認するかしないかの判断を下すことになる。

●2020年6月24日付のNew York Times紙は、“Wrongfully Accused by an Algorithm”と題する記事を掲載し、顔認識技術を利用したマッチングによる「初の」誤認逮捕の事例として、ミシガン州デトロイトの男性、Robert Julian-Borchak Williams氏のケースを取り上げた記事を掲載した¹²¹。内容は次のとおりである。2020年1月9日、職場にデトロイト警察から出頭要請の電話がかかってきた。1時間後に帰宅すると、警察車両が制止し、妻と2人の幼い娘の前で手錠をかけられ、収容所に連行された。マグショット、指紋、DNAを採取され、一晩過ごし、翌日の昼、取調室につれて行かれ、テーブルには3部の書類が置かれていた。盗難事件が起きたのは2018年10月。監視カメラの画像がミシガン州警察に送られ、4900万枚の写真との照合が行われた。ミシガン州ではDataWorks Plusという会社がマグショットの管理システムを受託していたが、2005年から外部ベンダーの開発した顔認識ツールを加えた。しかし「科学的な」検証がされないままだったという。Williams氏の運転免許証の写真もデータベースに含まれており、マッチした写真のうちの1つとして、“Investigative Lead Report”としてデトロイト警察に送られた（あくまでもleadであると注意書きまであった）。デトロイト市は、公式な顔認識技術ポリシーを2019年7月変更している¹²²。6月24日、ミシガン州のA.C.L.U.は、本ケースの完全な却

¹¹⁸ <https://medium.com/@CoalitionForCriticalTechnology/abolish-the-techtoprisonpipeline-9b5b14366b16>

¹¹⁹ <https://www.biometricupdate.com/202006/scientists-sociologists-speak-out-against-biometrics-research-that-allegedly-predicts-criminals>

¹²⁰ https://global-uploads.webflow.com/5e027ca188c99e3515b404b7/5ed1145952bc185203f3d009_FRTsFederalOfficeMay2020.pdf

¹²¹ <https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html>

¹²² <https://detroitmi.gov/sites/detroitmi.localhost/files/2019->

下、謝罪と Williams 氏の情報をデトロイトの犯罪データベースからの削除を求めて、市に申し立てを行った¹²³。

● [報告書] ミネソタ大学ロースクールの人権センター (Human Rights Center) の Krisztina Huszti-Orbán 博士と Fionnuala Ni Aoláin 教授が 2020 年 7 月、報告書「テロリストを特定するための生体計測データの利用：ベストプラクティスかリスクビジネスか？」を公表した¹²⁴。テロに対抗する際の人権および基本的自由の促進と保護に関する国連特別報告者の委任に基づいて作成された。

● [報告書] ミシガン大学公共政策大学院の科学、技術及び公共政策 (STPP) に 2019 年秋に開始されたテクノロジーアセスメント・プロジェクト (TAP) は、報告書「教室の中のカメラ：学校の中の顔認識技術 (Cameras in the Classroom: Facial Recognition Technology in Schools)」を公表した¹²⁵。顔認識技術について、人種差別を悪化させること、国家による監視を日常化させること、校則を遵守しない生徒を罰することになること、企業が子供のデータから利益を上げること、正確でないことを挙げ、国レベルで 4 点 (国レベルで顔認識技術の利用にモラトリアムを設けることなど)、州レベルで 2 点、学校区レベルで 9 点の勧告を行った

● 新型コロナウイルス感染症の感染拡大により、米国では司法試験が ExamSoft 社のシステムを使ってリモートでの実施が予定されていたが、有色人種の間で「明るさが足りない」という理由で顔認証がうまくなされないという問題が指摘されている¹²⁶。また、生体認証データの保持期間も明らかにされておらず、セキュリティ面での課題も指摘されている。

● マイアミ大学の学生らは、マイアミ大学警察 (UMPD) が、大学のコロナウイルス対策への抗議活動を行っている学生の特定のために顔認識技術を利用したと批判しているが、当局は否定しているという¹²⁷。2020 年 10 月下旬、抗議する学生たちは、顔認識技術を禁止するよう求める公開書簡を学校に提出した。この手紙には、20 以上のプライバシー擁護団体や市民的自由を求め

07/FACIAL%20RECOGNITION%20Directive%20307.5_0.pdf

¹²³ <https://www.aclu.org/letter/aclu-michigan-complaint-re-use-facial-recognition>

¹²⁴ <https://www.law.umn.edu/human-rights-center/research/use-biometric-data-identify-terrorists>

¹²⁵ <https://stpp.fordschool.umich.edu/research/research-report/cameras-classroom-facial-recognition-technology-schoolst>

¹²⁶ <https://venturebeat.com/business/examsofts-remote-bar-exam-sparks-privacy-and-facial-recognition-concerns/> 日本語記事は <https://gigazine.net/news/20201005-remote-recognition-concern-racism/>

¹²⁷ <https://www.campussafetymagazine.com/university/u-mami-facial-recognition/>

る団体が署名した。

●CNN は 2021 年 5 月 4 日、顔認識検索エンジンである PimEyes を取り上げたニュース記事を配信した¹²⁸。PimEyes は、自分の顔写真をアップロードするとオンライン上にある自分の写真を見つけてくれる検索サイトである。無料でも検索できるが、一部だけ、またモザイクがかかった形で提示され、完全な検索結果を見るには個人では月 29.99 ドルからの有料サービスに登録する必要がある。また同一人物の写真がインターネットに掲載されると警告を知らせるサービスもある。PimEyes の検索結果から削除してもらうことも有料で請け負っている。ワシントンポスト紙も 5 月 14 日の記事「この顔認識ウェブサイトは誰でも警察、またはストーカーになれる」で PimEyes を取り上げた¹²⁹。PimEyes は 2017 年に立ち上げられたポーランドのスタートアップで、Wroclaw 科学技術大学の 2 人の卒業生によって開始されたという。2020 年に PimEyes ブランドは セーシェル諸島に登録された“Face Recognition Solutions Ltd.”という会社に移ったが、匿名を保っている。

●米国各州で、ID.me という個人識別サービスに使われている顔認識技術の不具合によって失業給付を拒否される事例がしばらく前から相次いでいることが 2021 年 6 月報じられた¹³⁰。顔認識技術はもともと不正受給を防止するために採用されている。

●多くの NPO が集まり、小売り業者による店内での顔認識技術の利用をやめるように求めるキャンペーンが開始された¹³¹。ウォルマートなどの米国内の主要な小売業者を、それぞれ「使用するつもりがない」「使用するかもしれない」「実際に私用している」と色分けしている。

●デルタ航空は 2021 年 10 月 27 日、デルタ航空のマイレージプログラムの会員で、運輸保安庁 (TSA) のプリチェック (PreCheck) に登録している利用客を対象に、アトランタ空港で、顔認識技術を利用したサービスを開始した¹³²。乗客は、手荷物の預け入れから保安検査、そして搭乗まで、顔を示すだけで可能になる。手荷物の預け入れまで含めた点が新しい。利用を望まない人は利用する必要がなく、現在はオプトインで実施されているという。

¹²⁸ <https://edition.cnn.com/2021/05/04/tech/pimeyes-facial-recognition/index.html>

¹²⁹ <https://www.washingtonpost.com/technology/2021/05/14/pimeyes-facial-recognition-search-secrecy/>

¹³⁰ <https://www.vice.com/en/article/5dbywn/facial-recognition-failures-are-locking-people-out-of-unemployment-systems> 1

¹³¹ <https://www.banfacialrecognition.com/stores/>

¹³² <https://techcrunch.com/2021/10/27/delta-air-lines-partners-with-tsa-precheck-to-launch-biometrics-based-bag-drops/>

●Intercept は 2022 年 7 月 16 日、オンライン顔認識検索エンジン PimEyes について、子どもの画像検察について、現在のオーナーである Gobronidze 氏との 2 時間のオンラインインタビューの結果を交えて報じている¹³³。PimEyes を使うと、虐待を行った親が避難所に逃げた子どもの画像を検索したり、政府が反体制者の子どもをターゲットにしたり、小児性愛者が違法な児童性的虐待画像に出てきた被害者をストーキングしたりすることが可能である。逆に、いくつかの児童擁護団体は、人身売買対策として、警察が顔認識技術を使って被害者の居場所を特定することができると主張している。

また、Gobronidze 氏は、Safer というツールを使って、画像ハッシュ化技術により児童の性的虐待画像を検出することについて、PimEyes が Thorn 社と会話を行ったと言った。児童虐待防止 NPO である Thorn 社は、Ashton Kutcher と Demi Moore が設立し¹³⁴、Spotlight と呼ばれる顔認識ツールを開発し、性犯罪の捜査を行う捜査官や、全米行方不明・被搾取児童センター (National Center for Missing and Exploited Children) に提供している。全米 50 州とカナダの警察官に利用され、ウェブベースのツールは、過去 4 年間で 17,092 人の人身売買の被害児童の発見に役立ったという¹³⁵。Spotlight を使用することで、法執行機関は 1 日平均 9 人の子供を特定しているという。

3. 英国の動向

3.1 政府関係の動向

●Innovate UK と交通省 (Department of Transport) が実施した顔認識技術に関する公募で、UK ベースのバイオメトリクス企業 iProov 社が受託し、ユーロスターのロンドンからの乗客に対して、2021 年 3 月までに顔認識技術を用いたコンタクトレスの乗車システムの運用が開始される予定である¹³⁶。2020 年 6 月 17 日付で、iProov 社はプレスリリースを出している¹³⁷。

●2020 年 6 月 25 日、監視カメラコミッショナーから、2018～2019 年の年次報告書が公表され

¹³³ <https://theintercept.com/2022/07/16/facial-recognition-search-children-photos-privacy-pimeyes/>

¹³⁴ <https://www.thorn.org/>

¹³⁵ <https://www.thorn.org/spotlight/>

¹³⁶ <https://www.standard.co.uk/lifestyle/travel/travel-news/eurostar-face-scan-technology-a4472636.html>

¹³⁷ <https://www.businesswire.com/news/home/20200617005228/en/%C2%A0iProov-Provide-Contactless-Travel-Entry-Eurostar-Part>

た¹³⁸。6回目の報告にあたる。

●2020年3月19日に内務大臣（Home Secretary）に提出された、生体認証コミッショナー（Commissioner for the Retention and Use of Biometric Material）による2019年報告書が、7月2日に公表された¹³⁹。7月6日付で、本報告書に対する政府の回答も公表された¹⁴⁰。報告書で指摘された、新しい生体認証技術の警察利用に関するガバナンスの改善と立法措置の必要性について、また、警察による新しい生体認証技術の試行やデータ解析を増やすことについて、内務大臣は賛同した。

●英国の情報コミッショナー局（ICO）は、オーストラリアの情報コミッショナー（OAIC）とともに、Clearview社の個人情報の取り扱いについての共同捜査を開始したことを2020年7月9日、発表した¹⁴¹。

●監視カメラコミッショナーは2020年7月10日、監視カメラ行動規範（Code of Practice）¹⁴²への遵守を第三者機関が認証する仕組みについての、第三者認証指針を公表した¹⁴³。UKAS（英国認証機関認定審議会）が認証した3つの認証機関が二段階の認証プロセスを策定した。本指針はこのためのプロセスを説明したものである。

●Biometrics and Forensics Ethics Group (BFEG)は、2018年に公表した倫理原則を2020年12月22日、更新した¹⁴⁴。生体認識や法科学の適用プロセスにおいて差別を防ぐことを強調するために、原則2の“procedures should be used to advance justice”を“procedures should seek to respect the dignity of individuals and groups.”とした。原則3の“procedures should respect the human rights of individuals and groups,”も平等法（Equality Act）に明示的に言及し大きく変更された。原則4の“procedures should respect the dignity of all individuals”は、人権法（Human Rights Act）に明示的に言及する形で大きく変更された。以前の原則5にあった、“respect

¹³⁸ <https://www.gov.uk/government/publications/surveillance-camera-commissioner-annual-report-2018-to-2019>

¹³⁹ <https://www.gov.uk/government/publications/biometrics-commissioner-annual-report-2019>

¹⁴⁰ <https://www.gov.uk/government/publications/response-to-the-biometrics-commissioners-annual-report-2019>

¹⁴¹ https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/07/oaic-and-ico-open-joint-investigation-into-clearview-ai-inc/?utm_source=twitter&utm_medium=iconews&utm_term=7e9b390a-a756-4aa2-a07c-1f1a43f986b6&utm_content=&utm_campaign=

¹⁴² <https://www.gov.uk/government/publications/surveillance-camera-code-of-practice>

¹⁴³ <https://www.gov.uk/government/publications/surveillance-camera-code-of-practice-third-party-certification-scheme>

¹⁴⁴ <https://www.gov.uk/government/publications/ethical-principles-biometrics-and-forensics-ethics-group>

for private and family life”が原則 4 に移行された¹⁴⁵。6 原則は次の通りとなった。

原則 1：手続きは、公共の安全と公共の利益を高めるものでなければならない。

原則 2：手続きは、個人及び集団の尊厳を尊重するよう努めなければならない。

原則 3：手続きは、2010 年平等法で定義された「保護された特性（‘protected characteristics’）」（年齢、障害、性別変更、結婚または市民パートナーシップ、妊娠・出産、人種、宗教または信念、性別、性的指向）に基づき、最も脆弱な人々またはグループを意図的または不注意に標的としたり選択的に不利にしたりすべきではない。

原則 4：手続きは、1998 年人権法で定義された人権を差別することなく尊重しなければならない。私生活や家族生活を尊重する権利、表現の自由の権利など、絶対的でない権利の制限は、合法的な目的のため、比例的かつ必要なものでなければならない。

原則 5：科学技術の発展は、刑事司法のプロセスを促進し、無実の者の迅速な免責を促進し、被害者の保護と解決を可能にするために利用されるべきである。

原則 6：手続きは、確固たるエビデンスに基づくべきである。

また、Biometrics and Forensics Ethics Group (BFEG)は、ライブでの顔認識技術（LFR）を公的機関と民間組織が共同で利用することの倫理的課題を調査することを委託され、作業グループを作って様々な主体からエビデンスを収集し、その結果を 2021 年 1 月 21 日、Briefing Note として発表した¹⁴⁶。店舗やショッピングセンターといった誰でもアクセス可能な私的空間における LFR の使用に焦点をあてたものである。報告書では、データの共有、ウォッチリストの構築、第三者による監督など、7 点の勧告が示された。

1. 警察は、審査に合格した信頼できる組織としかデータを共有すべきではない。
2. データは必要最小限の人数と共有し、また必要最小限の人数によってアクセスされるべきである。

