個人情報保護委員会事務局　御中

個人識別符号に関する海外・国内動向の調査研究
報告書

2018 年 3 月

株式会社三菱総合研究所
社会 ICT イノベーション本部

目 次

1. 個人識別符号とは 1

1.1 法的定義 1
1.1.1 個人情報保護法における定義 1
1.1.2 海外における定義例 4
1.2 個人識別符号の利用例 7

2. 海外における法制度の状況及び利用例 9

2.1 海外における法制度の全体動向 9
2.2 海外における利用例 12

3. 各国の法制度の状況 15

3.1 米国 15
3.1.1 生体情報・DNA 15
3.1.2 ID 19
3.2 カナダ 23
3.2.1 生体情報 23
3.2.2 ID 26
3.3 シンガポール 27
3.3.1 PDPA 27
3.3.2 PDPA における個人情報の定義とその他の規定 27
3.4 欧州連合（EU） 30
3.4.1 GDPR における定義と規制の概要 30
3.4.2 経緯 35
3.5 EU 加盟国 42
3.6 小括・補足 48

4. 利用動向・技術動向 50

4.1 現在の主な利用事例 50
4.1.1 全体動向 50
4.1.2 事例 51
4.1.3 海外における利用動向の整理例 53
4.2 技術･標準化の動向 55
4.2.1 生体情報の特徴及び比較 55
4.2.2 新用途が期待される生体認証技術の開発 57
4.2.3 標準化動向 62
4.3 生体認証の現状及び今後の利用動向 65
4.3.1 生体認証の現状及び今後の動向 65
4.3.2 今後の動向に関するトレンド 66
4.3.3 市場の展望 68

本調査研究の目的

平成 29 年 5 月 30 日に全面施行された改正個人情報保護法（以下「法」という。）において、個人識別符号が定義されたことにより、個人情報の定義がより明確化された。具体的には、法第２条第２項において、「特定の個人の身体の一部の特徴を電子計算機の用に供するために変換した文字、番号、記号その他の符号であって、当該特定の個人を識別することができるもの」（第１号）及び「個人に提供される役務の利用若しくは個人に販売される商品の購入に関し割り当てられ、又は個人に発行されるカードその他の書類に記載され、若しくは電磁的方式により記録された文字、番号、記号その他の符号であって、その利用者若しくは購入者又は発行を受ける者ごとに異なるものとなるように割り当てられ、又は記載され、若しくは記録されることにより、特定の利用者若しくは購入者又は発行を受ける者を識別することができるもの」（第２号）のうちいずれかに該当する文字、番号、記号その他の符号のうち、政令で定めるものが個人識別符号であると定義された。

本調査は、特定の身体の特徴に関する情報等を活用した生体認証等に関する諸外国における制度的対応状況及び利用動向・技術動向について、事実関係を文献調査及びヒアリングに基づきとりまとめたものである。

1. 個人識別符号とは

本調査研究において「個人識別符号」が意味する範囲と、その法的定義について示す。

1.1 法的定義

最初に、個人識別符号の法的定義について整理する。

1.1.1 個人情報保護法における定義

本調査研究では、法第第 2 条第 2 項の分類に従い、

- 「特定の個人の身体の一部の特徴を電子計算機の用に供するために変換した文字、番号、記号その他の符号であって、当該特定の個人を識別することができるもの」（第 1 号）
- 「個人に提供される役務の利用若しくは個人に販売される商品の購入に関し割り当てられ、又は個人に発行されるカードその他の書類に記載され、若しくは電磁的方式により記録された文字、番号、記号その他の符号であって、その利用者若しくは購入者又は発行を受ける者ごとに異なるものとなるように割り当てられ、又は記載され、若しくは記録されることにより、特定の利用者若しくは購入者又は発行を受ける者を識別することができるもの」（同第 2 号）

を対象とする。

以下に、個人情報の保護に関する法律（平成 15 年法律第 57 号）および政令における定義を示す。

【法第 2 条第 2 項】[1]

> 第 2 条
> 2　この法律において**「個人識別符号」**とは、次の各号のいずれかに該当する**文字、番号、記号その他の符号**のうち、政令で定めるものをいう。
> 一　特定の個人の身体の一部の特徴を電子計算機の用に供するために変換した文字、番号、記号その他の符号であって、当該特定の個人を識別することができるもの
> 二　個人に提供される役務の利用若しくは個人に販売される商品の購入に関し割り当てられ、又は個人に発行されるカードその他の書類に記載され、若しくは電磁的方式により記録された文字、番号、記号その他の符号であって、その利用者若しくは購入者又は発行を受ける者ごとに異なるものとなるように割り当てられ、又は記載され、若しくは記録されることにより、特定の利用者若しくは購入者又は発行を受ける者を識別することができるもの

注：下線は本報告書による

[1] https://www.ppc.go.jp/files/pdf/290530_personal_law.pdf

【政令第１条】[2]

（個人識別符号）
第１条 個人情報の保護に関する法律（以下「法」という。）第２条第２項の政令で定める文字、番号、記号その他の符号は、次に掲げるものとする。
一　次に掲げる身体の特徴のいずれかを電子計算機の用に供するために変換した文字、番号、記号その他の符号であって、特定の個人を識別するに足りるものとして個人情報保護委員会規則で定める基準に適合するもの
イ　細胞から採取されたデオキシリボ核酸（別名ＤＮＡ）を構成する塩基の配列
ロ　顔の骨格及び皮膚の色並びに目、鼻、口その他の顔の部位の位置及び形状によって定まる容貌
ハ　虹彩の表面の起伏により形成される線状の模様
ニ　発声の際の声帯の振動、声門の開閉並びに声道の形状及びその変化
ホ　歩行の際の姿勢及び両腕の動作、歩幅その他の歩行の態様
ヘ　手のひら又は手の甲若しくは指の皮下の静脈の分岐及び端点によって定まるその静脈の形状
ト　指紋又は掌紋
二　旅券法（昭和 26 年法律第 267 号）第６条第１項第１号の旅券の番号
三　国民年金法（昭和 34 年法律第 141 号）第 14 条に規定する基礎年金番号
四　道路交通法（昭和 35 年法律第 105 号）第 93 条第１項第１号の免許証の番号
五　住民基本台帳法（昭和 42 年法律第 81 号）第７条第 13 号に規定する住民票コード
六　行政手続における特定の個人を識別するための番号の利用等に関する法律（平成 25 年法律第 27 号）第２条第５項に規定する個人番号
七　次に掲げる証明書にその発行を受ける者ごとに異なるものとなるように記載された個人情報保護委員会規則で定める文字、番号、記号その他の符号
イ　国民健康保険法（昭和 33 年法律第 192 号）第９条第２項の被保険者証
ロ　高齢者の医療の確保に関する法律（昭和 57 年法律第 80 号）第 54 条第３項の被保険者証
ハ　介護保険法（平成９年法律第 123 号）第 12 条第３項の被保険者証
八　その他前各号に準ずるものとして個人情報保護委員会規則で定める文字、番号、記号その他の符号

