科学技術に関する調査プロジェクト 2018 報告書

生体認証技術の動向と活用

2019 年 3 月

国 立 国 会 図 書 館
調査及び立法考査局

科学技術に関する調査プロジェクト2018報告書
生体認証技術の動向と活用

生体認証技術は、ビッグデータの活用と機械学習の導入により、顔認識技術を中心に実用化が急速に進んでいる。スマホやパソコンのロック解除や空港での本人確認ですでに便利さを経験した人も増え、東京 2020 オリンピック･パラリンピック競技大会でも採用される予定になっている。パスワードや鍵は忘れたり失くしたりしがちであるが、生体認証はそのようなリスクはないため、私たちの生活を便利なものにしていることは確かである。しかし、パスワードや鍵は他者に知られたり複製されたりすれば、別のものに変えればよいが、生体情報を変えることは極めて困難である。そのため、悪用や漏洩があった場合の潜在的被害は大きい。DNA 型や指紋情報といった生体情報は厳格に管理することは可能であり、そうすべきであるが、日常生活で露出される顔や歩容については隠すことが困難であり、厳格な管理は難しい。生体認証技術の利用に伴うリスクをできるだけ小さくしつつ、潜在的に持つ利益を最大限享受できるような社会の仕組みを構築することは、喫緊の課題である。

本報告書では、生体認証技術の急速な発展と普及の状況について、技術面、応用面、ガバナンス面から最先端の動向をまとめたものである。本報告書で取り上げた全ての国で、技術の急速な発展と社会における普及に対して、法規制や社会制度が十分に追いついておらず、議論の真っただ中にあることが分かるだろう。警察や出入国管理といった法執行機関、航空会社や空港、商業施設、国際援助団体、場合によっては教育機関までもが生体認証技術をすでに活用していたり、試行を開始したりしている一方で、プライバシー、人権、市民の自由などを擁護する市民団体からは、法規制の不備、監督メカニズムの欠如、萎縮効果の可能性など様々な問題点が指摘されている。技術を活用する側においても、新しい技術の社会実装に際して、法規制の整備、監督機関の設置、行動規範やガイドラインの作成、リスク評価の実施、第三者機関によるチェック、マルチステークホルダープロセスなど、様々な対応が試行錯誤されている。諸外国の試行錯誤の経験からは、日本において生体認証技術をどのように進めて行くかを検討する上で様々なヒントが得られるであろう。日本では本報告書で取り上げた諸外国ほどには、まだ社会的な議論が盛り上がっていないように見える。しかし、何も対応をしないと、私たちが生体認証技術による利益を十分に享受する前にリスクが過大視されてしまい、技術そのものにブレーキがかけられてしまうかもしれない。

本報告書は技術的な側面に焦点を当てた第 1 部と、社会面に焦点を当てた第 2 部から第 4 部までから成る。筆者らは、大学内のいくつかの場所に実験用カメラを設置し、取得した画像を研究用に用いるというプロジェクトを実施する中で、協働して適正な手順を模索した情報技術者と人文社会科学者から成るグループである。生体認証技術を社会実装していくためにも、日本社会全体で、情報技術と人文社会科学の協働が求められる。

大阪大学データビリティフロンティア機構　教授　岸本（きしもと）　充生（あつお）

要　　約

生体認証（「バイオメトリクス」と呼ばれる。）とは、人の身体的な特性・特徴や行動的な特性・特徴に基づいて、その人物を自動的に確認・識別することであり、その技術を生体認証技術という。生体認証には様々なモダリティ（様式、分類）が提案・研究・活用されているが、それらは身体的なもの（指紋、DNA、虹彩、静脈、顔等）と行動的なもの（歩容、署名等）に分けることができる。また、生体認証には大きく2つの使い方があり、同一性を確認する一対一認証（確認）と呼ばれるものと、あらかじめ用意されたデータベースの中から類似したものを見つける一対多認証（識別）と呼ばれるものである。前者の本人確認は、身分証、鍵、パスワードといった現在用いられている本人確認のための手段に代わるものとして生体情報を用いるものである。後者は、犯罪捜査、万引き防止、顧客サービスなどに利用されている。生体認証の結果は、あらかじめ決めておいたしきい値に基づき、本人誤拒否率（FRR）と他人誤受入率（FAR）によって評価されるが、両者はしきい値によって変化し、かつトレードオフの関係にあり、片方を下げると片方が上がる。