¹⁴⁵ <https://www.biometricupdate.com/202012/uk-biometrics-and-forensics-ethics-group-updates-principles-to-emphasize-rights-and-non-discrimination>

¹⁴⁶ <https://www.gov.uk/government/publications/public-private-use-of-live-facial-recognition-technology-ethical-issues/briefing-note-on-the-ethical-issues-arising-from-public-private-collaboration-in-the-use-of-live-facial-recognition-technology-accessible>

3. バイオメトリクスデータ（画像データを含む）は、安全かつセキュアに保管されなければならない。
4. ウォッチリストは対象を絞ったものでなければならない。
5. LFR の共同利用についての誰でもアクセス可能な記録が作成されなければならない。
6. LFR の共同利用は、巡査長（senior police officer）によって承認されるべきである。
7. 独立した倫理グループが、警察による、公民協働における LFR の利用を監督する必要がある。

●内務省大臣は、2021年3月1日付けで Fraser Sampson 氏を「バイオメトリクス及び監視カメラコミッショナー（Biometrics and Surveillance Camera Commissioner）」に任命した¹⁴⁷。Protection of Freedoms Act 2012 によって創設された2つのポストである「バイオメトリクス・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）」のポストを統合して作られた新しいポストである。3月18日には公式ブログにおいて、Sampson 氏が自己紹介を行った¹⁴⁸。

●政府は2021年3月9日付で、2019年7月に公表されていた、下院科学技術委員会による、バイオメトリクス・コミッショナーと法科学レギュレーターの仕事に関する報告書¹⁴⁹に対する回答書を委員会議長宛に送付した。バイオメトリクス（生体計測）については、ライブでの顔認識技術の利用について、政府としてはモラトリアムや禁止といった提案には同意しないとした。また、偽陽性の懸念についても最終判断は人が行うのだから問題ないことが強調された。

●Biometrics and Forensics Ethics Group (BFEG)は、2021年3月18日、2019年の年次報告書を公表した¹⁵⁰。3度目の年次報告書で、対象期間は2019年4月から2020年4月である。3月19日には、2021年3月で任期に達した7名のメンバー（6名が大学教授、1名がIBMの研究

¹⁴⁷ <https://www.gov.uk/government/news/new-biometrics-and-surveillance-camera-commissioner-appointed>

¹⁴⁸ <https://videosurveillance.blog.gov.uk/2021/03/18/appointment-of-professor-fraser-sampson-the-new-biometrics-and-surveillance-camera-commissioner/>

¹⁴⁹ <https://publications.parliament.uk/pa/cm201719/cmselect/cmsctech/1970/1970.pdf>

¹⁵⁰ <https://www.gov.uk/government/publications/biometrics-and-forensics-ethics-group-annual-report-2019>

者) 全員が二期目 (3年間) に再任されたことがアナウンスされた¹⁵¹。

●2021年6月18日、情報コミッショナーである Denham 氏は「公的空間におけるライブ顔認識技術の利用」に関する意見を発表した¹⁵²。

●下院 (House of Lords) の司法・内務委員会 (Justice and Home Affairs Committee) は、「新規技術と法の適用 (New technologies and the application of the law)」に関する調査を開始した¹⁵³。2021年6月より公開及び非公開の公聴会を開催するとともに、9月5日締め切りとして Call for Evidence (書面でのコメント募集) を7月22日開始した。募集するエビデンスとしては下記のようなものが例示された。

・法執行のために使用される新規技術は、何を達成することを目的とすべきであり、どのような場合にそれらを使用することが許容されるか？

・法執行の文脈で使用される高度なアルゴリズムは、信頼できる出力を生成するか？それは首尾一貫しているか？これらの技術を利用する人々 (警察官、司法のメンバー、弁護士、一般の人々など) は、技術がどのように機能し、どのように使用されるべきかをどの程度理解しているか？

・新規技術の展開を監視するには、どのようなメカニズムを導入する必要がありますか？新規技術の使用について誰が垂カウンタブルであるべきであり、どのようなアカウンタビリティの取り決めを実施する必要があるか？

・これらの技術の使用に関して、購入方法、結果の解釈方法、使用方法など、透明性をどのように確保できるか？

これらの結果、司法・内務委員会は2022年3月、報告書「テクノロジーが支配する？司法制度における新規技術の出現」を公表した¹⁵⁴。司法の文脈で用いられる新規技術の代表的な例として顔認識技術が挙げられている。

¹⁵¹ <https://www.gov.uk/government/news/biometrics-and-forensics-ethics-group-reappoints-seven-members>

¹⁵² <https://ico.org.uk/about-the-ico/media-centre/information-commissioner-s-opinion-addresses-privacy-concerns-on-the-use-of-live-facial-recognition-technology-in-public-places/>

¹⁵³ <https://committees.parliament.uk/work/1272/new-technologies-for-law-enforcement/>

¹⁵⁴ <https://committees.parliament.uk/work/1272/new-technologies-and-the-application-of-the-law/news/165183/technology-used-in-the-justice-system-is-outpacing-scrutiny-and-regulation/>

●2021年5月半ばに導入された NHS（国民保健サービス）の Covid pass アプリ¹⁵⁵は、ワクチン接種や検査・回復の状況を証明するアプリであり、デフォルトで顔認証（オプトアウト可能）を求める場合があり、その際に iProov 社に送付され、マッチングが行われていることを、9月15日付の Guardian が報じた¹⁵⁶。データ自体はセキュアな管理がされているというものの、NHS と iProov 社との契約は（セキュリティ上の理由で）公表されず、アプリのデータ保護影響評価(DPIA)も公表されていないという。

●英国で 2013 年に導入された「監視カメラ行動規範 (Surveillance camera code of practice)」の初めての改訂版が、2021年8月13日から9月8日までパブリックコンサルテーションにかけられた¹⁵⁷。2020年9月にサウスウェールズ警察によるライブ顔認識の利用を違法だとした判決を受けた修正などがなされているが、さっそく批判を浴びている¹⁵⁸。改訂版の行動規範は 11月16日に議会に提示され、2022年1月12日に施行された¹⁵⁹。監視カメラシステムの運用者に推奨される 12 の指針は以下のとおりである。

1. 監視カメラシステムの使用は、常に、正当な目的を追求し、特定された緊急の必要性を満たすために必要な特定の目的のために行われなければならない。
2. 監視カメラシステムの使用者は、個人とそのプライバシーへの影響を考慮し、その使用が正当であることを確認するために定期的に見直さなければならない。
3. 監視カメラシステムの使用にあたっては、情報へのアクセスや苦情のための連絡先を公表するなど、可能な限り透明性を確保しなければならない。
4. 収集、保有、使用される画像や情報を含むすべての監視カメラシステムの活動に対して、明確な責任 (responsibility) とアカウントビリティ (accountability) がなければならない。
5. 監視カメラシステムを使用する前に、明確なルール、方針、手順を定め、それらを遵守する必要のあるすべての人に周知しなければならない。
6. 監視カメラシステムの目的に照らして厳密に必要な枚数以上の画像や情報を保存すべきではなく、目的が達成され

¹⁵⁵ <https://www.nhs.uk/conditions/coronavirus-covid-19/covid-pass/>

¹⁵⁶ <https://www.theguardian.com/society/2021/sep/15/nhs-app-storing-facial-verification-data-via-contract-with-firm-linked-to-tory-donors>

¹⁵⁷ <https://www.gov.uk/government/consultations/surveillance-camera-code-of-practice>

¹⁵⁸ <https://www.bbc.com/news/technology-58206586>

¹⁵⁹ <https://www.gov.uk/government/publications/update-to-surveillance-camera-code>

た時点でそのような画像や情報は削除されなければならない。

7. 保持された画像及び情報へのアクセスは制限されるべきであり、アクセスできる者及びアクセスの目的について明確に規定されなければならない。画像及び情報の開示は、当該目的又は法執行のために必要な場合にのみ行われなければならない。
8. 監視カメラシステムの運用者は、システム及びその目的に関連して、すべての承認された運用、技術及び能力の基準を考慮し、これらの基準を満たし維持するよう努力しなければならない。
9. 監視カメラシステムの画像及び情報は、不正アクセス及び不正使用から保護するために適切なセキュリティ対策の対象となるべきである。
10. 法的要求事項、方針、基準が実際に遵守されていることを確認するために、効果的な審査と監査の仕組みがあり、定期的に報告書が発行されること。
11. 監視カメラシステムの使用が正当な目的の追求であり、その使用に対する緊急の必要性がある場合、証拠価値のある画像や情報を処理する目的で、公共の安全と法執行を支援するために最も効果的な方法で使用されなければならない。
12. 照合目的のために参照する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情報は、正確で常に最新のものに更新されるべきである。

●英国情報コミッショナー局（ICO）とオーストラリア情報コミッショナー局（OAIC）は、2020年7月に開始した Cleaview AI 社への合同調査を終了したと 2021 年 11 月 3 日、発表した¹⁶⁰。OAIC も文書を発表し、オーストラリアのプライバシー原則（APP）の要件を満たしておらず、オーストラリア人のプライバシーを侵害していると指摘し、ウェブサイトからのオーストラリア人の写真の収集を中止し、すでに収集された写真は 90 日以内にすべて破棄し、書面での確認を提出することを求めた¹⁶¹。ICO は 11 月 29 日、Clearview AI 社に対して、英国のデータ保護法に違反しているとして、£ 1700 万を超える罰金を課す予備的な意図を公表した¹⁶²。

¹⁶⁰ <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2021/11/clearview-statement/>

¹⁶¹ https://www.oaic.gov.au/_data/assets/pdf_file/0016/11284/Commissioner-initiated-investigation-into-Cleaview-AI,-Inc.-Privacy-2021-AICmr-54-14-October-2021.pdf

¹⁶² <https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2021/11/ico-issues-provisional-view-to-fine-clearview-ai-inc-over-17-million/>

●英国 ICO は 2022 年 5 月 23 日、Cleaview AI 社に対して、顔認識用のグローバル・オンライン・データベースを作成するためにウェブやソーシャルメディアから英国人の顔写真を収集し、利用したことに対して、£ 7,552,800 の罰金を科したことを公表した¹⁶³。また、同社に対して、インターネットから得られる、英国在住者の個人データを取得し、利用することをやめ、システムからデータを削除することを命じた、執行通知を発令した。

●2022 年 7 月 4 日、党派を超えた 67 名の国会議員が、英国における Hikvision と Dahua の監視機器の販売と使用を禁止するよう政府に求めた¹⁶⁴。さらに「英国における CCTV の規模、能力、倫理、権利の影響に関する独立した国家的なレビュー」を要求した。この動きは、Big Brother Watch による 2022 年 2 月公開の調査報告書¹⁶⁵において、英国中の多くの公共機関が両社製の CCTV カメラを使っていることが示唆されたことに基づいている。

●英国 ICO は 2022 年 10 月 26 日、新たなバイオメトリクス技術の利用を進める企業を支援するために 2 つの報告書を公表した¹⁶⁶。1 つは Biometrics insight report (インサイト報告書) で、もう 1 つは Biometrics foresight report (フォーサイト報告書) である。前者はバイオメトリクスの定義や法的基盤などが整理されたものであるのに対して、後者はバイオメトリクスの将来のシナリオや課題が挙げられた。金融や商業、フィットネスや健康、雇用、教育、エンターテインメントといったセクターごとに、2~3 年後 (短期)、4~5 年後 (中期)、5~7 年後 (長期) の利活用の見込みが検討された。そしてバイオメトリクスの将来の課題として、次の 4 点が挙げられた。

1 つ目は、用語の明確化とガイダンスの作成が必要となることである。

2 つ目は、分類目的でのバイオメトリクス技術の利用が増加することである。

3 つ目は、公的空間でデータを処理する際の透明性と適法性の要件への準拠の問題である (非接触で気づかれないうちにデータが取得される可能性がある)。

¹⁶³ <https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/05/ico-fines-facial-recognition-database-company-clearview-ai-inc/>

¹⁶⁴ <https://bigbrotherwatch.org.uk/2022/07/mps-call-on-government-to-ban-chinese-cctv-in-the-uk/>

¹⁶⁵ https://bigbrotherwatch.org.uk/wp-content/uploads/2022/02/Whos-Watching-You_The-dominance-of-Chinese-state-owned-CCTV-in-the-UK-17746.pdf

¹⁶⁶ <https://ico.org.uk/about-the-ico/research-and-reports/biometrics-technologies/>

4つ目は、感情AIが、高リスクなバイOMETリック技術であると考えられているにも関わらず、急速に発展していることである。

3.2 警察関係の動向

●2019年に控訴院 (High Court) でサウスウェールズ警察の自動顔認識技術 (AFR) の利用が合法であるとの判決が出たが、11月に控訴することが認められ、NPOである Liberty と Ed Bridges氏が控訴した控訴審が開始され、2020年6月23日から3日間公聴会が開催された¹⁶⁷。Liberty側の弁護士は、人種差別的であり、データ保護法にも違反していると主張した。警察側は、初期平等影響評価 (equality impact assessment) を実施したが、完全平等影響評価は必要ないと判断したと主張した¹⁶⁸。裁判において、サウスウェールズ警察側の証人として発言した、Northgate Public Services社の顔認識担当の Paul Roberts氏は、学習用顔データの出所を、インターネット上からかき集めたものでなく、バイアスの存在を否定したが、詳細は語らなかったと報道された¹⁶⁹。

●控訴院 (Court of Appeal) は2020年8月11日、NPOである Liberty と Ed Bridges氏による控訴を受けて、3人の判事は満場一致で、サウスウェールズ警察による自動顔認識 (AFR) 技術の利用 (2017年12月と2018年3月の2回) は、欧州人権条約 (ECHR)のもとでのプライバシー権 (論点1)、データ保護法 (論点3)、及び、人種差別や性差別への懸念に対処する義務 (論点5) に違反しているとする判決をくださった¹⁷⁰。原告が挙げた5つの論点のうち3つ (論点、1、3、5) を裁判所は支持した。すなわち、自動化顔認識 (AFR) Locate がどこで利用され、ウォッチリストに誰が含まれるべきかに関する明確な指針が存在しないこと、データ保護影響評価 (DPIA) に欠陥があること、及び、ソフトウェアが人種と性別のバイアスを持つかどうか調査するための責任ある取り組み (Public Sector Equality Duty) を行っていないこと、である。この判決に対して、監視カメラコミッショナーの Tony Porter氏は同日、コメントをウェブサイトに掲載し¹⁷¹、これまでと同様、内務省 (Home Office) に対して、監視カメラ行動規範 (Surveillance