法第 2 条第 2 項第 1 号が政令第 1 条第 1 号（イ～ト）で示され、法第 2 条第 2 項第 2 号が政令第 1 条第 2 号～第 8 号にて示されている。

なお、政令第 1 条第 1 号（DNA の塩基配列及び生体情報）に関しては、「個人情報の保護に関する法律についてのガイドライン（通則編）」[3]において、以下のように示されている。

[2] https://www.ppc.go.jp/files/pdf/290530_personal_cabinetorder.pdf
[3] https://www.ppc.go.jp/files/pdf/guidelines01.pdf

表 1-1　個人識別符号（第１号）のガイドライン（通則編）における説明

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

出所：政令及び委員会規則より作成

1.1.2 海外における定義例

次に、海外における法的定義の例を示す。

(1) 欧州連合（EU）における定義

欧州連合（EU）の一般データ保護規則（General Data Protection Regulation: GDPR）では、第 4 条（定義）において、「個人データ」「遺伝データ」「生体データ」「健康に関するデータ」の定義が示されており、それぞれ以下のとおりである[4]。

(1) 「個人データ」とは、識別された又は識別され得る自然人（以下「データ主体」という。）に関するあらゆる情報を意味する。識別され得る自然人は、特に、氏名、識別番号、位置データ、オンライン識別子のような識別子、又は当該自然人に関する物理的、生理的、遺伝子的、精神的、経済的、文化的若しくは社会的アイデンティティに特有な一つ若しくは複数の要素を参照することによって、直接的に又は間接的に、識別され得る者をいう。

(1) 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

(13) 「遺伝データ」とは、自然人の生理機能又は健康に関する固有の情報を与え、特に当該自然人からの生物的サンプルの分析から得られる、継承又は獲得した自然人の遺伝的特性に関わる個人データをいう。

(13) 'genetic data' means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;

(14) 「生体データ」とは、顔画像又は指紋確証データのように、当該自然人に特有の識別性を認められる又は確かめられる、自然人の身体的、生理的又は行動的特性に関する特定の技術的処理から得られる個人データをいう。

(14) 'biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

(15) 「健康に関するデータ」とは、医療サービスへの提供状況を含む健康状態について

[4] 和訳は一般財団法人日本情報経済社会推進協会による仮日本語訳（2016 年 8 月）。以下、本報告書で GDPR の条文の和訳を示す際は、この訳を用いる。https://www.jipdec.or.jp/archives/publications/J0005075

の情報を明らかにする自然人の身体的又は精神的な健康に関する個人データをいう。

(15) 'data concerning health' means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;

「遺伝データ」「生体データ」「健康に関するデータ」のいずれについても、具体的な列挙を行わない形で定義を行っている（生体データについての詳細は 3.4.1 節にて後述）。

(2) 米国における定義（州法）

米国では、連邦法においては生体情報を直接規定していない。他方、いくつかの州法（詳細は 3.1.1 節(3)にて後述）では生体情報を直接規定しているものがある。ここではそれらの嚆矢となったイリノイ州の生体情報プライバシー法（Biometric Information Privacy Act: BIPA）[5]の定義を示す。以下に示すとおり、生体情報（ここでは個人を識別するための生体情報として「生体識別子」とされている）が具体的に列挙され、かつ該当しないケースも詳細に示されている。前述の GDPR の場合と比べてこの定義内容は対照的である。

なお、日本では静脈（手のひら又は手の甲若しくは指の皮下の静脈）や歩容が定義に含まれているが、この BIPA の定義にはいずれも含まれていない。BIPA の制定は後述するように 2008 年であるが、具体的に列挙する形で直接定義する場合、生体認証技術の進歩に応じて随時法改正を行う必要が生じる。

第 10 条　定義

「生体認証識別子」とは、網膜または虹彩のスキャン、指紋、声紋、手または顔の幾何学的配置のスキャンを意味する。生体認証識別子には筆跡、署名、写真、有効な科学的試験またはスクリーニングに用いる生体サンプル、人口統計データ、刺青、身長、体重、髪の色、眼の色などの身体的特徴は含まれない。また、イリノイ臓器移植法により定義された移植された臓器、人体組織、器官や、（略）血液、血清は生体認証識別子に含まれない。遺伝情報保護法により規制される生物学的物質は生体認証識別子に含まれない。医療保険の携行性と責任に関する 1996 年法（HIPPA）に従い、ヘルスケアにおいて取得、収集、蓄積される情報は生体認証識別子に含まれない。X 線、レントゲン、CT、MRI、PET スキャン、マンモグラフィ、その他疾病等の診断、予測、治療や科学的試験・スクリーニングの有効性を高めるために用いられる人体に関する画像またはフィルムは、生体認証識別子に含まれない。

Sec. 10. Definitions. In this Act:

"Biometric identifier" means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry. Biometric identifiers do not include writing samples, written signatures, photographs, human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions, or physical descriptions such as height, weight, hair color, or eye color. Biometric identifiers do not include donated organs, tissues, or parts as defined in the Illinois Anatomical

[5] 原文は http://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57

Gift Act or blood or serum stored on behalf of recipients or potential recipients of living or cadaveric transplants and obtained or stored by a federally designated organ procurement agency. Biometric identifiers do not include biological materials regulated under the Genetic Information Privacy Act. Biometric identifiers do not include information captured from a patient in a health care setting or information collected, used, or stored for health care treatment, payment, or operations under the federal Health Insurance Portability and Accountability Act of 1996. Biometric identifiers do not include an X-ray, roentgen process, computed tomography, MRI, PET scan, mammography, or other image or film of the human anatomy used to diagnose, prognose, or treat an illness or other medical condition or to further validate scientific testing or screening.

注：下線は本報告書による

(3) 米国における定義（連邦法案）

成立には至ってないが、連邦法案において生体情報を規定したものがある。

Consumer Privacy Protection Act of 2015（2015 年消費者プライバシー保護法案）[6]は、センシティブな個人情報（sensitive personal information）のプライバシーおよびセキュリティ強化、ID 窃盗の防止、センシティブな個人情報に関するセキュリティ侵害の通知、法執行の強化、その他個人情報への不正アクセスや悪用等への対策を目的として提案された。

同法案では、生体情報については第 3 条(10)項(D)号にて、「センシティブな個人識別情報」のうちの「一意な生体情報」として規定している。この定義では具体的な列挙に加えて「その他の一意な身体的特徴」が追加されており、その点で前掲の BIPA とは異なる。

第 3 条　定義

本法では以下の定義を適用する。

(10)センシティブな個人識別情報

「センシティブな個人識別情報」とは、下記を含む、電子的またはデジタル形式の情報または情報を編集したものを意味する。

(D) 一意な生体データ、すなわち顔画像、指紋、声紋、瞳または虹彩の画像、またはその他の一意な身体的特徴

SEC. 3. DEFINITIONS.