生体認証技術の中でも、コンピュータビジョンやパターン認識の技術に基づく顔認識技術については、近年、大量の学習データと機械学習の導入により、精度が飛躍的に進歩しており、また、顔画像からはそれが誰であるかだけではなく、性別や年齢層の推定、表情による感情や意図の推定、健康情報の推定など、多岐にわたる研究がなされ、それらのうちのいくつかは既に社会実装されている。生体認証技術は、あらゆる技術と同様、様々な新しいことを可能とする一方で、使い方によっては新たなリスクを生み出すことが指摘されている。生体認証技術、特に顔認識技術の急速な発展と普及に対して、世界各国で、既存の法規制はどこまで対応可能か、社会としてどのようなルールを策定すべきか、どのような監督体制（ガバナンス枠組み）を用意すべきか、といった議論が続いている。米国では、生体情報の取得や利用を規制する連邦法がない中で、法執行機関による国境管理目的での利用が先行している。イングランドとウェールズでは、警察が大きなイベントで監視カメラから得られたライブ映像に顔認識技術を適用する試みを繰り返している。スコットランドは、顔認識技術のガバナンス枠組みを確立しようとしている。オーストラリアは、連邦政府と州政府が顔写真データベースの共有に合意した。EU では、生体情報は明示的にセンシティブデータに含まれ、生体認証が普及していない反面、移民の流入に対する国境管理において生体情報を利用する動きがある。インドでは、世界最大規模の国民 ID システムに生体情報を含める試みが始まっている。国際援助の文脈では、国連機関が生体認証技術の利用を推進している反面、生体認証技術を使用しないことを決めた人道支援団体もある。

日本では個人情報保護法において生体情報は「個人識別符号」とされ、個人情報の１つであることが明記された。生体情報を取り扱う場合は、個人情報取扱事業者としての義務が生じる。生体認証技術の利用に際しては、個人情報保護法の遵守に加えて、プライバシーの保護や萎縮効果の防止のために、業界団体や学会によるガイドライン策定といった、自主的な社会的及び倫理的取組が始まりつつある。

Summary

Biometrics are used to verify and automatically identify a person based on their physiological or behavioral characteristics. Various modalities have been proposed, researched, and utilized as biometrics: they can be divided into 1) physiological biometrics, such as fingerprints, DNA, iris measurements, as well as vein and face characteristics, and 2) behavioral biometrics, such as gait and handwriting. Biometrics have mainly been used in two ways. One is called one-to-one verification, which verifies an individual's identity. The other is called one-to-N identification, which finds the most approximate individual out of a prepared database. The former, verification, uses biometrics as a surrogate for the tools currently used to confirm identity, such as ID cards, keys, or passwords. The latter, identification, is used for criminal investigation, prevention of shoplifting, as well as by customer service. The performance of biometrics is usually defined by the method's false acceptance rate (FAR) and false rejection rate (FRR) using a predetermined threshold. Both FAR and FRR are dependent on the given threshold level, which means there is a trade-off between them. If one is lowered, the other increases.

Among biometrics, facial recognition technology based on computer vision and pattern recognition has progressed dramatically with the introduction of big data and machine learning, which enable us not only to know who an individual is and to estimate their age and sex, but also to infer emotions and intent from facial expressions and to diagnose potential disorders based on facial images. Some of those functions have already been deployed in the real world. The field of biometrics, like other emerging technologies, brings us new experiences, while it has been pointed out that it can also bring about emerging risks depending on how the biometrics are used.

In the face of rapid progress and the prevalence of biometrics, particularly facial recognition technology, many countries have started or continued discussions regarding to what extent existing laws and regulations can apply, how to regulate biometrics, and what the best governance framework is. In the United States, law enforcement organizations have already applied biometrics to border management in the absence of comprehensive federal laws regulating acquisition and usage of biometrics. In England and Wales, the police department has repeatedly run trials of live facial scans using surveillance cameras at large events, such as festivals and concerts. Scotland is in the process of establishing a governance framework for facial recognition technology. In Australia, the federal and state governments have agreed to share their facial photo databases. In the EU, biometrics have not been prevalent compared to their usage in other developed countries, since biometric data have been explicitly designated as sensitive data in the General Data Protection Regulation. India has begun to incorporate biometrics into the largest national ID system in the world. In the context of international aid, UN agencies promote the use of biometrics, while some nongovernmental organizations have decided not to use them for fear of data leaks.

In Japan, biometric data are classified as "individual identification codes," one form of personal information in the Amended Act on the Protection of Personal Information. Those who work with biometric data must carry out the obligations specified in the law for "Personal Information-Handling Business Operators." In addition to complying with the law, business and academic organizations have already embarked on an effort to prepare voluntary guidelines in order to protect privacy and prevent possible chilling effects.

生体認証技術の動向と活用
目　次

Current Trends in Biometrics
Contents