¹⁶⁷ <https://www.theguardian.com/technology/2020/jun/23/uks-facial-recognition-technology-breaches-privacy-rights>

¹⁶⁸ <https://www.bbc.com/news/uk-wales-53166044>

¹⁶⁹ https://www.theregister.com/2020/06/30/nec_neoface_watch_afr_locate_details_liberty/

¹⁷⁰ 判決文は、<https://www.judiciary.uk/judgments/r-bridges-v-cc-south-wales/>

報道は例えば、<https://www.independent.co.uk/news/uk/home-news/facial-recognition-unlawful-violation-human-rights-court-of-appeal-a9664441.html> Bridges氏はクラウドファンディングを利用して£9000の裁判費用を調達した。

¹⁷¹ <https://www.gov.uk/government/speeches/surveillance-camera-commissioners-statement-court-of->

Camera Code of Practice) の更新を訴えた。

●ロンドン警視庁 (MPS) による、事後的な (遡及的な) 顔認識システム (retrospective facial recognition system) ¹⁷²に関する、Northgate Public Services 社との契約を、ロンドン市長の警察・犯罪対策室 (The Mayor of London's Office for Policing and Crime : MOPAC) が承認したと、2021 年 9 月末に報じられた¹⁷³。4 年契約で £ 300 万を超える。2021 年末か 2022 年初頭には利用可能になるとされる。ロンドン警視庁は、新たに設置された、ロンドン警察活動倫理パネル (London Policing Ethics Panel : LPEP) に、ガバナンスについて意見を求めた。LPEP は 10 月のミーティングにおいて、事後的な顔認識のもたらす倫理的課題について調査することを引き受けた。

●サウスウェールズ警察は、2020 年に高裁判決以来中止していたライブ顔認識技術の利用を、2022 年 3 月 19 日にカーディフ市の中心部で試行から再開すると発表した¹⁷⁴。再開する準備をしており、試行では判決で指摘された事項に対応できていることを確認する。警察・犯罪コミッションナーの Alun Michael 氏の言葉を以下に引用する。

「顔認識技術の使用に関して倫理的・社会的な懸念が表明されているため、私は技術の導入に関する運用上の決定を綿密に精査し、新しいステップごとに独立した監督と精査を行うことにしている。人々は、何も悪いことをしていない一般市民が不適切な監視の対象になっていないこと、そして彼らのプライバシーと匿名性が尊重され保護されることを知りたがっている。しかし、人々はまた、私たちが自分たちの安全を守り、重大な罪を犯した人々を逮捕し、街から排除するためにこの技術を利用することを望んでいる。強固な精査と挑戦のシステムを導入した結果、私たちはこのバランスをうまくとっていると、国民の皆さまに安心していただけると思っている。私たちは、市民の安全を守るだけでなく、人権の保護にも力を注いでいる。」「警察官は、これまでも指名手配中の人物を発見し、路上で呼び止めることができた。この技術の使用による違いは、単純に、個人を特定し逮捕するスピードと正確さ、そして、人違いを解消するスピードにある。」

appeal-judgment-r-bridges-v-south-wales-police-automated-facial-recognition
<https://videosurveillance.blog.gov.uk/2020/08/11/what-next-for-automated-facial-recognition/>

¹⁷² <https://www.london.gov.uk/what-we-do/mayors-office-policing-and-crime-mopac/governance-and-decision-making/mopac-decisions-0/retrospective-facial-recognition-system>

¹⁷³ <https://www.forbes.com/sites/emmawoollacott/2021/09/28/londons-met-police-buying-retrospective-facial-recognition-technology/>

¹⁷⁴ <https://www.south-wales.police.uk/news/south-wales/news/2022/maw-mar/keeping-south-wales-safe-with-facial-recognition-technology/>

●英国の警察大学（College of Policing）は2022年3月22日、1年間のパブリックコメント期間を経て、イングランドおよびウェールズの警察向けの「ライブ顔認識」についてのガイダンスとなる報告書を公表した¹⁷⁵。策定プロセスの中で、一般市民、警察、規制機関、キャンペーン団体との協議を経たうえで、また、Bridges v South Wales Police 控訴院判決（2020年）を踏まえて作成され、判決で指摘された問題に対処しているとされている。

●ロンドン警察（MPS）はコロナ禍により中断されていたライブ顔認識（LFR）の利用を2022年に入ってから再開し、7月末までに6回（Oxford Circusで4回、Leicester Squareで1回、Piccadilly Circusで1回）実施していたことが明らかになった¹⁷⁶。最初のもは2022年1月28日、ロンドン中心部のウェストミンスター周辺にLFRカメラバンを設置し、LFRシステムの警告を吟味した警察官によって指名手配中の4人を逮捕したことを公表した¹⁷⁷。MPSの資料には、ウォッチリストの人数、合計アラート、間違っアラート、真のアラート、逮捕件数に加えて、スキャンされた顔の数も掲載されている。先の1回目では9,756人分のウォッチリストが用意され、11の警告があったとされている。2022年に逮捕されたのは、麻薬所持、救急隊員への暴行、出頭拒否、交通違反など8人だけだった¹⁷⁸。

3.3 その他の動向

●Ada Lovelace Institute は2020年、地理的に代表性を考慮したおよそ60人の市民からなる「市民バイオメトリクス委員会（Citizens' Biometrics Council）」を立ち上げた¹⁷⁹。同時に、プロセスが機能することを保証するために「監督グループ（Oversight Group）」も立ち上げられた。監督グループのメンバーは以下のとおりである。Ali Shah氏（Head of Technology Policy, ICO）、Jack Stilgoe博士（Senior Lecturer in Science and Technology Studies, UCL）、Julie Dawson氏（Director of Regulatory and Policy, Yoti）、Lindsey Chiswick氏（Head of Intelligence and Covert Policing, Metropolitan Police Service）、Pete Fussey博士（Professor of Sociology, University of Essex）、Zara Rahman氏（Deputy Director, The Engine Room）。市民バイオメ

¹⁷⁵ <https://www.college.police.uk/article/live-facial-recognition-technology-guidance-published>

¹⁷⁶ <https://www.met.police.uk/SysSiteAssets/media/downloads/force-content/met/advice/lfr/deployment-records/lfr-deployment-grid.pdf>

¹⁷⁷ <https://www.pariaki.com/2022/01/four-arrests-in-live-facial-recognition-operation-in-central-london/>

¹⁷⁸ <https://www.computerweekly.com/news/252523634/Met-Police-ramp-up-facial-recognition-despite-ongoing-concerns>

¹⁷⁹ <https://www.adalovelaceinstitute.org/our-work/identities-liberties/citizens-biometrics-council/>

トリクス委員会での議論は2020年10月で終了し、6分野（独立の監督機関・法制化・規制、データ管理、多様な文脈における比例性、バイアス・差別・正確性、同意とオプトアウト、透明性）31項目からなる勧告を含む報告書は2021年3月に公表され、同時にイベント「バイオメトリクス技術の利用については何がOKで何がNGなのか」が開催された¹⁸⁰。

●複数のUber Eatsの配達員とUber運転手が、Uber社が採用した「人種差別的な」顔識別ソフトウェア（Uber社は“photo comparison”ツールと呼んでいる）にIDが確認されなかったとして解雇され、ロンドン交通局（Transport for London：TfL）によってライセンスが取り消されたとWIREDが2021年3月1日付で報じた¹⁸¹。Uberは2020年4月に英国において、“Real Time ID Check”システムを立ち上げた。労働組合（App Drivers & Couriers Union：ADCUとWorker Info Exchange：WIE）は、顔認識技術を提供しているMicrosoft社に対して、Uber社が採用しているB2B顔認識の利用を停止するように要請した¹⁸²。ADCUは、TfLは本件について平等影響評価（Equality Impact Assessment）を実施していないことを指摘している。

●2022年6月、Ada Lovelace研究所が2020年に委託し、Matthew Ryder QCが主導したレビューが「Ryderレビュー：イングランドとウェールズにおける生体計測データのガバナンスに関する独立の法的レビュー」として公表された¹⁸³。バイオメトリクスの間違った利用から人々を保護するために包括的な新法と執行組織が「緊急に必要」であると結論づけた。レビューは、1）レビューチームによる調査、（2）様々な関係者とのインタビュー、（3）諮問委員会（Advisory Board）との連携、という3つの柱からなる。インタビューは、2020年9月から2021年2月にかけて24人に対して実施された。イングランドとウェールズにおける生体計測データのガバナンスを発展させるための10の提言が策定された。以下に抜粋を示す。

- 提言1：新たな法的枠組みの必要性。
- 勧告2：法的枠組みは、識別（identification）と分類（classification）のための生体計測データの使用をカバーすべきである。
- 勧告3：特定の分野や技術を規制するために、生体計測データの使用に関する具体的な行動規範（code of practice）を公表すべきである。スコットランドの生体認証技術コミッ

¹⁸⁰ <https://www.adalovelaceinstitute.org/event/citizens-biometric-council/>

¹⁸¹ <https://www.wired.co.uk/article/uber-eats-couriers-facial-recognition>

¹⁸² <https://techcrunch.com/2021/03/19/uber-under-pressure-over-facial-recognition-checks-for-drivers/>

¹⁸³ <https://www.adalovelaceinstitute.org/report/ryder-review-biometrics/>

ショナーに与えられたものと同様の遵守メカニズムを、このような行動規範に付随させるべきである。

- 勧告 4：ライブ顔認識（LFR）、特に警察による LFR 利用を統治する法的拘束力のある行動規範（code of practice）を、できるだけ早く政府によって公表すべきである。
- 勧告 5：新しい法的枠組みと行動規範（code of practice）が整備されるまで、いかなる状況下でもライブ顔認識（LFR）の使用を停止すべきです。
- 勧告 6：1998 年人権法、2010 年平等法、2018 年データ保護法の下で生じる義務は、生体計測データの使用に引き続き適用されるべきである。
- 勧告 7：国の生体認証技術倫理委員会（Biometrics Ethics Board）を設立し、公共部門の生体認証技術の使用に関して強制的な助言の役割（mandatory advisory role）を与えるべきである。
- 勧告 8：生体認証技術倫理委員会（Biometrics Ethics Board）の助言は公表されるべきである。倫理委員会の助言に反して生体認証技術の導入を決定した場合、導入機関は倫理委員会の助言から 14 日以内に、倫理委員会の助言を拒否した理由、または導入前に委員会の助言に対応するためにとった措置の概要説明を公表する。
- 勧告 9：監督機能を統合、明確化し、適切なリソースを提供すべきである。
- 勧告 10：生体認証技術の民間部門での利用と官民シェアリングのトピックについて、さらなる取り組みが必要である

同時に、上記の法的レビューに加えて、生体認証技術に対する人々の態度に関する一般市民参加型調査を含む、同研究所における 3 年間のバイオメトリクスガバナンスに関する研究プログラムの成果として、政策レポート「対策：英国における生体認証技術を管理するための新たな法律の必要性」も発表した¹⁸⁴。以下に勧告部分の抜粋を示す。

1. 政府は、生体認証技術の使用を規定する新規の一次法案を成立させるべきである。

¹⁸⁴ <https://www.adalovelaceinstitute.org/report/countermeasures-biometric-technologies/>

2. この法律の監督と執行は、生体認証技術に焦点を当てた、国の独立した、十分なリソースと権限を持つ新しい規制機能の中に位置づけられるべきものである。

3. この規制機能は、2つのレベルで生体認証技術の評価を監督する必要がある。

・すべての生体認証技術が、正確性、信頼性、妥当性に関する、科学に基づき、明確に確立された基準を満たすことを要求する必要がある。

・公共部門によって、公共サービスにおいて、誰でもアクセス可能な空間において使用されるもの、または個人について重要な決定を行うものについては、使用前に、提案された文脈における生体認証技術の比例性 (proportionality) を評価する必要がある。

4. 包括的な法律が成立するまで、誰でもアクセス可能な空間における一対多の本人識別と、公共部門における、公共サービスのための、誰でもアクセス可能な空間における分類のための生体認証技術の使用はモラトリアムにすべきである。

● [報告書] ケンブリッジ大学の研究者らによる独立チームである Minderoo Centre for Technology and Democracy から「社会技術的監視：警察による顔認識の利用を評価する」と題する報告書が2022年10月27日、発表された¹⁸⁵。研究者らが顔認識技術のガバナンスのための「最低限の倫理的・法的基準」を策定し、英国警察（ロンドンとサウルウェールズ）の3つの実践例を監査したところ、3つとも上記基準を満たしていなかったと報告した。

4. スコットランドの動向

●議会の「警察活動に関する司法小委員会 (Justice Sub-Committee on Policing)」は2019年10月から2020年2月まで、スコットランドにおける警察活動が顔認識技術をどのように利用していたかについての調査を実施し、2020年2月11日、報告書「顔認識：スコットランドにおける警察活動がこの技術を利用しているか」を公表した¹⁸⁶。ポイントは、顔認識技術の利用が、合法的で、倫理的で、必要で、比例的で、透明であるかどうかであるとしたうえで、報告書では結論として、現時点ではライブでの顔認識技術は利用すべきでないことは明白であるとし、スコットランド警察が導入しないことを確約することを望むとした。事後的な (retrospective) 顔認識

¹⁸⁵ <https://www.mctd.ac.uk/a-sociotechnical-audit-assessing-police-use-of-facial-recognition/>

¹⁸⁶ <https://digitalpublications.parliament.scot/Committees/Report/JSP/2020/2/11/Facial-recognition--how-policing-in-Scotland-makes-use-of-this-technology>

技術はすでに利用されているが、有罪判決を受けなかった人の顔写真の保持と利用については対処すべき事項として挙げられた。

●2020年3月10日に「スコットランド生体認証コミッショナー法（Scottish Biometrics Commissioner Bill）」を可決したスコットランド議会は、11月末、初のバイオメトリクス・コミッショナー（Biometrics Commissioner）の公募を、12月17日締め切りで開始した。任期は8年で、給与は7万ポンドで年金付きとされた。2021年4月12日、レスター大学で犯罪学の博士号を取得した Brian Plastow 博士は初代の Biometrics Commissioner に任命された¹⁸⁷。

●スコットランドの North Ayrshire 地区の9つの中学校が、2021年10月17日、ランチタイムの食堂の行列をスピードアップするために顔認識技術を利用し始めたと報じられた¹⁸⁸。すでに設置されている指紋認証やカード支払いシステムに代わるものとして導入された。North Ayrshire council によると97%の生徒や保護者が新しいシステムの実施へ同意したという。専門家は、学校での顔認識の常態化する（normalize）ことがもたらす影響、さらにはその先にあり得る GDPR への影響について懸念を表明したという。