In this Act, the following definitions shall apply:

(10) SENSITIVE PERSONALLY IDENTIFIABLE INFORMATION.—The term “sensitive personally identifiable information” means any information or compilation of information, in electronic or digital form that includes the following:

(D) Unique biometric data, such as faceprint, fingerprint, voice print, a retina or iris image, or any other unique physical representation.

注：下線は本報告書による

[6] 2015 年 4 月に上院に、同 7 月に下院に、それぞれ提出されているが、最終ステータスは委員会に回送された状態となっている。https://www.congress.gov/bill/114th-congress/senate-bill/1158/
https://www.congress.gov/bill/114th-congress/house-bill/2977

1.2 個人識別符号の利用例

具体的な利用例は以下のとおりである。なお、これらは代表的な利用例、または近い未来に実用化が期待される利用例を示したものであり、これらに限られるものではない。利用分野・用途については第 4 章で後述する。

表 1-2　個人識別符号の利用例

分類	個人識別符号	利用例（個人認証）	利用例（その他）
特定の身体の特徴に関する情報等を活用した生体認証等	顔	●顔画像による本人認証（例：機器のログオン、入場管理・アクセス権限管理、旅券、等）	●顔画像検出・蓄積（例：カメラ画像や SNS 投稿画像からの顔画像検出・蓄積、個人特定、セグメント判別等）
	虹彩	●虹彩による本人認証（例：機器のログオン、入場管理・アクセス権限管理、出入国管理、等）	●捜査機関による、虹彩の照合による個人の特定・検出
	声紋	●本人認証（例：音声入力での認証）	●登録されている声紋との照合による個人の特定・検出
	歩容	●歩容による本人認証（例：入場管理）	●本人特定（例：カメラ画像から歩容を用いて個人を特定・検出（例えば監視カメラに映った侵入者・逃走者の捜査等）） ●セグメント判別（例：カメラ画像を用いた歩行者・来場者の性別や年齢の分析）
	静脈	●静脈（手のひら、手の甲、指先等）の静脈パターンを用いた本人認証（例：金融機関 ATM、入退室管理、施設チェックイン、勤怠管理、等）	●ー
	指紋・掌紋	●指紋や掌紋を用いた本人認証（例：機器のログオン、サービスへのログイン、入場管理・アクセ	●登録されている指紋・掌紋との照合による個人の特定・検出（例：犯罪者、出入国履歴等）

分類	個人識別符号	利用例（個人認証）	利用例（その他）
		ス権限管理、旅券、等）	
	DNA（ゲノム情報）	●DNA 鑑定･照合による本人確認（例：法医学、犯罪捜査、等）	●ゲノム情報を用いた、体質、疾病罹患リスク、遺伝的特質等の分析・推測・判定等
特定の利用者に割り当てられる ID 等	公的 ID[*1]	●サービス等利用時の本人認証（例：職員証を兼ねるマイナンバーカード、等）	●ー

*1　例：マイナンバー/国民 ID、旅券番号、等

2. 海外における法制度の状況及び利用例

ここでは、海外における個人識別符号に関する法制度の全体的な状況及び利用動向を整理する。

2.1 海外における法制度の全体動向

個人識別符号に関する海外の法制度の全体像を以下に示す。

表 2-1　個人識別符号に関する海外の法制度の全体像

国・地域	生体情報	DNA	ID 等
米国	【連邦法】 ・明文規定なし。 【ガイドライン等】 ・FTC が顔画像認識を消費者向けサービスで使用する際の消費者保護に関するベストプラクティスを公表。 ・NTIA も顔画像認識の商用利用に関するベストプラクティスを公表。 【州法】 ・イリノイ州、テキサス州、ワシントン州の 3 州において生体情報保護に関する州法が成立。他の 8 州では法案提出されるも不成立。	【連邦法】 ・遺伝情報差別禁止法（Genetic Information Nondiscrimination Act: GINA） 【州法】 ・イリノイ州は遺伝情報プライバシー法を制定。	【連邦法】 ・1974 年プライバシー法にて、連邦政府が保有する個人特定可能な情報（Personal Identifiable Information: PII）を規定。 ・HIPPA（医療保険の携行性と責任に関する法律）にて個人が特定可能な保健情報の取扱いを規定 【ガイドライン等】 ・労働省（DOL）は職員及び取引事業者が PII 保護に関して守るべきガイダンスを規定。 ・NIST（標準化機関）が PII の定義を公表。 【州法】 ・カリフォルニア州はセキュリティ侵害通知法にて PII の取扱いを規定。
カナダ	【連邦法】 ・明文規定なし 【ガイドライン等】 ・OPC が、生体情報が個人情報に当たることを認めている（ただし	【連邦法】 ・遺伝情報差別禁止法案が議会で審議中	【連邦法】 ・個人情報保護及び電子文書法（PIPEDA）

国・地域	生体情報	DNA	ID 等
	明確な定義は示されていない) ・OPC が生体情報を用いる際のガイダンスを公表している		
シンガポール	【法律】 ・個人情報保護法（PDPA）にて、個人識別可能な情報の一つとして指紋、虹彩等が挙げられているが、明文的な規定ではなく、「個人識別可能性」を判断して決定するとされている。	【法律】 ・個人情報保護法（PDPA）にて、個人識別可能な情報の一つとして DNA が挙げられているが、明文的な規定ではなく、「個人識別可能性」を判断して決定するとされている。	【法律】 ・個人情報保護法（PDPA）にて、個人識別可能な情報の一つとして ID 番号、旅券番号等が挙げられているが、明文的な規定ではなく、「個人識別可能性」を判断して決定するとされている。
EU	【EU 規則】 ・一般データ保護規則（GDPR）にて規定。	【EU 規則】 ・一般データ保護規則（GDPR）にて規定。	【EU 規則】 ・一般データ保護規則（GDPR）にて規定。
イギリス	【法律】 ・現行法である 1998 年データ保護法では明文規定はないが、生体情報が個人情報に該当することを ICO が示していた。 ・2017 年データ保護法案では生体情報についても明文規定を設けている（GDPR の定義に沿った内容となっている）。	【法律】 ・現行法である 1998 年データ保護法では明文規定はないが、生体情報が個人情報に該当することを ICO が示していた。 ・2017 年データ保護法案では生体情報についても明文規定を設けている（GDPR の定義に沿った内容となっている）。	【法律】 ・現行法である 1998 年データ保護法にて規定。 ・2017 年データ保護法案では生体情報についても明文規定を設けている（GDPR の定義に沿った内容となっている）。
フランス	【法律】 ・現行法である情報処理・データと自由に関する法律には明文規定はない。 ・GDPR の発効に伴い、GDPR の規定が直接適用される。 【ガイドライン等】	【法律】 ・現行法である情報処理・データと自由に関する法律には明文規定はない。 ・GDPR の発効に伴い、GDPR の規定が直接適用される。	【法律】 ・現行法である情報処理・データと自由に関する法律にて規定。 ・GDPR の発効に伴い、GDPR の規定が直接適用される。