●2022年4月20日、スコットランドの生体情報コミッショナー（SBC）は、スコットランドでの刑事司法および警察の目的での生体計測データの取得、保持、使用、および破棄に関する「行動規範（‘code of practice’）」の草案（Draft Version 0.4）のパブリックコンサルテーションを開始した¹⁸⁹。6月1日締め切り。12の指導原則と倫理的考慮事項を中心に構成されている。内容は第5部で説明されている。

また、新たな生体計測技術を実装する際のプロセスも提案され、データ保護影響評価（DPIA）、平等と人権への影響評価（EQHRIA）、コミュニティ影響評価（CIA）が実施され、人々の安全と公共の善のために、評価結果は公表されるべきであるとされた。

6月15日、スコットランドのバイオメトリクス・コミッショナーである Brian Plastow 博士は、スコットランド議会に、警察が保有する生体計測情報についての「行動規範（‘code of practice’）」の草案を提出した¹⁹⁰。スコットランド議会の司法委員会で8月に承認された行動

¹⁸⁷ <https://www.biometricscommissioner.scot/about-us/who-we-are/>

¹⁸⁸ <https://techmonitor.ai/policy/privacy-and-data-protection/facial-recognition-in-schools-ayrshire>

¹⁸⁹ <https://www.biometricscommissioner.scot/news/public-consultation-on-the-scottish-biometrics-commissioner-s-code-of-practice/>

¹⁹⁰ <https://www.scotsman.com/news/politics/scotland-could-mark-significant-human-rights-achievement-if-biometric-data-code-of-practice-is-introduced-says-commissioner-3732625>

規範（Code of Practice : CoP）（Ver.1.0）は、11月16日に施行された¹⁹¹。12の指針原則は以下のとおりある。

1. 法的権限と法的根拠（Lawful authority and legal basis）
2. 必要性（Necessity）
3. 比例性（Proportionality）
4. 公共の安全と公益の増進（Enhance public safety and public good）
5. 倫理的行動（Ethical behaviour）
6. 個人及び集団の人権の尊重（Respect for the human rights of individuals and groups）
7. 正義とアカウンタビリティ（Justice and accountability）
8. 科学技術の発展を促進（Encourage scientific and technological advancement）
9. 子ども、若者、脆弱な成人の保護（Protection of children, young people, and vulnerable adults）
10. プライバシー保護技術の推進（Promoting privacy enhancing technology）
11. 平等の促進（Promote equality）
12. 法律で許可された保存期間（Retention periods authorised by law）

●[報告書]英国スターリング大学（University of Stirling）の研究者らが受託研究報告書「警察における身体装着型ビデオ（BWV）の一般的な使用経験と信頼性に関するエビデンス・レビュー」を、迅速研究プロジェクトとして2022年6月29日、公表した¹⁹²。2021年秋にスコットランド警察、スコットランド警察当局（SPA）、スコットランド警察研究所（SIPR）から委託されたもので、調査は、2021年11月から12月にかけて、文献レビューとBWV専門家との一

¹⁹¹ <https://eandt.theiet.org/content/articles/2022/11/scotland-publishes-first-code-of-practice-for-the-use-of-biometric-data/>

¹⁹² <https://www.sipr.ac.uk/research-resources/rapid-research-project-evidence-review-into-public-experience-and-confidence-of-body-worn-video-in-a-policing-context/> あるいは、<http://www.crisp-surveillance.com/blog/224214/evidence-review-public-experience-and-confidence-body-worn-video-policing-context>

連の半構造化インタビューからなる方法論を用いて実施された。調査目的は、将来スコットランドで BWV が広く展開される可能性があることを念頭にスコットランド警察に対して助言と指針を提供することである。提言は、市民・地域社会とのかかわりに関わるもの 4 点、警察における BWV の活用とベストプラクティスに関するもの 4 点、BWV のガバナンス：法的・倫理的問題として 3 点挙げられた。

5. カナダの動向

●2020 年 2 月 21 日、連邦政府と、ケベック州、ブリティッシュコロンビア州、アルバータ州のプライバシー保護当局が合同で、Clearview AI 社と当社の顔認識技術の利用について捜査を開始することを発表した¹⁹³。各種メディア報告を受けたもので、当社が本人の同意なしに個人情報を収集・利用しているかどうか焦点となっており、連邦や州のプライバシー法制を遵守しているかどうかについての調査が開始された。

●2020 年 7 月 6 日、カナダの連邦プライバシー・コミッショナー局（OPC）は、ニュースリリースで、連邦と各州の共同捜査に対して、Clearview AI 社がカナダにおける顔認識サービスの提供をやめることを表明したことを伝えた¹⁹⁴。これは、カナダで最後のクライアントであった RCMP（カナダ騎馬警備隊）との契約を解除することを意味する。このことについて、Ann Cavoukian 氏は「すばらしいニュースだ」とコメントした¹⁹⁵。

●2021 年 2 月 2 日、1 年前からの Clearview AI 社への調査結果が公表された¹⁹⁶。3 つ問いの問いへの回答は以下の通りある。

Issue 1: Did Clearview obtain requisite consent? →得ていなかった。

Issue 2: Was Clearview collecting, using or disclosing personal information for an appropriate purpose? →適切でも合法的でもなかった。

Issue 3: Did Clearview satisfy its biometric obligations in Quebec? →満たしていなかった。

¹⁹³ https://www.priv.gc.ca/en/opc-news/news-and-announcements/2020/an_200221/

¹⁹⁴ https://www.priv.gc.ca/en/opc-news/news-and-announcements/2020/nr-c_200706/

¹⁹⁵ <https://www.cbc.ca/news/technology/clearview-ai-stops-facial-recognition-in-canada-1.5639380>

¹⁹⁶ <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2021/pipeda-2021-001/>

そのうえで、Clearview 社に対して下記を勧告した。

1. 当該調査の対象となっているカナダのクライアントへの顔認識サービスの提供をやめること。
2. カナダにおける個人から写真と顔特徴量を収集、使用、及び開示することをやめること。
3. カナダにおける個人からすでに収集した写真と顔特徴量を削除すること。

調査に対して、Clearview AI 社の主張は、当社はカナダにリアルなつながりはなく、カナダの法律が適用されない、そして収集した情報は誰でも利用可能なものであるために個人からの同意は必要ないと主張した。しかし、プラットフォーム各社は、人々の情報をスクレイピングすることはそれらの利用ポリシーに規約に反していると主張し、Clearview AI 社に中止するように要請していた。

●カナダ議会の下院（庶民院：House of Commons）の「情報公開・プライバシー・倫理常任委員会（Standing Committee on Access to Information, Privacy and Ethics：ETHI）」の2021年5月10日のミーティング「顔認識技術の利用と影響」において¹⁹⁷、プライバシー・コミッショナーの Daniel Therrien 氏は、下院に提案されている Bill C-11（Consumer Privacy Protection Act：CPPA）について不十分であると批判した。

●カナダ政府のプライバシー・コミッショナー局（OPC）は、2021年6月10日付の国会への特別報告書において、王立カナダ騎馬警察（Royal Canadian Mounted Police：RCMP）は Clearview AI の顔認識技術を利用することでカナダのプライバシー法に違反していると結論づけた¹⁹⁸。同時に、OPC は、州と準州（provincial and territorial）のプライバシー当局とともに、「警察機関による顔認識技術の利用に関する指針案」を6月15日、公表し、パブリックコンサルテーションを始めた。

●2021年7月、トロントのピアソン国際空港で2016年に6か月間、連邦政府が秘密裡に顔認識技術进行测试していたことがGlobe and Mail が情報公開請求により入手した文書により明らかになった¹⁹⁹。ターミナル3の到着エリアに31台のカメラが到着客の顔を映し、5000人規模の出国リストと照合された。目的は、カナダ国境サービス庁（Canada Border Services Agency：CBSA）が、偽のIDによって入国を試みようとしていると疑った人物を見つけることであった。

¹⁹⁷ <https://www.ourcommons.ca/DocumentViewer/en/43-2/ETHI/meeting-34/notice>

¹⁹⁸ https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/202021/sr_rcmp/

¹⁹⁹ <https://www.theglobeandmail.com/canada/article-ottawa-tested-facial-recognition-on-millions-of-travellers-at-torontos/>

●ケベック州の情報アクセス委員会 (Commission d'Accès à l'Information : CAI) は 2021 年 10 月 28 日、パンデミックの状況下で、顔認識機能付きサーマルカメラを使用して個人情報を収集したことは、民間部門における個人情報の保護を尊重する法律に違反すると結論づけた²⁰⁰。この決定に基づいて、委員会はある企業に対して、従業員の体温を測定・記録する業務の停止を命じた。

●ケベック州では 2021 年、「民間企業における個人情報保護に関する法律 (Act respecting the protection of personal information in the private sector)」が改正され、2022 年 9 月 22 日に施行される²⁰¹。情報アクセス委員会 (Commission d'Accès à l'Information : CAI)によるサマリーでは、事業者は「個人の身元を確認するために生体計測技術を使用する前に、委員会に通知する」必要があると述べている²⁰²。

●下院の情報公開・プライバシー・倫理常任委員会 (ETHI) は、「顔認識技術の利用と影響」と題する継続的な調査を行っており、様々なステークホルダーが参加している²⁰³。2022 年 5 月 2 日には、連邦のプライバシー・コミッショナーの Daniel Therrien 氏²⁰⁴、オンタリオ州の情報プライバシー・コミッショナーである Patricia Kosseim 氏、ケベック州の情報アクセス委員会の委員長である Diane Poitras 氏らが証人として意見を述べた。

●プライバシー・コミッショナー局はパブリックコンサルテーションを経た「警察組織のための顔認識に関するプライバシー指針」の最終版を 2022 年 5 月、公表した²⁰⁵。前提として、警察による顔認識技術の使用に関する現在の法規制が不十分であると指摘している。そのうえで、法的要求を満たすだけでなく、プライバシーを保護する必要性が強調されている。そのために、警察機関は、個人情報の収集・使用・開示を伴う取り組みを実施または大幅に修正する前に、PIA (プライバシー影響評価) を実施する必要があること、そしてカナダの一部の管轄区域では、政府機関が PIA を実施することが義務付けられていることが述べられている。それ以外にも、正確性、アカウントビリティ、データ最小化、目的の制限、保持、データセキュリティ、オープン・透明性・個人のアクセスが挙げられた。

²⁰⁰ <https://www.cai.gouv.qc.ca/cameras-thermiques-outils-de-reconnaissance-faciale-la-commission-se-prononce/>

²⁰¹ <https://www.legisquebec.gouv.qc.ca/en/document/cs/P-39.1>

²⁰² https://www.cai.gouv.qc.ca/documents/CAI_FI_New_Obligations_Businesses.pdf

²⁰³ <https://www.ourcommons.ca/Committees/en/ETHI/StudyActivity?studyActivityId=11566271>

²⁰⁴ https://www.priv.gc.ca/en/opc-actions-and-decisions/advice-to-parliament/2022/parl_20220502/

²⁰⁵ https://www.priv.gc.ca/en/privacy-topics/surveillance/police-and-public-safety/gd_fr_202205/

●連邦政府の Bill C-27 の一部として提案されているプライバシー法案は、下院 (House of Commons)において2022年6月16日に第一読会が開催された²⁰⁶。Part 3の”Artificial Intelligence and Data Act”部分では、民間部門において、生体計測技術 (バイオメトリクス) を含む AI の設計・開発・利用において標準的な基準を確立する規制も含まれている (ただし、警察は対象外とされている)。「影響力の大きい AI システム」の場合、「そのシステムの使用から生じ得る危害又は偏った出力のリスクを特定し、評価し、及び軽減するための措置を定めなければならない」こととされている。大臣は、「差し迫った重大な危険を生じさせると信じるに足る合理的な理由がある場合」に当該システムの使用を中止させることができる。

●2022年10月4日、カナダ下院の情報アクセス・プライバシー・倫理常任委員会 (ETHI) は、9回の公聴会を開催し、33人の証人から聞き取りを行い、それらの結果を報告書「顔認識技術と AI の発展する発展」として公表した²⁰⁷。報告書²⁰⁸では、現時点では顔認識技術や AI を適切に規制する法的枠組みは存在しないため、連邦警察業務における顔認識技術の使用については、国家としてモラトリアムを設けるべきである (提言 18) など、19の提言が行われた。本報告書に対して、プライバシー・コミッショナーから、本報告書の公表を歓迎する声明が出された²⁰⁹。提言 18以外にも下記のような提言がなされている。

提言 11 政府は、顔認識技術やその他のアルゴリズム技術の許容可能な用途を適切な法律で定義し、マスサーベイランスを含むその他の用途を禁止すること。

提言 12 カナダ政府は、プライバシー法を改正し、政府機関が顔認識技術の採用、作成、使用に先立って、プライバシー・コミッショナーの助言と勧告を求め、影響評価を同委員会の事務所に提出することを義務付けること。

提言 15 カナダ政府は、民間団体による生体情報の収集についてオプトインのみの要件を実施し、当該団体が生体情報の提供を条件として商品やサービスの提供を行うことを禁止すること。

提言 17 カナダ政府は、顔認識技術のデータベースや AI のアルゴリズムに組み込む目的で、インターネットや公共の場からカナダ人の画像をキャプチャする行為を禁止するために、プライバ

²⁰⁶ <https://www.parl.ca/legisinfo/en/bill/44-1/C-27>

²⁰⁷ <https://www.ourcommons.ca/DocumentViewer/en/44-1/ETHI/news-release/11957568>

²⁰⁸ <https://www.ourcommons.ca/Content/Committee/441/ETHI/Reports/RP11948475/ethirp06/ethirp06-e.pdf>

²⁰⁹ https://www.priv.gc.ca/en/opc-news/speeches/2022/s-d_20221006/

シー法などを改正すること。

6. 欧州の動向

6.1 EU

●欧州データ保護会議（EDPB）は2020年6月9日に開催された第31回EDPB会合の全体セッションにおいて（議題3.1）、議員（MEP）らからの、法執行当局によるClearview AIの利用に関する質問への回答を示した²¹⁰。法執行指令（Law Enforcement Directive (EU) 2016/680）の第8条（適法性）や第10条（特別カテゴリーの個人データの処理）の厳しい条件に従えば、自然人の識別を行う目的に限って生体情報を処理することができるとしたうえで、Clearview AIのようなサービスの利用は、EUのデータ保護体制になじまないとの見解を示した。

●2020年6月24日、スペインのデータ保護当局と欧州データ保護監督官（EDPS）の共同ペーパー「生体識別と認証に関する14の誤解（14 misunderstandings with regard to biometric identification and authentication）」が公表された²¹¹。これに対して、多国籍の10名の研究者らによる「誤解における誤解」と題するペーパーが公表されている²¹²。

●欧州の欧州国境沿岸警備機関（European Border and Coast Guard Agency：Frontex）は、陸上の国境におけるスマート出入国システム（entry-exit system：EES）のために生体認証技術等の検証を行う予定である²¹³。欧州議会は、EU規制2017/2226²¹⁴によって、第三国からの旅行者を登録するための共通出入国システム（entry-exit system：EES）を導入することに同意している。すなわち、陸・空・海の国境経由でシェンゲン国に入国する際に、第三国の国民は4本の指の指紋と顔写真を登録することが2022年までに義務付けられることになる。

●European Digital Rights (EDRi)は2020年5月に44の市民団体で、生体認証技術を使ったマ

²¹⁰ <https://edpb.europa.eu/news/news/2020/thirty-first-plenary-session-establishment-taskforce-tiktok-response-meps-use>

²¹¹ https://edps.europa.eu/data-protection/our-work/publications/papers/14-misunderstandings-regard-biometric-identification_en

²¹² https://eab.org/files/documents/2020-08-01_EAB-EDPS_aepd-response.pdf

²¹³ <https://www.biometricupdate.com/202008/eu-pilots-biometric-solutions-for-smart-entry-exit-system-to-protect-land-border-crossings>

²¹⁴ <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R2226&from=EN>

スサーベイランスの禁止を欧州委員会と EU 加盟国に対して呼び掛けた²¹⁵。11 月には 12 団体で、「あなたの顔を取り返せ (Reclaim Your Face)」キャンペーンを開始した²¹⁶。そして、2021 年 1 月 7 日、新しい欧州市民イニシアティブ (ECI) として、生体認証技術を使ったマスサーベイランスの実践の禁止を呼び掛ける市民イニシアティブが登録された²¹⁷。2021 年 2 月 17 日から、署名活動 “Reclaim Your Face” が公式に ECI として開始された²¹⁸。ECI は、EU 市民に対して、新規の法規制枠組みを要求する運動を組織化するためのスペースを提供するツールである。7 か国以上の 100 万人の署名が集まれば、欧州委員会は新規の法律を求める正式な要請として対応し、欧州議会は議論を開始することが義務付けられる。2022 年 10 月現在、署名はまだ 8 万人に達していない。

●2021 年 1 月 20 日、欧州議会は報告書「人工知能：国際法の解釈と適用に関する疑問 (Artificial intelligence: questions of interpretation and application of international law)」を、賛成 364、反対 274、棄権 52 で採択し²¹⁹、公表した²²⁰。この中で、欧州委員会に対して、顔認識システムの利用に対してモラトリアムを導入することの帰結を評価し、その結果次第では、技術基準が基本的人権を完全に保護し、結果にバイアスがなく、差別的でなく、また、誤用に対する厳しい安全対策が確保されるまでは、法執行機関による準公共空間における顔認識システムの利用についてだけでなく、公的機関による公的空間での利用に対してもモラトリアムを設けることを検討すべきであるとした (56)。

●European Digital Rights (EDRi)を含む 56 の市民団体の連合が 2021 年 4 月 1 日、欧州委員会の司法委員である Didier Reynders 氏に対して、生体認証技術を使ったマスサーベイランスの禁止を求めるオープンレターを送った²²¹。これは近々発表され予定の AI に関する EU 法案に向けたものである。

●2021 年 4 月 21 日、欧州委員会 (European Commission) は AI (人工知能) の規制法案を公

²¹⁵ <https://edri.org/our-work/blog-ban-biometric-mass-surveillance/>

²¹⁶ <https://edri.org/our-work/campaign-reclaim-your-face-calls-for-a-ban-on-biometric-mass-surveillance/>

²¹⁷ https://europa.eu/citizens-initiative/initiatives/details/2021/000001_en

²¹⁸ <https://reclaimyourface.eu/>

²¹⁹ <https://www.biometricupdate.com/202101/new-european-parliament-guidelines-for-ai-and-facial-recognition-invite-moratorium-consideration>

²²⁰ https://www.europarl.europa.eu/doceo/document/TA-9-2021-0009_EN.html

²²¹ <https://edri.org/our-work/european-commission-must-ban-biometric-mass-surveillance-practices-say-56-civil-society-groups/>

表した²²²。第5条で列挙された「禁止されるAI実践」の1つに、「法執行の目的のための、誰もがアクセス可能な空間（publicly accessible spaces）における「リアルタイムでの」リモート生体情報識別システム（‘real-time’ remote biometric identification systems）の利用」が挙げられた。また、第6条で規定された高リスクAIシステムの1つにも、附録IIIにおいて「自然人の生体識別および分類（Biometric identification and categorisation of natural persons）」が挙げられ、「自然人の「リアルタイム」および「ポスト」リモート生体識別に使用することを目的としたAIシステム」とされた。高リスクAIシステムを利用する際には第二章で規定された要件を遵守する必要があるとされた。

●2021年5月27日、Privacy International²²³を含む活動団体は、オーストリア、フランス、ギリシャ、イタリア、及び英国の個人データ保護当局に Clearview AI 社について告訴した（filed complaints）²²⁴。これに対して Clearview AI 社は欧州には顧客がいないと主張している。

●2021年6月21日、EDPBとEDPSは欧州委員会によるAIに関する共通ルールを示した規制案についての共同意見を採択した²²⁵。両者は、提案を強く歓迎するとともに、国際的な法執行協力をスコープ外としたことに懸念を表明した。

●EDRi（European Digital Rights）は、学生組織である EIJI（Edinburgh International Justice Initiative）と共同で2021年7月、報告書「EUにおける生体認証技術によるマスサーベイランスの台頭」を公表した²²⁶。ドイツ、ポーランド、オランダの3か国のケーススタディが実施された。

●[報告書] 欧州議会の司法委員会（JURI）と請願委員会（PETI）からの要望を受けて、Policy Department for Citizens’ Rights and Constitutional Affairs による委託で、ウィーン大学の研究者らが執筆した報告書「生体認識と行動検知」が2021年8月に公表された²²⁷。生体認証技術の利用について、生体識別、生体カテゴリー分け、生体検知の倫理的及び法的な課題を分析したも

²²² <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206>

²²³ <https://privacyinternational.org/campaigns/get-out-our-face-clearview>

²²⁴ <https://www.bloomberg.com/news/articles/2021-05-27/clearview-ai-hit-by-wave-of-european-privacy-complaints>

²²⁵ https://edpb.europa.eu/news/news/2021/edpb-edps-call-ban-use-ai-automated-recognition-human-features-publicly-accessible_en

²²⁶ https://edri.org/wp-content/uploads/2021/07/EDRI_RISE_REPORT.pdf

²²⁷

[https://www.europarl.europa.eu/RegData/etudes/STUD/2021/696968/IPOL_STU\(2021\)696968_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2021/696968/IPOL_STU(2021)696968_EN.pdf)

ので、提案中である AI 規制案への提言がなされた。

● 欧州議会は 2021 年 10 月 6 日、「刑事事件における、刑法と、警察と司法当局によるその利用における AI (artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters)」に関する (法的拘束力を持たない) 決議を、377 対 248 (棄権 62) の賛成多数で採択した²²⁸。

顔認識には、照合/認証、識別、検出など様々なタイプのものがあることが指摘されたうえで、顔認識システムの法執行における利用は、比例性と必要性の原則及び適用可能な法律を完全に尊重したうえで、明確に認可された目的に限定されるべきであるとした。照合/認証システムについては、その悪影響が軽減され、こうした (25 で示された) 要件を満たす場合に限り、利用され続けてもよいとされた。誰もがアクセスできる空間において、顔以外の人間の特徴 (歩容、指紋、DNA、声紋、その他の生体計測的及び行動的特徴) の自動化された分析および/または認識を使用することを恒久的に禁止することが呼び掛けられた (26)。法執行目的での識別機能を持つ顔認識システムの利用については、犯罪被害者の特定目的に限定して用いるのでない限り、技術的基準が完全に基本的権利を保護し、得られた結果にバイアスや差別がなく、法的枠組みが誤用に対する厳しい安全策や厳格な民主的コントロールや監督を提供し、そういった技術の利用のための必要性と比例性の実証的なエビデンスが存在するまでは、モラトリアムを設けることが呼び掛けられた (27)。また、法執行機関が Clearview AI 社のデータベースのような、民間の顔認識データベースの利用の禁止が呼び掛けられた (28)。法執行や司法の文脈で用いられる生体計測に基づく識別 (感情認識技術を含む) は常に「高リスク」とみなされるべきであり、AI に関する欧州委員会の高レベル専門家グループの勧告に従って、追加的な要件に従うべきであるとされた (30)。Horizon 2020 のもとで展開されている研究プロジェクト (iBorderCtrl project) への懸念が表明され、欧州委員会に対して、誰でもアクセスできる空間におけるマササーベイランスにつながるような、法執行目的での顔写真を含む生体計測データの処理を禁止するよう要請するとともに、公的空間における無差別のマササーベイランスにつながりうる生体計測の研究や利用、プログラムへの資金提供を止めるように要請した (31)。AI を利用した個人の大規模なスコアリングの禁止を提唱する高レベル専門家グループの勧告への支持が表明された (32)。この決議案は、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) から提出された報告書²²⁹に基づいたものである。

²²⁸ https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_EN.html

²²⁹ https://www.europarl.europa.eu/doceo/document/A-9-2021-0232_EN.html

●2022年5月16日から6月27日まで、EDPBは、「法執行分野における顔認識技術の利用に関するガイドライン 05/2022」案がパブリックコンサルテーションにかけられた²³⁰。

6.2 フランス

●2021年2月18日、スポーツクラブがスタジアムの観客に対して、一部の観客の入場を禁止するため、及び、武器を発見するために顔認識技術を適用しているという報告を受けて、データ保護機関であるCNILは調査を実施し、CNIL長官であるMarie-Laure Denis氏はクラブに対して、GDPRとフランスのData Protection Actのもとで違法であることを告げた²³¹。CNILはスポーツクラブを明記していないが、Ligue 1に所属するサッカークラブであるFC Metzであると報道されている²³²。

●CNILは、2021年11月26日の決定2021-134号により、Cleaview AI社に対し、GDPRの第6条、第12条、第15条、第17条の規定を2カ月以内に遵守するよう正式に通達した。CNILは2020年5月から12月にかけて複数の訴えを受けて、調査を開始した。2021年5月27日にはPrivacy Internationalからの訴えを受け取った。その結果、2件のGDPR違反が明らかになった。1つは、個人データの収集及び利用にあたって違法な処理を行っていること（第6条違反）であり、もう1つは、自分自身のデータへのアクセス権や消去権を尊重していない点（第12、15、17条違反）が挙げられた。そのため、Clearview AIに対して、フランス領内にいる主体が、インターネット上の顔写真の収集と再利用を中止することと、個人の権利の行使を容易にしたり削除要求に答えたりすることを命じた²³³。

CNIL委員長が出した正式な通知と2回の督促に対して回答がなかったため、2022年6月2日、委員長は（1978年1月6日の改正法22条に基づいて）Claude Castelluccia氏を報告者に任命した。調査終了後の2022年7月14日、報告者は本件で発生したと考えられるGDPR違反の詳細を記載した報告書を同社に通知した。この報告書に対し、同社は意見書を提出せず、本件は2022

²³⁰ https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-052022-use-facial-recognition_en

²³¹ <https://www.cnil.fr/fr/reconnaissance-faciale-et-interdiction-commerciale-de-stade-la-cnil-adresse-un-avertissement-un-club>

²³² <https://www.nasdaq.com/articles/french-watchdog-warns-sports-club-about-unlawful-use-of-facial-recognition-technology-2021>

²³³ <https://www.cnil.fr/en/facial-recognition-cn-il-orders-clearview-ai-stop-reusing-photographs-available-internet>

年 10 月 13 日開催の会議で報告された。

CNIL は審議の結果、2022 年 10 月 17 日、Clearview AI 社に対して以下のことを命じた²³⁴。

- ・ 2000 万ユーロ（約 20 億円）の罰金を科すこと
- ・ 法的根拠なくフランス領内の個人の個人情報を収集及び処理しないこと。個人情報、特に削除を要求した個人の情報をすべて削除すること。
- ・ 本決定通知後 2 か月の機関終了後に、遅延 1 日につき 10 万ユーロの違約金を差止命令に付加すること。

GDPR 第 6 条、12 条、15 条、17 条に関連する違反は、第 83 条に基づき、2000 万ユーロと年間売上高の 4% までのいずれか高い額の行政罰の対象となりうる基本原則の違反であることに留意し、また、同社が売上高に関する情報を一切提供しなかったことも考慮し、2000 万ユーロの罰金を課すことは正当であるとした。また、違反が継続し、内容が重大であることから差止命令を出す必要があるとし、これを遵守しない場合は、遅延 1 日につき 100,000 ユーロの違約金の支払いを課すことも決定した。

●2020 年 5 月 28 日に開催された UEFA チャンピオンリーグ（リバプール対レアルマドリード）では、競技場「スタッド・ド・フランス」の場外で、リバプールファンに対して警察が催涙スプレーを浴びせて入場を制限した問題について、フランス政府は「偽造チケット」が大量に流通したのが原因だと述べた。2021 年 2 月、CNIL は、対テロキャンペーンの一環として、スタジアムへの入場禁止者を選別するために顔認証システムを実験的に導入した FC Metz サッカークラブに警告を発した。フランスではすでに公共空間での顔認識技術の利用を禁止しており、「重要な公益上の理由」などの例外を認めているものの、スタジアムの入り口でのファンの本人確認は含まれていない。EU 理事会と欧州議会では、欧州委員会が提案した AI 規制法案の審議が続いており、この提案の第 5 条は、「法執行の目的で、公的にアクセス可能な場所でのリアルタイム遠隔生体認証システムの使用」を原則禁止している。しかし、今回の騒動と合わせて、2024 年の夏季オリンピックがパリで開催されることもあり、顔認識技術の利用の是非についての議論が再燃することが予想される²³⁵。