国・地域	生体情報	DNA	ID 等
	・CNIL は職場における生体認証制御システムに関する裁可を公表（GDPR のプライバシーバイデザイン、プライバシバイデフォルト、データ保護インパクト評価に対応して、従来の裁可を改訂したもの）。		
ドイツ	【法律】 ・連邦データ保護法（BDSG）には明文規定はない。ただし公共空間における監視ビデオ画像は個人情報として規定されている。 ・GDPR の発効に伴い、GDPR の規定が直接適用される。	【法律】 ・連邦データ保護法（BDSG）には明文規定はない。 ・GDPR の発効に伴い、GDPR の規定が直接適用される。	【法律】 ・現行法である連邦データ保護法（BDSG）にて規定。 ・GDPR の発効に伴い、GDPR の規定が直接適用される。

なお、各国における法制度の概要は第 3 章にて記載する。

2.2 海外における利用例

次に、個人識別符号が各国においてどのように利用されているか、についての概略を以下に示す。個人識別符号は、政府機関による利用（各種公的サービスや、生体情報であれば出入国管理等）のほか、民間サービスでの利用も広まっている。なお、以下は全体的な傾向・特徴を示すための例示であり、網羅的な整理ではない。より詳細な利用動向については第4章を参照。）

表 2-2　個人識別符号の海外における利用例

個人識別符号	政府機関による利用	民間利用
生体情報（顔）	●2004 年より開始された出入国管理システム（US-VISIT）において、ビザを所持する渡航者の顔画像及び指紋の登録を行っている。（米国）	●ユーザの顔画像によるスマートフォンのロック解除。（Apple Inc.） ●モノ、顔、テーマを認識する画像マッチングソフトウェアを用いて、顧客、セキュリティ会社、広告会社が利用可能な画像 DB を作成。（Amazon Web Services Inc.）[*1]
生体情報（虹彩）	●空港の税関・出入国審査に虹彩認識技術を導入し、登録済みの旅客は時間をかけずに通過することが可能。（CANPASS Air プロジェクト, NEXUS プロジェクト(米国-カナダ間のみ)）[*2]	
生体情報（声紋）		●モバイル決済サービスにて、音声認証によって口座残高確認等、各種サービスの利用が可能。（Nuance オランダが金融機関 ING に提供）[*3]
生体情報（歩容）	●法廷において、防犯カメラに映った強盗犯と被告が同一人物であることを歩容で認証した結果を証拠として採用（英国）[*4] ●FBI は捜査における生体情報活用に取り組んでおり、歩容についても研究開発等を推進している。（米国）[*5]	
生体情報（指紋）	●2004 年より開始された出入国管理システム（US-VISIT）において、ビザを所持する渡航者の顔画像及び指紋の登録を行ってい	●非接触クレジットカードに指紋センサを搭載し、カード内に指紋データを登録して指紋認証による支払いが可能。（MasterCard

個人識別符号	政府機関による利用	民間利用
	る。（米国） ●国籍取得申請者や長期滞在する外国人は、政府に指紋情報を提出することが義務付けられている。指紋情報は、対象者に配布される在留カード RC(Residence Card)、在留許可証 BPR (Biometric Residence Permit)に記録される。（英国）*8 ●IC 旅券を用いた指紋認証出入国管理システムを運用し、高速かつ正確な出入国手続を実現（シンガポール）。*9 ●顔写真、指紋（10 指）、虹彩（両眼）を任意で登録し、本人確認などに用いることができる国民識別番号制度 Aadhaar を運用。（インド）	（本社：ニューヨーク州パーチェス）、Zwipe（本社：ノルウェー、オスロ））*6 ●学校のランチ販売時に、行列と支払カードを忘れてしまうことへの対応として指紋を利用。（ピッツバーグ）*7（“THE OECD PRIVACY FRAMEWORK ” (OECD, 2013) でも紹介。）
DNA	●世界最大規模の国家 DNA 型 DB を保有。（英国）	●「遺伝情報差別禁止法案」（An Act to prohibit and prevent genetic discrimination）が議会で審議中。財・サービスの提供、取引、契約等に際して、遺伝子テストを受けることや結果の開示を求めることを禁ずる内容。（カナダ）*10
ID	●NRIC（国民登録カード）番号及び共通のパスワードを組み合わせた SingPass により、さまざまな行政サービスをオンラインで利用することが可能。（シンガポール）*11	●社会保障番号(SSN)が携帯電話の契約時や預金口座の開設時になど、様々な場面で民間利用されている。（米国） ●本人の同意に基づき、新国民 ID カード(eID)に対応する個人属性情報を事業者が取得することが可能。（ドイツ）

*1 https://www.bloomberg.com/news/articles/2017-07-20/tech-companies-are-pushing-back-against-biometric-privacy-laws

*2 https://otc-cta.gc.ca/eng/publication/nexus-and-canpass-air

*3 https://www.nuance.com/about-us/newsroom/press-releases/ing-netherlands-launches-nuance-voice-biometrics.html

*4 http://news.bbc.co.uk/2/hi/programmes/click_online/7702065.stm

*5 https://archives.fbi.gov/archives/news/testimony/overview-of-fbi-biometrics-efforts
https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/biometric-center-of-excellence/modalities

*6 https://www.cnbc.com/2014/10/17/mastercard-and-zwipe-launch-first-contactless-fingerprint-payment-card.html

*7 http://pittsburgh.cbslocal.com/2014/11/04/biometrics-could-soon-make-plastic-cards-a-thing-of-the-past/

*8 https://www.gov.uk/government/news/changes-to-biometric-collection-categories

*9 https://www.mfa.gov.sg/content/mfa/overseasmission/beijing/consular_services/application_sg_passport.html

*10 http://www.parl.ca/DocumentViewer/en/42-1/bill/S-201/third-reading

*11 http://www.clair.or.jp/j/forum/c_mailmagazine/20150804/124-2.pdf

3. 各国の法制度の状況

本章では、各国・地域における法制度の概要及び経緯等について記載する。

3.1 米国

3.1.1 生体情報・DNA

最初に生体情報及び DNA に関する法制度の概要を示す。

(1) 連邦法・連邦政府機関等によるガイダンス

米国の 1974 年プライバシー保護法には、生体情報に関する明示的な規定等はない。

他方、顔画像認識については、画像解析やオンラインサービスでの顔画像検出などの技術の進展や普及を背景に、顔画像認識を使用する場合のベストプラクティスやガイドラインが政府機関より公表されている。FTC（連邦取引委員会）は、 2012 年に、顔画像認識（facial recognition）を商用の製品・サービスで使用する際の課題やケーススタディなどをベストプラクティスとして公表している[7]。また NTIA（商務省電気通信情報局）も、2016 年に、顔画像認識を商用利用する場合に遵守すべき原則をガイドラインとして公表している[8]。

表 3-1　米国・連邦政府機関等による顔認証に関するベストプラクティス

公表機関・文書名	目的・問題意識・位置づけ	指摘・提言等
FTC “Best Practices for Common Uses of Facial Recognition Technologies” (2012)	●顔画像の商業利用が拡大している。（認証、オンラインサービスでの顔検出、画像利用、等） ●商用利用に対するガイドを提供することで、イノベーションとプライバシー保護を実現できるようにする。	●FTC が主催した討論会とパブコメの結果に基づいて策定。データ漏えいのほか、同意なしの撮影、群衆の中からの個人識別の懸念が示された。 ●プライバシーバイデザイン、消費者の選択の簡潔化（適切なタイミングと状況での選択）、透明性、の 3 つの原則に従い、3 つのユースケースについて推奨事項を提示。
NTIA “Privacy Best Practice	●生体情報の利用拡大（例：認証、オンラインサービス、アク	●透明性（Transparency）、データ管理のグッドプラクティス

[7] FTC: “Facing Facts: Best Practices For Common Uses of Facial Recognition Technologies “ https://www.ftc.gov/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies

[8] NTIA: “Privacy Best Practice Recommendations For Commercial Facial Recognition Use “ https://www.ntia.doc.gov/files/ntia/publications/privacy_best_practices_recommendations_for_commercial_use_of_facial_recogntion.pdf

Recommendations For Commercial Facial Recognition Use" (2016)	セスコントロール）や潜在的用途の広さから、全般的なガイドラインが必要。 ●FTC の FIPPs*1 に基づき、一般的なガイドラインを作成。 ●認証を行わない場合や、顔画像を集積しない場合は対象外。	の開発（Developing Good Data Management Practices）、データ主体によるデータ利用組織の限定（Use Limitation）、セキュリティ上の安全対策（Security Safeguards）、データ品質（Data Quality）、問題解決・是正プロセスの提供（Problem Resolution and Redress）、を推奨。

*1 Fair Information Practice Principles の略。オンラインでプライバシー情報の収集、利用を行う各組織（政府機関、民間事業者の両方）に対し、プライバシー情報を適切に取扱い保護することを FTC が要請しているもの。Notice/Awareness、Choice/Consent、Access/Participation、Integrity/Security、Enforcement/Redress の 5 項目からなる。

これらはいずれも「ベストプラクティス」であり、FTC がプライバシー保護に関して定めている原則（FIPPs 等）に従って、顔画像についても適切に取扱うことを要請し、そのための事例やガイダンスを示す、という位置づけのものである。米国には、大手オンラインサービス事業者をはじめ、顔画像認識技術の開発や活用を行っている企業が多いこともあり、こうした自主的な対応を求めているとも考えられる。

(2) 連邦法案

法的定義（1.2.2 節(3)）でも記載したとおり、生体情報に関する規制を盛り込んだ法案が提出されている[9]。なお、あくまでも法案であり、最近の連邦レベルでの議論の一つとして参考という位置づけにて記載する。

法案が対象とする生体情報は前述のとおりであるが、主な規制内容は、生体情報（も含めた、センシティブな個人識別情報）を一定以上の規模で扱う事業者に対して、リスク評価、リスク管理、従業員教育、脆弱性テストなどを求めるという、比較的重い内容である。

当該法案は第Ⅰ編、第Ⅱ編、第Ⅲ編に分かれており、第Ⅰ編では、センシティブな個人識別情報を含むセキュリティ侵害について、その隠蔽に対する罰則を設けるとともに、規制機関に対して botnet（ボットネット）[10]の遮断を行う権限を付与すると規定している。

[9] 前述のとおり、委員会・小委員会に回送された時点で止まっており、可決には至っていない。委員会・小委員会での審議は行われていないとみられる。

[10] ボットとは、コンピュータウイルスの一種で、コンピュータに感染し、そのコンピュータを、ネットワーク (インターネット)を通じて外部から操ることを目的として作成されたプログラム。感染すると、外部からの指示を待ち、与えられた指示に従って内蔵された処理を実行する。この動作が、ロボットに似ているところから、ボットと呼ばれる。ボットが構成するネットワークをボットネットと呼び、数百～数万台

第Ⅱ編は A と B に分かれており、A では消費者プライバシーおよびデータセキュリティプログラム（センシティブな個人識別情報のセキュリティを保護するための、管理的・技術的・物理的保護手段）について規定している。

対象となるのは、年間に合衆国の個人 10,000 人以上に関する電子的またはデジタル形式のセンシティブな個人識別情報の収集、使用、アクセス、伝送、蓄積、処理を、州をまたいで行っている事業者である。ただし、金融機関、ヘルスケア関連事業者、伝送・ルーティング・一時的な蓄積等のみを提供する通信事業者は対象から除く。

プログラムにはリスク評価およびリスク管理が含まれ、その他従業員教育や脆弱性テストの実施も求められる。

また、連邦政府司法長官や州政府司法長官による法執行についても規定されている。

B ではセキュリティ侵害に関する通知について規定している。

第Ⅲ編は、予算措置に関する規定が記載されている。

(3) 州法

生体情報を規制する州法は、イリノイ州が先陣を切って、指紋、虹彩、顔面のスキャンの商業利用を規制した Biometric Information Privacy Act (通称 BIPA) を 2008 年に制定した。

その後、10 州がそれに相次ぐ観測もあったが、オンラインサービス企業等の激しいロビイングにより、結果的にはテキサス州（2009 年）とワシントン州（2017 年 5 月）において成立したのみである。ニューヨーク州を含む他の 8 州については成立しなかった。

ワシントン州法は、事業者のロビイング[11]の結果、BIPA よりも規制内容が緩くなっている（BIPA よりも生体情報の利用に関する規制が少ない、消費者の同意要件が狭められた、既にオンラインにある顔面画像に関しては一定の免除がある等）。

表 3-2　米国・生体情報を規制する州法の制定に関する動向

州	生体情報保護に関する法制化状況
イリノイ	2008 年に Biometric Information Privacy Act (BIPA)[12]が成立。 網膜または虹彩のスキャン、指紋、声紋、手または顔の幾何学的配置のスキャンが対象。 事業者は、生体情報を収集、蓄積する際に、ユーザーに対し書面での説明を提示し、書面での事前同意を取得する必要がある。また生体情報を保持する期間に関するポリシーを公表し、

の規模で構成される。同一の指令サーバの配下にある複数のボットは、指令サーバを中心とするネットワークを組み、フィッシング目的などのスパムメールの大量送信や、特定サイトへの DDoS 攻撃、スパイ活動 (感染したコンピュータ内の情報を外部へ送信)などに利用される。参考：情報処理推進機構（IPA）「ボット対策について」https://www.ipa.go.jp/security/antivirus/bot.html、JPCERT/CC「ボットネットの概要」https://www.jpcert.or.jp/research/2006/Botnet_summary_0720.pdf