●フランス CNIL は 2022 年 7 月 19 日、AI 機能付きのカメラ（“拡張型カメラ”）に関するオピ

²³⁴ <https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000046444859>

²³⁵ <https://cepa.org/champions-league-spurs-facial-recognition-debate/>

ニオンを公表した²³⁶。そのために、ポジションの草案が発表され、あらゆるステークホルダーが意見を述べるができるよう、2ヶ月間のパブリックコンサルテーションに付された。これらを受けての最終とりまとめとなる。拡張型カメラの利用は、自動画像解析は人々が知らないうちに個人データの大規模な処理につながる可能性があり、個人に対する監視意識がさらに強まることが指摘されている。そのため、明確なルールがない中で導入する組織は、ケースバイケースに、その「正当な利益」や比例性を事前に示すとともに、プライバシー・バイ・デザインを徹底する必要があることも指摘されている。CNIL はオピニオンの結論として、「そのため、多くの場合、公共空間での拡張カメラの使用を許可する規制や法律の文章が必要になります。この法的分析は、公権力が「技術的に可能なこと」を超えて、倫理的・社会的に望ましいことと、民主主義社会ではそうでないことの間で線を引くという政治的必要性に沿ったものである。」としている。

●2022年11月、フランスのスポーツ省は、2024年にパリで開催されるオリンピック・パラリンピックでは、セキュリティ対策として顔認証を使用しないことを明らかにした²³⁷。2024年パリ・オリンピックの組織に関する法案の一部において明示的に顔認識技術の使用を除外することが明記される予定であるという。

6.3 イタリア

●2022年3月9日、イタリアのデータ保護当局（Garante per la protezione dei dati personali, or GDPR）は Clearview AI 社に対して、国民の同意を得ることなしに生体計測情報を収集したに基づき、2000万ユーロの罰金と、イタリアの個人から収集したデータの削除とさらなる収集・処理の禁止を命じた²³⁸。これらを受けて、Clearview AI 社は欧州の IP アドレスからの同社ソフトウェアへのアクセスを遮断した。

●イタリア南部の都市レッチェ (Lecce) などが顔認識技術の利用を実験していることに対して、データ保護当局は 2022 年 11 月 14 日、批判する声明を出した²³⁹。データ保護当局によると、特定の法律が施行されるか、2023 年 12 月 31 日までは、司法捜査または犯罪防止・抑止目的のため

²³⁶ <https://www.cnil.fr/fr/cameras-dites-augmentees-dans-les-espaces-publics-la-position-de-la-cnil>

²³⁷ <https://www.biometricupdate.com/202211/facial-recognition-ruled-out-for-2024-olympics-and-paralympics-by-french-ministry-of-sport>

²³⁸ <https://www.biometricupdate.com/202203/italian-privacy-authority-fines-clearview-ai-e20m-orders-biometrics-deletion>

²³⁹ <https://www.reuters.com/technology/italy-outlaws-facial-recognition-tech-except-fight-crime-2022-11-14/>

めの処理を除き、生体情報を用いた顔認識システムの設置・使用は認められておらず、自治体がビデオ監視システムを使用できるのは、市長と政府との間で「都市安全協定」が結ばれているときに限るとされた。

6.4 オランダ

●オランダでは、データ保護機関（AP）が、業界団体（CBL）を通して、スーパーマーケット・セクターに顔認識カメラの利用に関するルールを通知したと、2020年6月5日、報道された²⁴⁰。顔情報はGDPRでは特別カテゴリでありその使用は原則禁止されており、例外は、1) 明示的な同意を得られているときか、2) 「重要な公共的利益」のためにセキュリティや認証目的で利用される場合であるとされた。

●オランダの警察は、2020年に不正に顔データベースに登録された約21.8万件の顔写真を顔認識データベースから削除したことを明らかにした²⁴¹。2010年に警察が未決勾留での容疑者写真を撮ることを義務付けたため、それ以前の顔写真が削除された。

6.5 スウェーデン

●スウェーデンのプライバシー保護当局（IMY）は2021年2月、調査の結果、スウェーデン警察当局に対して、Clearview AI社の顔認識ソフトウェアを利用して個人を特定する際に、同国のCriminal Data Actに違反して個人データを処理したと結論づけ、250万SEK（約25万ユーロ）の罰金を命じた²⁴²。何人かの被雇用者が事前の認可を受けずに同ソフトウェアを利用したことが明らかになった。また、実施が義務付けられているデータ保護影響評価（DPIA）を実施していなかったことも指摘された。警察当局は、Clearview AI社にデータが送られたデータ主体に通知し、さらに送付されたデータを可能な限り削除するように命じられた。

6.6 ギリシャ

●ギリシャのデータ保護当局（HDPA）は2022年7月13日、22ページの決定文書を発表し、Clearview AI社がGDPRの一部（第5条、6条、9条、12条、14条、15条、27条）に違反し

²⁴⁰ <https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-wijst-supermarkten-op-regels-gezichtsherkenning>
(オランダ語)

²⁴¹ <https://nltimes.nl/2021/07/23/police-removed-218000-photos-facial-recognition-database-last-year>

²⁴² <https://www.imy.se/en/news/police-unlawfully-used-facial-recognition-app/>

ているとして、2000 万ユーロの罰金を課すとともに、ギリシャ国内の個人に関する生体計測データの処理の停止を要求し、同社にすでに蓄積されたデータをすべて削除しなければならないとした²⁴³。この決定は、2021 年 5 月に、ギリシャの Homo Digitalis を含む多くのプライバシー擁護団体がギリシャ、英国、イタリア、オーストリア、フランスの当局に提出した訴状に対するものである。Clearview AI 社は、The Record への声明の中で、ギリシャや EU に事業所を持たず、ギリシャや EU に顧客はいないと述べている。同社はまた、同社の製品がギリシャで使用されたことはなく、"GDPR の対象となるような活動も行っていない"と主張している。

6.7 ドイツ

●ドイツの新しい三党連立政権は 2021 年 11 月 24 日に明らかにされた合意事項の中で、欧州委員会による AI 規制案における、公共空間でのリモートの顔認識技術の利用や政府による自動的なスコアリングを禁止とする提案を支持することが明らかになった²⁴⁴。

7. オーストラリア・ニュージーランドの動向

7.1 オーストラリア

●2020 年 4 月、オーストラリアの大学による、コロナウイルス感染症のパンデミック中に、自宅で試験を受ける学生に対して、ソフトウェアを使ってウェブカメラで監視する計画に対して、抗議が起こっている²⁴⁵。オーストラリア国立大学 (ANU) は、米国ベースの Proctorio 社と契約を結んだことを明らかにした。クイーンズランド大学とシドニー大学は、同じく米国ベースの ProctorU 社と契約を結んだ。キャンベラ大学は業者を選定中とのこと。両者ともに、試験前に学生が写真 ID といった生体情報をアップロードする必要があり、機械学習や顔認識技術を使って、学生の個人確認と怪しい行為の発見を行うことになっている。Queensland 大学の医学部学生らから、ProctorU ソフトウェアによるプライバシー侵害を懸念する声が上がっていることが 2020 年 6 月 15 日、報じられた²⁴⁶。4 月には、学生組合が、在宅の学生を撮影し、パーソナルデ

²⁴³ <https://therecord.media/clearview-ai-fined-20-million-banned-from-processing-biometric-data-in-greece-after-gdpr-violations/>

²⁴⁴ <https://www.politico.eu/article/german-coalition-backs-ban-on-facial-recognition-in-public-places/>

²⁴⁵ <https://www.theguardian.com/australia-news/2020/apr/20/concerns-raised-australian-universities-plan-use-proctorio-proctoru-exam-monitoring-software>

²⁴⁶ <https://www.brisbanetimes.com.au/national/queensland/uq-students-complain-about-exam->

ータを第三者企業に保管・商品化されることは受け入れられないと主張していた²⁴⁷。

●[報告書]モナーシュ (Monash) 大学の研究者らによる「自動化社会作業グループ (Automated Society Working Group)」による報告書「顔認識技術に対するオーストラリア人の態度：全国調査」²⁴⁸が2020年5月に、Whitepaper #01として公表された。18歳以上のオーストラリア国民への全国調査が実施され、2291人から回答を得た。

調査対象者のほぼ半数(49%)が、公共の場での顔認識技術の使用はプライバシーの侵害にあたると感じており、3分の1以上(複数回答)が「顔認識技術の使用によるリスクはメリットを上回る」という意見に同意した一方、60%以上が「顔認識データベースからオプトアウトする権利を持つべき」と考えている。他方、61%の回答者が「公共安全のために有用なツールになる」とも回答している。

●7-Eleven Australia はすべての700店舗で顔認識技術を、顧客からのフィードバックを集めるために(のみ)採用すると報じられた²⁴⁹。「サイトは常時ビデオ監視下にあります。入店することにより、顔認識カメラがあなたの画像を撮影し、保存することに同意するものとします("Site is under constant video surveillance. By entering the store you consent to facial recognition cameras capturing and storing your image,")」という通知が出たことがtwitterなどで報告された²⁵⁰。利用目的は、万引きや詐欺の防止ではなく、顧客フィードバックとされている。ソフトウェアは、店舗に置かれたタブレット機器上で操作できるオンラインCX(消費者体験)計測ツールであるRate Itに接続される予定である²⁵¹。担当者によると、顧客がRate Itタブレットを使うときのみ、顔認識技術がアクティベートされるとのことである。その場合7日間保存される。そのため、使用しない顧客のデータは記録・保有されない。

●オーストラリアの情報コミッショナー局(OAIC)は、英国の情報コミッショナー局(ICO)とともに、Clearview社の個人情報の取り扱いについての共同捜査を開始したことを2020年7月

monitoring-software-20200615-p552qm.html

²⁴⁷ <https://www.brisbanetimes.com.au/national/queensland/uq-students-raise-privacy-concerns-over-third-party-exam-platform-20200419-p54177.html>

²⁴⁸ https://www.monash.edu/__data/assets/pdf_file/0011/2211599/Facial-Recognition-Whitepaper-Monash,-ASWG.pdf

²⁴⁹ <https://www.itnews.com.au/news/7-eleven-australia-deploys-facial-recognition-on-customer-feedback-tablets-549538>

²⁵⁰ <https://www.rt.com/news/492724-australian-7eleven-facial-recognition/>

²⁵¹ <https://techwireasia.com/2020/07/why-7-eleven-australia-is-using-facial-recognition-in-stores/>

9日、発表した²⁵²。

●連邦政府は数年前から、全国の規制当局が顔認証照合を行える全国規模の生体認証データベースの構築を計画しており、2019年7月に「ID-Matching Services 法案」を議会に提案した。オーストラリア政府評議会（COAG）の合意に基づき、データベースには各州から運転免許証の写真などの生体情報が提供され、当局による1対1および1対多数の顔認識マッチングに使用されることになった。しかし、同法案は、議会のインテリジェンス及び安全保障合同委員会（Parliamentary Joint Committee on Intelligence and Security PJCS）が「単なる修正ではなく、相当量の再策定が必要だ」として否決して以来、議会で中断している。

●オーストラリア人権委員会（Australian Human Rights Commission：AHRC）は2021年5月27日、38項目の勧告を含む「人権とテクノロジー」最終報告書を公表した²⁵³。Part Aが新規技術に関する国家戦略について、Part BがAIについて、Part Cが効果的な規制について、Part Dがアクセス可能な技術という構成で、Part Bの第9章「生体サーベイランス、顔認識、及びプライバシー」において顔認識技術が取り上げられている。勧告19では、オーストラリア（連邦・州・地方）政府は顔認識技術や他の生体認証技術の利用を規制する法律を導入すべきであるとした。続く勧告20では、勧告19で勧告した法律が導入されるまでは、オーストラリア（連邦・州・地方）政府は、個人に法的または同様に重要な効果をもたらす、または警察活動や法執行といった、人権に対して高いリスクがある意思決定における顔認識技術や他の生体認証技術の利用に対してモラトリアムを導入すべきであるとした。

●2021年8月末から、外国あるいはNSW州（シドニー）やVictoria州（メルボルン）から帰宅した人がホテルではなく自宅で隔離できるように、位置情報とライブでの顔認識チェックインを用いて居場所を確認するアプリ（Home Quarantine SA）の試行が南オーストラリア州で実施された²⁵⁴。うまくいけば海外からの帰国者にも適用されるという。毎日複数回ランダムな時間に通知があり、通知があると15分以内に位置情報とライブ顔認識チェックインを実施しなければならない。チェックインがない場合は電話がかかってくることになっている。また毎日、症状のチェックを実施する必要もある。

これに対して、オーストラリア人権委員会（AHRC）を含む様々な専門家や市民団体から、顔認

²⁵² <https://www.oaic.gov.au/updates/news-and-media/oaic-and-uks-ico-open-joint-investigation-into-clearview-ai-inc/>

²⁵³ <https://humanrights.gov.au/about/news/media-releases/australians-deserve-tech-protects-their-rights>

²⁵⁴ <https://www.abc.net.au/news/2021-08-23/home-quarantine-trial-in-south-australia/100398330>

識技術には、民族、肌の色、ジェンダーによる精度の差が存在する点や、顔画像等のデータのセキュリティ等について懸念も表明されている²⁵⁵。南オーストラリア州政府によると、アプリを通して取得された情報はすべてただちに暗号化され、セキュアなサーバに保管されるという。

●オーストラリア情報コミッショナー局（OAIC）が、英国情報コミッショナー局（ICO）とともに2020年7月に開始したCleaview AI社への合同調査が11月3日に終了した²⁵⁶。OAICは文書を発表し、オーストラリアのプライバシー原則（APP）の要件を満たしておらず、オーストラリア人のプライバシーを侵害していると指摘し、ウェブサイトからのオーストラリア人の写真の収集を中止し、すでに収集された写真は90日以内にすべて破棄し、書面での確認を提出することを求めた²⁵⁷。

●2022年1月17日付けのInnovationAusの記事によると、シドニー工科大学（University of Technology Sydney:UTS）が実施している顔認識技術のモデル法を提案するプロジェクトには、前人権コミッショナーのEd Santow氏も参加しており、年半ばには研究成果が政策立案者らに公表される予定であり、7月頃に法案が作成される予定であるという²⁵⁸。現在、オーストラリアには顔認識技術に関する法律は存在しないため、監督を欠いたまま様々な用途で利用されている。Santow氏らは、適切な監督が可能になるまで、オーストラリア全土での高いリスクのある利用（1対多の利用など）のモラトリアムを求めている²⁵⁹。

●オーストラリアの消費者団体であるCHOICEは2022年6月15日、オーストラリアの主要な小売りチェーンであるKmart（ホームセンター）、Bunnings（ホームセンター）、及びThe Good Guys（家電量販店）が、客にきちんと通知することなしに顔認識技術を利用していることを報じた²⁶⁰。プライバシーポリシーは見つけづらく、かつ、オンラインで確認してから店舗を尋ねる客はいない。KmartとBunningsは店舗の入り口に小さいポスターがあったものの、小さくて目立たず、ほとんどの買い物客が見過ごしてしまうようなものだった。Bunningsの最高執行役員は