[11] 3.6 節も参照。

[12] http://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57

州	生体情報保護に関する法制化状況
	不要になった時点で廃棄する義務を負う。
テキサス	2009 年に Texas Business and Commerce Code - BUS & COM § 503.001 (Capture or Use of Biometric Identifier)[13]が成立。 網膜または虹彩のスキャン、指紋、声紋、手または顔の幾何学的配置のスキャンが対象。訴訟を提起する権限が州司法長官のみに限定され、個人が訴訟を提起することはできない。
ワシントン	2017 年にワシントン州下院法案 HB 1493 が成立[14,15]。 対象とする生体識別子（biometric identifier）として、「指紋、声紋、網膜、虹彩、その他特定の個人を識別するために用いられるユニークな生物学的パターンまたは特徴」と記載されているが、他方で「物理的またはデジタルの写真、ビデオ、音声の記録、あるはそれらから生成されたデータ」は対象外と明記されており、事業者はそれら（例：顔写真のデータ）を使うことができる。 商業目的で生体識別子を利用する事業者は規制の対象として、通知、同意取得、当初の目的以上の商業利用を本人が制限する手段の提供、などが義務づけられている。他方、従業員の勤怠管理やアクセス管理に生体識別子を用いる事業者は規制の対象外とされている。 訴訟を提起する権限が州司法長官のみに限定され、個人が訴訟を提起することはできない。
カリフォルニア	個人情報を収集する企業に対し、その誤用・悪用を防ぐ義務を課す法案をサクラメントの議員が 2015 年に提出。州下院を通過したが、上院での採決には至らなかった。
コネチカット	生体情報を取得される消費者から書面での同意を得る義務を定めた法案が 2016 年に州下院を通過したが、上院は通過しなかった。2017 年にも同様の法案が提出されたが、委員会を通過しなかった。
モンタナ	BIPA のように事前同意を求める法案が提出されたが、産業界の激しい反対等により不成立。
アリゾナ、ミズーリ	学生のプライバシーを保護するための法案が 2017 年に提出されたが、不成立。
アラスカ、ニューハンプシャー、ニューヨーク	3 州とも法案を提出したが不成立（ニューヨーク州では 2 度提出されたが 2 度とも不成立）。

[13] http://codes.findlaw.com/tx/business-and-commerce-code/bus-com-sect-503-001.html

[14] https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2017/06/1493-S.SL_.pdf

[15] 成立した州法には特定の名称はないが「ワシントン・バイオメトリック・プライバシー法」として言及されている、と報道されている。（以下の記事の冒頭のパラグラフ参照。）
https://www3.swipeclock.com/blog/learn-washingtons-new-biometric-privacy-law-affects-businesses

出所：報道[16][17]を参考に作成

3.1.2 ID

次に、PII（Personally Identifiable Information）のうち ID に関する法制度について記載する。

(1) 連邦法

米国では、公的部門においては、連邦法である 1974 年プライバシー法 The Privacy Act of 1974）[18]が、政府機関による記録システム(a system of records)で保持されている PII について、その取得、保持、利用、頒布について規定している。日本のマイナンバーに相当する社会保障番号（Social Security Number; SSN）の取扱いは同法にて規制される。

同意なく PII を陳列、購入、販売することを禁止する法案（Privacy Act of 2005）や、フィッシングを通じて PII を取得することを防止する法案（Anti-Phishing Act of 2005）、SSN の頒布を制限する法案（Social Security Number Protection Act of 2005, Identity Theft Prevention Act of 2005）等も度々提出されてきているが、立法化には至っていない。

なお、議会（Congress）及びホワイトハウスは、 諜報活動及び国家安全の名の下にバイオメトリクスを収集している[19]。

(2) 政府機関に対するガイドライン

米国労働省（Department of Labor; DOL)は、PII の保護に関する内部向けガイダンス（Guidance on the Protection of Personal Identifiable Information）を出している[20]。

このガイダンスでは、DOL の職員及びコントラクターは PII にアクセスすることが可能であることから、PII の紛失と不正利用を防止する責任があると規定し、セキュリティポリシーに基づく適切な取扱いを義務づけている。また PII の紛失は ID 窃盗や当該情報の悪用など重大な損害をもたらすとしている。

なお、ガイダンスでは、PII について以下のように定義している。

> PII を次のように定義する：
> (i) 個人を直接特定する情報（例：氏名、住所、社会保障番号
> (ii) 他のデータにより個人を間接的に特定する、間接的情報（例：性別、人種、生年月日、地理的情報やその他の情報等を組み合わせて特定する）

16 https://www.bloomberg.com/news/articles/2017-07-20/tech-companies-are-pushing-back-against-biometric-privacy-laws

17 https://www.natlawreview.com/article/law-unintended-consequences-bipa-and-effects-illinois-class-action-epidemic

18 Pub.L. 93‐579, 88 Stat. 1896, 1974 年 12 月 31 日制定, 5 U.S.C. § 552a

19 https://www.bloomberg.com/news/articles/2017-07-20/tech-companies-are-pushing-back-against-biometric-privacy-laws

20 https://www.dol.gov/general/ppii

物理的またはオンラインの契約において個人を特定する情報も PII に含まれる。

PII is defined as information: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors). Additionally, information permitting the physical or online contacting of a specific individual is the same as personally identifiable information. This information can be maintained in either paper, electronic or other media.

(3) 民間分野に関する法制度

米国では、民間部門（連邦法）については分野ごとのセクトラル方式が採られている。

例えば、医療分野では、DHHS（Department of Health and Human Services: 保健社会福祉省）は、1996 年に制定された医療保険の携行性と責任に関する法律 (Health Insurance Portability and Accountability Act: HIPAA) に基づき、健康情報に関するプライバシールール（HIPAA Privacy Rule）及びセキュリティルールを策定し、同プライバシールールにおいて、PII と似た概念である患者の「保護対象保健情報」（Protected Health Information (PHI)）について規定するとともに、その取扱いも定めている。

なお、医療分野及び金融分野以外の分野については、3.1.2 節(1)に記載した法案が提出されているが、成立には至っていない。

HIPPA プライバシールールの概要を以下に示す。

表 3-3　HIPPA プライバシールールの概要

保護対象	保護対象保険情報（Protected Health Information; PHI）、データ保持者又はそのビジネスアソシエートに保持、送付される全ての「個人が特定可能な保健情報」（電子媒体、紙媒体、口頭などの全ての手段が含まれる。）
定義	個人が特定可能な保健情報は、以下について言及する統計データを含む情報である。 ・ 個人の過去、現在、将来の身体的又は精神的な健康状況 ・ 個人へのヘルスケアの対策 ・ 個人の過去、現在、将来のヘルスケアの支払いの状況 ・ その他個人を特定するもの又は特定のために利用されると考えられる合理的な基礎があるもの 個人が特定可能な保健情報とは、多くの共通の識別子（例：氏名、住所、生年月日、社会保障番号）が含まれる。 当該事業者が保持する従業員記録及び、Family Educational Rights and Privacy Act, 20 U.S.C. §1232g.に規定されている教育その他の記録は対象外。
具体的な規制内容（概略）	・データ使用の原則（ プライバシールールにより許可される、要求される場合と、対象となる個人（又は代諾者）が文書により許可した場合以外はデータを使用してはならない） ※ 匿名化された保健情報(de-identified health information)の使用又は開示には制限はない。 ・許可される使用又は開示（個人の許諾を得ずに保護対象の保健情報を使用又は開示することが許可される場合） ・許諾・認定による使用又は開示（治療、支払、ヘルスケア、それ以外のプライバシー ルールにより許可された使用以外） ・必要最小限の限定的な使用又は開示 ・管理上の要求

出所：以下に基づいて作成

https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html

http://www.mhlw.go.jp/shingi/2010/06/dl/s0616-4g.pdf

(4) 州法

州レベルにおいてもプライバシー法が制定されている。中でも、最初にセキュリティ侵害通知法（security breach notification law; California Civil Code §1798.82)を制定したカリフォルニア州はプライバシー法分野において先進的な存在といわれる。カリフォルニア州法（The California Online Privacy Protection Act）では、個人を特定可能な情報（PII)として SSN（社会

保障番号）を含む具体例が明記されている[2122]。

22577 定義 「個人を識別可能な情報」とは、個々の消費者を識別することができる情報で、オペレーターにより当該個人からオンラインで収集されたもので、かつオペレーターによりアクセス可能な形態で管理されており、以下のいずれかを含む： (1) ファーストネーム及びラストネーム (2) 住所（街路名や都市名を含む） (3) 電子メールアドレス (4) 電話番号 (5) 社会保障番号 (6) 特定の個人に接触することができる物理的またはオンラインの識別子 (7) Web サイトまたはオンラインサービスがユーザーについてオンラインで収集している情報で、個人を識別可能な形態にて、ここに示す他の識別子と関連づけて管理しているもの 225777 The term “personally identifiable information” means individually identifiable information about an individual consumer collected online by the operator from that individual and maintained by the operator in an accessible form, including any of the following: (1) A first and last name. (2) A home or other physical address, including street name and name of a city or town. (3) An e-mail address. (4) A telephone number. (5) A social security number. (6) Any other identifier that permits the physical or online contacting of a specific individual. (7) Information concerning a user that the Web site or online service collects online from the user and maintains in personally identifiable form in combination with an identifier described in this subdivision

当該州法においては、インターネットを通じてカリフォルニア在住の消費者に関する個人識別可能情報を収集する商業ウェブサイトのオペレーターは、情報の取扱いに関するプライバシーポリシーを目立つように掲載することとされている。

また、改正法によって、未成年者の場合、当該オンライン情報の削除又は削除要請を認めること、当該コンテンツをどのように削除、削除要請できるかを示すこと、が規定されているほか、未成年者に違法な広告（例：酒、火器、タバコ、刺青、宝くじ等）が禁止されている。

---

21 https://content.next.westlaw.com/Document/I02064fbd1cb611e38578f7ccc38dcbee/View/FullText.html?contextData=(sc.Default)&transitionType=Default&firstPage=true&bhcp=1

22 http://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=BPC&division=8.&title=&part=&chapter=22.&article=

(5) 標準化機関によるガイダンス等

米国の国立標準技術研究所 (NIST: National Institute of Standards and Technology)は PII を保護するためのガイド(”Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)”）[23]を公表しており、その中で PII は以下のように定義されている。

> PII is ―any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual‘s identity, such as name, social security number, date and place of birth, mother‘s maiden name, or biometric records（注：氏名、SSN、誕生日・場所、母親の旧姓、生体情報）; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information（注：医療、教育、金融、雇用に関する情報）.

当該ガイドの内容は概略以下のとおりである。

- PII を利用する組織は、保有するすべての PII について確認すべきである
- PII を利用する組織は、PII の使用、収集、保管について、自らの事業目的やミッションを果たす上で最低限必要なものとすべきである
- PII を利用する組織は、PII について、PII 機密性影響レベルに基づいて分類すべきである（評価視点の例：個人識別性、PII の量（件数）、データ項目の機微性、使用状況、機密保護義務、PII へのアクセスと保管場所）
- PII を利用する組織は、 PII 機密性影響レベルに基づき、適切な保護手段を適用すべきである（例えば、PII の機密性保護のためのポリシー及び手順の策定、訓練の実施、PII の匿名化（de-identify）、PII へのアクセスコントロールポリシーの策定と実装、モバイルデバイスに対するアクセスコントロール、通信の秘匿化（情報または通信の暗号化等）、監査）
- PII を利用する組織は、PII の侵害に対する事故対応計画を策定すべきである
- PII を利用する組織は、関係者（プライバシー責任者、CIO、CISO、弁護士、プライバシー保護に関する上級官僚等）の間の密接な調整を促進すべきである

3.2 カナダ

3.2.1 生体情報

(1) 連邦法

カナダのプライバシー法である PIPEDA（Personal Information Protection and Electronic Documents Act: 個人情報保護及び電子文書法）では、生体情報に関する直接の規定はないた

[23] http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf

め、生体情報の個人情報該当性が一つのポイントとなる。この点についてはプライバシーコミッショナーから見解が示されているので、次節にて記載する。

(2) プライバシー･コミッショナーによるガイド（生体情報の個人情報該当性）

カナダのプライバシーコミッショナーである Office of the Privacy Commissioner of Canada (OPC)は、2011 年に公表したガイド（”DATA AT YOUR FINGERS”）[24]において、生体データが個人情報に当たると述べ、例示も行っている。

しかし、生体データの明示的な定義は示されておらず、具体的にどのような生体データが個人情報に当たるかについては不明確である。

同ガイドでは、生体情報の個人情報該当性について以下のように述べている。

指先、顔、虹彩をスキャンして収集したものは、いずれの場合においても、個人を識別可能な個人情報である。 whether a fingertip, a face or an iris is being scanned, what’s being collected is personal information about an identifiable individual.

また、生体情報として以下のような例示を行っている。個人情報に該当する具体的な境界は定められていないが、主要な生体情報は含まれている。

人々の身体・行動の特徴、例えば顔の特徴、声紋、指紋、掌紋、指・掌の静脈の形状、眼の構造（虹彩、網膜）、歩容 people’s physical and behavioural attributes, such as facial features, voice patterns, fingerprints, palm prints, finger and palm vein patterns, structures of the eye (iris or retina), or gait.