²⁵⁵ <https://www.sbs.com.au/news/controversial-facial-recognition-technology-could-be-the-key-to-opening-australia-s-borders/5451e07c-47c4-41bd-a9b1-4a48b8e8aefc>

²⁵⁶ <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2021/11/clearview-statement/>

²⁵⁷ https://www.oaic.gov.au/_data/assets/pdf_file/0016/11284/Commissioner-initiated-investigation-into-Cleaview-AI,-Inc.-Privacy-2021-AICmr-54-14-October-2021.pdf

²⁵⁸ <https://www.innovationaus.com/ed-santow-leading-development-of-australian-facial-recognition-model-law/>

²⁵⁹ <https://www.innovationaus.com/experts-back-facial-recognition-moratorium/>

²⁶⁰ <https://www.choice.com.au/consumers-and-data/data-collection-and-use/how-your-data-is-used/articles/kmart-bunnings-and-the-good-guys-using-facial-recognition-technology-in-store>

「一部の店舗では、CCTV システムで顔認識技術を利用しています。この技術は、過去に店舗で問題となった事件に関与した人物を特定するのに役立っています」とコメントした。

CHOICE によると、Kmart と Bunnings が 7 月末、カメラの利用を一時的に「停止」したことを公表したという²⁶¹。The Good Guys はすでに使用を停止していた。CHOICE の指摘を受けて、OAIC も公式な調査を開始した。

●前述のシドニー工科大学のプロジェクトは 9 月末、報告書「顔認識技術：モデル法に向けて」を公表した²⁶²。モデル法は、顔認識技術のイノベーションを促進し、責任ある利用を可能にすると同時に、人権に対するリスクから保護することを目的としている。6.2 節の Figure 2 においてモデル法の鍵となる要素がまとめられている。法のスコープ、リスク評価アプローチ、あらゆる人権の制限に対する正当化、顔認識影響評価 (FRIA) アプローチ、法的要件 (ベースレベルとそれより少し高いレベルのリスク・アプリケーション)、高リスク顔認識アプリケーションのための法的要件、独立のレビュー、からなる。

7.2 ニューージーランド

●公的情報公開法 (Official Information Act) に基づいて公表された文書によると、内務省 (Department of Internal Affairs : DIA) が生体認証大手の米国の DXC Technology 社の子会社と契約 (master deal) を 2018 年 12 月に結び、多くの公共機関 (自動的に) や地方自治体 (オプトインで)、さらには民間企業 (承認を得て) までもが生体情報へアクセスできるようになるというものであることが明らかになったと 2020 年 10 月、報じられた²⁶³。DXC 社は NEC の Neoface ソフトウェアを採用している。また、プライバシー影響評価 (PIA) が閾値チェックとして 2020 年 1 月に作成・公表されている²⁶⁴。プロジェクト全体のリスクは中程度 (medium) と評価され、完全 PIA は必要ないと判断された。

●ニューージーランド法財団 (New Zealand Law Foundation) は 2020 年 11 月、Nessa Lynch 准

²⁶¹ <https://www.choice.com.au/consumers-and-data/data-collection-and-use/how-your-data-is-used/articles/facial-recognition-win>

²⁶² <https://www.uts.edu.au/partners-and-community/initiatives/social-justice-uts/centre-social-justice-inclusion/research-support/facial-recognition-technology-towards-model-law>

²⁶³ <https://www.rnz.co.nz/news/national/428103/government-facial-recognition-tech-deal-offers-wide-access>

²⁶⁴ <https://assets.documentcloud.org/documents/7224765/DIA-Privacy-Threshold-OIA-2021-0150-Oct-2020.pdf>

教授（ヴィクトリア大学ウェリントンの法学部）をリーダーとするプロジェクトの報告書「ニュージーランドにおける顔認識技術：法的及び倫理的枠組みに向けて」を公表した²⁶⁵。研究は、文献レビュー、課題ペーパー作成、ワークショップとパネルディスカッション、報告書執筆、ピアレビューと公表、の5段階で実施された。結論として15の勧告を行っている。

提言 1：個人情報に生体計測情報（biometric information）という新たなカテゴリーを設ける。

提言 2：個人情報に対するさらなるコントロール権限を個人に付与する。

提言 3：バイオメトリクス委員会などといった監督機構を設置する。

勧告 4：質の高いプライバシー影響評価（PIA）を実施する。

提言 5：アルゴリズム憲章（Algorithm Charter）に強制力と監督機能を追加する。

勧告 6：顔認識技術（FRT）の使用における透明性。

勧告 7：生体計測情報に対する行動規範（code of practice）を導入する。

勧告 8：顔画像の情報共有の合意は適切で透明性のあるものでなければならない。

提言 9：警察によるライブでの自動化顔認識（AFR）の利用を一時停止する。

勧告 10：立法のためのコンサルテーションと協議を実施する。

提言 11：警察による顔画像の収集・保管を見直す。

提言 12：警察の画像システムで比較できるようになるまでの閾値を設ける。

勧告 13：警察の画像データベースの監督を行う。

提言 14：顔認識技術（FRT）のような新興技術を監督する。

提言 15：公共の場での顔認識技術（FRT）による監視を規制する。

●2021年10月7日、プライバシー・コミッショナー局（OPC）は、プライバシー法がバイオメトリクスをどのように規制するかについての見解を示すポジションペーパーを公表した²⁶⁶。5.2

²⁶⁵ <https://www.lawfoundation.org.nz/?p=11497>

²⁶⁶ <https://www.privacy.org.nz/publications/guidance-resources/biometrics-and-privacy/>

節は「OPC は、バイオメトリクスを含むすべてのプロジェクトについて、プライバシー影響評価 (PIA) を実施することを期待する。」と題して、標準的な PIA の検討事項に加えて以下の質問にも答えることを勧告した。

- 生体情報の機微性 (sensitivity) は考慮されているか？
- 提案されているバイオメトリクスの使用は目的が絞られたものであり (targeted)、比例的であるか (proportionate) ？
- マオリ (Te Ao Māori) の視点は考慮されているか？
- 関連するステークホルダーと協議したか？
- バイオメトリクスの代替手段は提供されるか？
- バイオメトリクスの使用に関する透明性は、どのように提供されるか？
- どのような形で人間による監督が必要なのか？

2022 年 8 月中旬から OPC はこのポジションペーパーを見直し、「ニュージーランドにおけるバイオメトリクスのプライバシー規制」というコンサルテーションペーパーを作成し、広く一般に公開した。問い (Q) が 24 問並べられた。締め切りの 9 月 30 日までに個人、企業、政府機関、支援団体などから約 100 件の意見が集まり、2022 年末までに規制アプローチについて報告され、2023 年にさらなるガイダンスや規範が作成される予定である。

●ニュージーランド警察は、顔認識技術の警察による利用に関する独立の立場からのレビューを、法律を専門とする Lynch 氏と機械学習を専門とする Chen 氏に委託し、85 ページの報告書が 2021 年 12 月、公表された²⁶⁷。彼らは文献レビューとともに、関係者へのインタビューを行い、下記のような 10 の勧告を提示した。

勧告 1：ライブの自動化された顔認識技術のあらゆる検討の中断は継続すること

勧告 2：顔写真の収集と保持について再検討すること

²⁶⁷ <https://www.police.govt.nz/sites/default/files/publications/facial-recognition-technology-considerations-for-use-policing.pdf>

勧告 3：技術の倫理的な採用のためのプロセスの強化を継続すること

勧告 4：実装のガバナンスと監督を継続すること

勧告 5：マオリと協力して条約を支持する

勧告 6：透明性

勧告 7：公共の場所における監視についてのポリシーステートメント

勧告 8：第三者システムへのアクセスのためのガイドラインを施行すること

勧告 9：データを倫理的に使用する文化を組織内に埋め込むこと

勧告 10：進行中のホライズンスキニングのためのシステムを実践すること

8. その他の国の動向

8.1 ブラジル

●2018年8月、ブラジル消費者保護研究所（Brazilian Institute of Consumer Protection：IDEC）は、サンパウロの地下鉄運営会社である ViaQuatro に対して、米国の AdMobilize 社が開発したスマート広告システム（Digital Interactive Doors System）について²⁶⁸、集団の被害の補償を求めて提訴（public civil action）したという経緯がある²⁶⁹。当該技術は、広告パネルを見る行人の顔を検知し、「パーソナルデータを処理することなく」感情・性別・年齢を予測するとされた。これに対して、Access Now は、拒否できない公的空間において、行人の生体データを収集・処理しており、感情を予測する技術には科学的な基礎づけがなく、また性別も男女の二通りの区別のみであり性的少数者の権利を侵害していると主張した。2週間後に、判事は、ViaQuatro に

²⁶⁸ 2018年4月、サンパウロの地下鉄運営会社である ViaQuatro が、Line 4-Yellow platforms に、AdMobilize 社が開発した「デジタル・インタラクティブ・ドア」を導入することを発表した。<https://mobilidadesampa.com.br/2018/04/viaquatro-lanca-portas-interativas-digitais-nas-plataformas-da-linha-4-amarela/>（ポルトガル語）

²⁶⁹ <https://www.accessnow.org/data-for-sale-in-brazil/> 詳しくは https://www.accessnow.org/cms/assets/uploads/2020/06/Expert_Opinion_Brazil_Facial_Categorization.pdf

対して、データ収集を中止し、カメラを取り除くように要請した²⁷⁰。

●Access Now は 2020 年 6 月 23 日、IDEC vs. ViaQuatro の裁判に専門家意見を提出した²⁷¹。その中で、感情検出技術の科学的基礎づけが欠如している点や、性的少数者に対する、自動化された性別認識技術による体系的な加害について警告された。

●2021 年 5 月 7 日、サンパウロの裁判所は、民事訴訟において、サンパウロの地下鉄に顔認証プラットフォームを販売している民間会社 Via Quatro 社に対して、乗客の同意なしに、写真、音声、その他の個人データを取得することを禁ずる判決を出した²⁷²。

●2022 年 3 月 22 日、サンパウロ州裁判所が、サンパウロの地下鉄を運営する会社（メトロポリターノ・デ・サンパウロ社（METRO））に対して、顔認識技術の使用停止、すなわち顔認識用の生体データの取得と処理のプロセスを直ちに停止することを命じた²⁷³。さらに、地下鉄利用者の顔認識データを取得・処理できる新しい機器を展開することも停止させたという。また、この決定では、違反した場合、1 日当たりの罰金が設定された。これは、IDEC など、複数の人権団体が、特に黒人、ノンバイナリー、トランスの人々に対する差別のリスクを飛躍的に増大させることを指摘し、顔認識技術の使用禁止を求める民事訴訟を起こしたことを受けたもの²⁷⁴。

8.2 ウクライナ

●Clearview AI 社の CEO は 2022 年 3 月 11 日、Reuter 記者に対して、ウクライナの防衛省が Clearview AI 社の顔認識技術の使用を開始したことを伝えた²⁷⁵。ロシアのソーシャルメディアである VKontakte 内の顔データをデータベースに含んでいるため、ロシアの襲撃者を特定したり、死亡者の身元と特定したりできる。CEO である Hoan Ton-That 氏がキーフに支援のためのレターを政府関係者に送付したことがきっかけだという。ウクライナ国内において無料で利用可能となる。なお、ロシアには技術を提供していないという。

²⁷⁰ <https://idec.org.br/idec-na-imprensa/justica-determina-que-empresa-pare-de-coletar-dados-faciais-do-metro-em-sp>（ポルトガル語）

²⁷¹ <https://www.accessnow.org/data-for-sale-in-brazil/>

²⁷² <https://www.accessnow.org/sao-paulo-court-bans-facial-recognition-cameras-in-metro/>

²⁷³ <https://www.zdnet.com/article/sao-paulo-subway-ordered-to-suspend-use-of-facial-recognition/>

²⁷⁴ <https://www.zdnet.com/article/brazilian-civil-rights-organizations-call-for-facial-recognition-ban-in-sao-paulo-subway/>

²⁷⁵ <https://www.reuters.com/technology/exclusive-ukraine-has-started-using-clearview-ais-facial-recognition-during-war-2022-03-13/>

8.3 ロシア

●モスクワ市当局が、2020年の年内にモスクワ市の地下鉄に顔認証システムを導入することを、BBC ロシアが2020年7月、報じた²⁷⁶。「モスクワ地下鉄の全車両の4分の1にあたる約1500台の車両が同システムに接続され、各車両にそれぞれ8台のカメラが設置される。」とのこと。年末までに顔バイオメトリクスによる運賃支払いがすべての地下鉄で可能になるとされている²⁷⁷。生体情報を銀行に提出した個人は、改札か券売機前に現れると、銀行カードから引き落とされる。スマートフォンを使ったApple Payシステムが利用される。TASS通信によると、モスクワの地下鉄の顔認識システムによって、900人以上の容疑者が逮捕されたという²⁷⁸。

●モスクワの地下鉄では2021年5月、銀行カードと連動した顔認証改札システムであるFace Payの実証試験が行われた²⁷⁹。そんな中で、7月、モスクワ当局は、地下鉄の顔認識システムによって指名手配中の容疑者を221人発見したことを発表した²⁸⁰。

●Human Rights Watchは2021年9月15日、ロシア当局が、規制や監督、データ保護といった仕組みなしに、全国的に顔認識技術の利用を拡大し続けており、人権や自由への影響が懸念されることを報じた²⁸¹。モスクワ政府は顔認識に加えて「シルエット」認識を実用化しようとしている。

●モスクワの地下鉄の240以上の駅において、2021年10月15日から顔認証決済システムであるFace Payが開始された²⁸²。利用者はサービスを利用するために、モバイルアプリを通して、顔写真、銀行カード、地下鉄カードを連携させる必要がある。モスクワ当局は今後3年間で最大15%の乗客がFace Payを利用すると見込んでいる。乗客のデータは「セキュアに暗号化されて」データ処理センターに保管され、内務省スタッフだけがアクセスできるという。しかし、市民団体などは、警察や保安機関に利用される可能性を指摘している。実際、モスクワでは、17万5千台以上の監視カメラネットワークが構築され、顔認識技術が利用されており、デモ参加者の特定

²⁷⁶ <https://jp.sputniknews.com/science/202007227630616/>

²⁷⁷ <https://www.biometricupdate.com/202103/moscow-metro-to-introduce-facial-recognition-system-for-fare-payment>

²⁷⁸ <https://tass.com/society/1261721>

²⁷⁹ <https://jp.sputniknews.com/russia/202105148380677/>

²⁸⁰ <https://kod.ru/sistema-raspoznvaniya-lic-v-metro-moscow/>（ロシア語）

²⁸¹ <https://www.hrw.org/news/2021/09/15/russia-broad-facial-recognition-use-undermines-rights>

²⁸² <https://www.theguardian.com/world/2021/oct/15/privacy-fears-moscow-metro-rolls-out-facial-recognition-pay-system>

に使われた。

●2022年7月、ロシア国会は、銀行や国家機関が顧客の顔画像や音声サンプルなどの生体計測データを、生体計測データの中央データベースに入力することを義務付ける法律を採択した²⁸³。この法律は2023年3月に施行され、銀行が顧客のデータを渡す前に顧客の同意を求める必要はなくなる。生体データの中央データベースは2018年に作成された。ロシア当局は以前から、AI顔認証を使って、デモ参加者などの政府批判者を監視・訴追してきたが、今年2月のウクライナ侵攻以来、顔認識技術は、反戦デモを抑圧するための政府のツールの1つとなった。

8.4 アフガニスタン

●タリバンによる制圧によって、米軍とアフガニスタン政府が収集したアフガニスタン人の生体情報データベースがタリバンの手に渡ったのではないかと2021年に報道されている²⁸⁴。

8.5 中国

●香港の女子中学校（True Light College）ではオンライン授業に、4 Little Trees という名称の生徒の感情を認識するAIプログラムが使われていたという²⁸⁵。先生が生徒に対して、リアルタイムでの反応に対応できることで、よりインタラクティブに、かつ、パーソナライズドな教育を可能にすることを目的としていた。パンデミックの間に、4 Little Trees を利用する学校の数が34から83に増えたという。

●最高人民法院（最高裁）は2021年7月28日、商業目的の顔認証技術の使用に関する規定を公表し、ホテルや商店、駅などでの顔認証技術の使用は違法とし、アプリなどで使用する場合は消費者の同意を得よう求めるとともに、「同意しなければサービスを提供しない」という規定も違法とし、マンションの出入りに顔認証を使う場合は同意しない人のために代替手段を提供することを義務付けたという²⁸⁶。

●全国人民代表大会（全人代）常務委員会が、2021年8月20日に個人情報保護法を可決した。

²⁸³ <https://www.hrw.org/news/2022/07/23/russian-governments-advance-biometric-data>

²⁸⁴ <https://www.newsweekjapan.jp/stories/world/2021/09/post-97024.php>
<https://jp.reuters.com/article/afghanistan-conflict-tech-idJPKBN2FQ020> なお、最初に報じたのは、The Intercept である。<https://theintercept.com/2021/08/17/afghanistan-taliban-military-biometrics/>

²⁸⁵ <https://edition.cnn.com/2021/02/16/tech/emotion-recognition-ai-education-spc-intl-hnk/index.html>

²⁸⁶ <https://www.afpbb.com/articles/-/3362870>

2021年11月1日に施行される。同法は第26条で、「公共の場所で顔認証システムを導入する際は、政府当局の規定を満たした上でシステムの存在をはっきりと示し、集めた個人情報は公共安全を維持する目的以外に使用してはならない（本人の同意が得られた場合は、この限りではない）」と定めたとされる²⁸⁷。

8.6 インド

●インド国民的生体認証システム Aadhaar を監督する UIDAI（インド固有識別番号庁）の地域オフィスは2022年5月27日、ホテルや劇場ホールなどの「認可を受けていない民間団体」が、個人の指紋と網膜スキャンを結びつける12桁の固有番号である Aadhaar のコピーを収集・保管することは「許可されていない」とし、人々は悪用を防ぐために Aadhaar のコピーを共有しないよう警告した。しかしすでにホテル等に広く共有されていることから、広範な反発を招くことになり、警告は5月29日、撤回された²⁸⁸。

9. 国際機関の動向

●国際連合の Human Rights Council が、国連人権高等弁務官事務所（United Nations High Commissioner for Human Rights : OHCHR）に対して、ICTを含む新規技術の人権（特に平和的抗議を含む集会の自由）への影響に関する報告書の作成を依頼し、これに対する回答としての報告書を Michelle Bachelet 氏が2020年6月25日に公表した²⁸⁹。ICTを含む新規技術は、人権を促進するためにも利用可能であるが、インターネット切断等、人権を抑圧することにも利用可能であることを指摘したうえで、顔認識技術を含む監視技術を取りあげた。多数の勧告の中で、顔認識技術についても大きく取り上げられている。

(h)顔認識技術を集会に平和的に参加している者を識別するためにはけっして用いてはならない。

(i)もし参加者が重大な犯罪行為に従事している、または従事しようとする具体的な兆候がなく、記録が、必要・十分なセーフガード付きで、法によって行われるのでないならば、集会参加者の

²⁸⁷ <https://www.businessinsider.jp/post-242006>

²⁸⁸ <https://www.reuters.com/world/india/india-withdraws-warning-national-biometric-id-after-online-panic-2022-05-29/>

²⁸⁹ <https://news.un.org/en/story/2020/06/1067112>

映像を記録することを慎むべきである。

(j) 当局がプライバシーとデータ保護を遵守していることと、重大な正確性の問題や差別的影響がないことを示すことができ、以下の勧告(i から v)が実行されるまでは、平和的な集会における顔認識技術の利用に関してモラトリアムを設けるべきである。

(i) 顔認識技術デバイスを採用する前に、及び、採用されたツールの全ライフサイクルを通して人権デューデリジェンスを体系的に実施する。

(ii) 独立のデータ保護当局のような、顔認識技術の利用に対する、効果的で、独立で、不偏の監督メカニズムを確立し、集会での顔認識技術の利用について、独立組織による事前の認証の要件を課すことを検討する。

(iii) 顔テンプレートを含む個人データの収集、保持、解析、及び処理を規制する厳しいプライバシーとデータ保護法を整備する。

(iv) 情報を与えたうえでの一般人、専門家、市民社会とのコンサルテーションや、顔認識技術の購入、サプライヤーの名前、ツールの正確性に関する情報提供を通して、集会における画像記録と顔認識技術について透明性を確保する。

(v) 顔認識技術の調達や採用が民間企業による場合は、潜在的及び実際の人権への悪影響を特定し、予防し、軽減し、対応するために、当該事業者の人権デューデリジェンスを実施するよう要請し、特に、データの保護と差別がないことを、当該技術の設計段階と実施段階に組み込むことを確保する。

● 市民的自由組織の国際ネットワーク (International Network of Civil Liberties Organizations: INCLO) は 2021 年 1 月、報告書「顔認識技術のストーリーと権利：世界中からの害」を公表した²⁹⁰。顔認識技術と表現の自由、顔認識技術と平等と差別されない権利、顔認識技術と平和的集会と結社の自由の権利、顔認識技術とプライバシー権のそれぞれについて解説するとともに、該当する世界各国のケースが集められた。

● Privacy International が 2021 年 5 月、対テロという名目で生体情報が不透明な形で収集され、

²⁹⁰ プレスリリース <https://www.inclo.net/pdf/in-focus-facial-recognition-tech-stories-press-release.pdf> 報告書 <https://www.inclo.net/pdf/in-focus-facial-recognition-tech-stories.pdf>

利用されている実態に関する報告書を公表した²⁹¹。そこには、イラクとアフガニスタンで始まった米軍による生体情報データベース、イスラエル国家によるパレスチナ人の顔データの収集と監視、ソマリアにおける様々な国際的アクターによる生体情報の収集が地元住民にもたらす有害な影響、の3つのケーススタディが含まれている。各国政府や国際機関が、十分な法的保護や関連するリスクの慎重な検討なしに、テロと戦うための集中的で、かつ、相互運用可能なシステムの整備に向けて急いでいることに警鐘を鳴らした。

●Human Rights Watch (HRW) は2021年6月15日付のニュース記事で、国連難民高等弁務官事務所 (UNHCR) が、不適切にロヒンギャ難民の個人情報収集し、バングラデシュ政府と共有していたこと、そしてバングラデシュ政府がそれらをミャンマー政府と共有していたことを指摘した²⁹²。UNHCRは、自らのポリシー²⁹³が要求している、完全なデータ保護影響評価 (DPIA) を実施しておらず、難民に対してミャンマー政府とデータを共有することについてのインフォームドコンセントを得ていないケースもあったという。HRWは2020年9月から2021年3月にかけて、バングラデシュのコックスバザールでロヒンギャ難民24人にUNHCRへの登録体験についてインタビューし、ロヒンギャ登録を見学または参加した関係者20人に話を聞いた。

●Oxfamは2021年6月24日、人道目的で生体認証技術を利用する際の、7原則からなる新しい方針を発表した²⁹⁴。Oxfamは生体認証技術の利用について2015年に「モラトリアム」を開始した。2017年にはEngine Roomに、国際援助文脈における生体認証技術のリスクとベネフィットに関する研究を委託し、勧告を含む報告書が公開されている²⁹⁵。これはすでにある、Data Protection Policy と Responsible Data in Program Policy を補完するものとなる。7つの主要な原則は以下のとおりである。

1. 私たちは計画し、比例的であり、責任を持たなければならない。
2. 私たちは、個人と彼らのコミュニティに対してアカウントブルでなければならない。

²⁹¹ <https://privacyinternational.org/long-read/4528/biometrics-collection-under-pretext-counter-terrorism>

²⁹² <https://www.hrw.org/news/2021/06/15/un-shared-rohingya-data-without-informed-consent>

²⁹³ <https://www.refworld.org/docid/55643c1d4.html> 4.5節において、個人データの収集や処理、移転が「大規模」「繰り返し実施」「構造的 (データが複数主体で共有される等)」の場合に DPIA (データ保護影響評価) の実施が必要となるとされている。

²⁹⁴ <https://oxfam.app.box.com/v/OxfamBiometricPolicy>

²⁹⁵ <https://www.theengineroom.org/wp-content/uploads/2018/03/Engine-Room-Oxfam-Biometrics-Review.pdf>

3. 私たちは、個人と彼らのコミュニティとコントロールを共有しなければなりません。
4. 私たちは、個人と彼らのコミュニティへのリスクに対処しなければなりません。
5. 私たちは、セキュリティ・リスクに対処しなければなりません。
6. 私たちは、責任あるバイオメトリクスの実践をしなければなりません。
7. 第三者との関係を明確にし、コントロールしなければなりません。

●国連人権高等弁務官（OHCHR）である Michelle Bachelet 氏は 2021 年 9 月 15 日、記者会見を行い、人権へ重大なリスクを及ぼす AI システムの販売と使用に対して十分な安全策が講じられるまでモラトリアムをもうける必要性を強調し、国際的な人権法に違反する AI 応用の禁止を要求した²⁹⁶。同時に報告書を公表した。

勧告 (d)では、公的空間における遠隔での生体認識技術の利用について、少なくとも責任を持つ当局がプライバシーとデータ保護基準を遵守し、重大な正確性の問題や差別的な影響がないことを示すことができるまで、及び、顔認識技術に言及した 2020 年の報告書 (A/HRC/44/24) の 53 節(J)²⁹⁷で挙げたすべての勧告が実施されるまでは、モラトリアムを課すことを勧告した。また、国家と企業への勧告の(a)では、「設計、開発、展開、販売、取得、または運用する AI システムのライフサイクル全体を通じて、人権デューデリジェンスを体系的に実施すること。人権デューデリジェンスの重要な要素は、定期的で包括的な人権影響評価（human rights impact assessments）であるべきだ。」と書かれている。

●世界経済フォーラム（WEF）は、法執行機関による顔認識技術（FRT）の責任ある利用について、インターポール（INTERPOL）と、国連地域間犯罪司法研究所（UNICRI）、オランダ警察とともに 2021 年 10 月、いくつかのユースケースをもとに、政策枠組みを提案する報告書（ホワイトペーパー）を公表した。政策枠組みは 2 つの要素、すなわち、原則リストと自己評価アンケートからなる。多様なステークホルダーによる参加を通して形成された。今後はオランダ警察等において実施されるパイロットフェーズに移る。原則は以下の 9 点からなり、自己評価アンケートは各原則に複数の質問項目が用意されている。1) 人権および基本的人権の尊重、2) 必要かつ比例的な使用、3) 透明性の確保、4) 人間の監視とアカウントビリティ、5) システムパフォーマンス、6) リスク軽減のための戦略、7) 顔検査担当者の訓練、8) プローブ画像と参照デ

²⁹⁶ <https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=27469&LangID=E>

²⁹⁷ <https://undocs.org/A/HRC/44/24>

データベースの使用、9) 画像とメタデータの整合性、である。

●国連のテロ対策委員会執行事務局（Counter-terrorism Committee Executive Directorate : CTED)は2021年12月21日、Analytical Briefとして「バイオメトリクスと対テロ」と題するレポートを公表した²⁹⁸。CTEDの加盟国193か国との対話により、対テロ活動におけるバイオメトリクスの利用には大きな地域差があること、すなわち、欧州加盟国の約半数で広く利用されているが、中東ではごくわずかしき導入されておらず、アフリカの加盟国の半数以上は、まだバイオメトリクスを全く導入していないことが分かった。

●2022年10月にトルコのイスタンブールで開催された第44回世界プライバシー会議（GPA）において、「顔認識技術における個人情報の適切な利用に関する原則及び期待」に係る決議案が採択された²⁹⁹。民間部門と公的部門のあらゆる利用に適用される。原則は6つの大項目（①法的根拠、②合理性・必要性・比例性、③人権の保護、④透明性、⑤責任、⑥データ保護原則）で構成される。

²⁹⁸ <https://www.un.org/securitycouncil/ctc/content/cted-analytical-brief-biometrics-and-counter-terrorism>

²⁹⁹ 2022年11月16日に開催された第224回個人情報保護委員会において決議の仮訳も含めて紹介された。<https://www.ppc.go.jp/aboutus/minutes/2022/20221116/>

ELSI NOTE No. 25

生体認証技術の ELSI に関するグローバル動向
2020 年 4 月～2022 年 11 月

令和 4 年 12 月 27 日



大阪大学 社会技術共創研究センター
Research Center on Ethical, Legal and Social Issues

〒565-0871 大阪府吹田市山田丘 2-8
大阪大学吹田キャンパステクノアライアンス C 棟 6 階
TEL 06-6105-6084
<https://elsi.osaka-u.ac.jp>

 大阪大学

Osaka University
Research Center on
Ethical, Legal and
Social Issues