(3) プライバシー･コミッショナーによるガイド（生体情報の取扱いに関するガイド）

“DATA AT YOUR FINGERS”では、生体情報利用のプライバシー上の課題、（他分野におけるプライバシー保護対策・リスク軽減策のうち）生体情報の利用に適用できるもの、推奨されるプライバシー原則、を提示している。その概要を以下に示す。

a. 目的・背景

- 生体情報を利用して個人認証に活用したり、自動的に識別するシステムが政府機関および民間セクターにおいて広がりつつある。
- 収集される生体情報が何であれ、それらは個人情報である。
- このガイドでは、生体情報の利用におけるプライバシー関連事項とリスク低減策について記載する。

[24] https://www.priv.gc.ca/media/1982/gd_bio_201102_e.pdf

b. プライバシー上の課題

- 生体情報における特徴的なプライバシー上の課題としては以下が挙げられる。
  - 生体情報の隠れた収集と利用（例：顔画像などは、データ主体に気づかれずに、また同意を得ずとも、取得可能）
  - クロスマッチング（生体情報の不変性と認証力の高さから、収集・蓄積された目的以外での利用が容易）
  - 二次情報（例：虹彩画像は認識のほか健康に関する情報を分析することも可能、指紋から個人の地位や社会経済的なステータスを知ることができる、DNA からは健康に関する幅広い情報がわかる、等）

c. 適用可能な対策

- 生体情報のプライバシーに関する政策や基準はカナダにはないが、OPC に対し、他の分野におけるプライバシー保護対策・リスク軽減策が生体情報についても適用できるという主張・要請が多く寄せられている。
  - プロアクティブなプライバシー対策（設計段階等からプライバシーを考慮する）
  - プライバシー影響評価（PIA）（※公的セクターに対しては PIA が義務づけられている）
  - 生体情報利用に関する 4 項目テスト（①生体情報利用は必要か、②効果的か、③生体情報利用のメリットはプライバシーリスクに釣り合っているか、④よりプライバシー侵害の少ない代替手段はないか）

d. プライバシー原則

- OPC 及び関連する機関は、生体情報を用いるシステムにおけるプライバシー安全策を強化するためのいくつかの原則を提案する。
  - サマリー・データの記録（生の生体情報ではなくテンプレートデータのみを記録する）
  - 認証（Verification）のみに用い、識別（Identification）は行わない
  - ローカル端末への蓄積（中央データベースではなく、ローカル端末、スマートカード等に生体情報を記録する）

(4) まとめ

カナダでは法律による規制は行われていないものの、ガイドで挙げられているプライバシー上の課題では、データ主体の認識のない形でのデータ取得、二次情報など、現代的な問題意識が示されている。

2000 年代に生体認証が本格的に導入された際は、本人から直接、同意に基づいて取得され、本人確認に用いられるという利用形態が典型的であり、認証精度（本人拒否・他人受容）や、漏洩の影響の大きさ（生体情報が変更できないため）、などが生体情報の利用に関する個人情報保護・プライバシーにおける課題であった。

他方、最近では、画像認識・解析技術の進歩やカメラ、スマートフォンなどの普及、SNSの利用者拡大、ディープラーニング・機械学習による個人識別技術の進化などを背景に、生体情報が取得されうる機会が増え、またそれを利用し流通させることが容易になったため、上記のようなプライバシーリスクが課題となってきているが、これは上記の問題意識と重なるものである。

また、ガイドにおいて示されている対策（プライバシー原則）もいずれも重要なものである。後述するが、ローデータではなくテンプレートを使うことで漏洩リスクを減少させる、ローカル端末（スマートフォン等）での認証、などは技術開発や標準化、実装が進められている[25]。また、認証[26]のみに用いて識別[27]には用いないという点も、不要な識別を排除するという意味では重要であると考えられる[28]。

3.2.2 ID

カナダで個人情報の保護に関係する主な連邦法としては連邦プライバシー法（Privacy Act）[29]と個人情報保護及び電子文書法（PIPEDA）がある。連邦プライバシー法は、連邦政府機関が個人情報の収集、利用等を行う場合を対象とした規定であり、データ主体に対して連邦政府機関が保有する個人情報へのアクセス権や訂正請求権等を認めている。一方、個人情報保護及び電子文書法（PIPEDA）は、民間事業者による個人情報の取扱いを対象とする規定である。

連邦プライバシー法では第 3 条[30]において個人情報（”personal information”）が「識別可能な個人に関する情報で、任意の形式で記録されているもの」（” information about an identifiable individual that is recorded in any form”）と定義されており、例として列挙されているもの（ただしそれらに限定されない）ものに「(c)識別可能な番号、記号その他個人に割り当てられたもの（(c) any identifying number, symbol or other particular assigned to the individual）」が含まれている。

カナダの日常生活で使用されている ID には幾つかがあり[31]、多く使われているものの一つとして社会保険番号（Social Insurance Number: SIN）が考えられる。SIN の事務的な取扱いについては、社会保険番号規則（Social Insurance Number Regulations）が定めているが、SIN と関係する個人情報保護については、雇用及び社会開発省法（” Department of Employment

---

25 これらについては第 4 章で後述する。

26 本人と、予め登録してあるデータが 1:1 の関係にあり、予め登録された本人であることを確認するという意味。

27 予め登録されている多数のデータの中から、本人から取得したデータと合致するものを探し、本人が誰であるかを特定すること。本人と登録データの関係は 1:n となっている。

28 法律による禁止ではなく、あくまでもガイドによる推奨であり、自主的な取組によって不要な識別が回避されることが期待される。

29 http://laws-lois.justice.gc.ca/eng/acts/P-21/page-1.html

30 連邦プライバシー法（Privacy Regulations）第 3 条では、「個人情報とは、個人を識別できる情報（personal information means information about an identifiable individual）」であると規定されている。

31 Government of Canada, “Canadian Identification”, http://www.canadainternational.gc.ca/uae-eau/consular_services_consulaires/identity-identite.aspx?lang=eng.

and Social Development Act”）[32]の第 4 部（第 30 条～第 43 条）において規定されている[33]。

第 30 条(1)では同法における「（個人）情報」については、プライバシー法第 3 条の定義に従うとしているが、この定義には ID（上述の(c)）だけでなくさまざまな情報が含まれ、また、雇用及び社会開発省法における個人情報保護の目的（第 31 条）も対象は ID の保護に限定されていない。これらもふまえると、SIN は同法第 30 条～第 43 条の規定に基づいて保護されることと解される。これらの各条では、通知、同意、透明性、アクセス、利用制限などの一般的な規定に加えて、研究開発や政策立案に利用する場合の条件等が定められている。

なお SIN は他にも雇用保険法、所得税法、年金制度等の場面[34]で使用されている。

3.3 シンガポール

3.3.1 PDPA

シンガポールにおいては PDPA（Personal Data Protection Act）[35]が個人データの保護に関する包括的な法律である。

PDPA は、国境を越えるデータ転送サービスを念頭[*1]に、シンガポールのデータ保護体制を国際基準と同等に保つために制定された。PDPA は国際競争力も重視しており、個人データを保護する重要性と、個人データを収集、使用または開示する組織の必要性とのバランスを取ることを目的としている〔第 3 条〕。すなわち、個人情報保護と企業活動のバランスを重視しているといえる。

3.3.2 PDPA における個人情報の定義とその他の規定

(1) 個人情報の定義

PDPA には、生体情報について直接規定する条項はない。また、PDPA では「個人データ」について、「個人識別可能性」を基準にして個々のケースに応じて判断するとしている。したがって、生体情報についてもこの基準により個人情報の該否が判断され、個人情報に該当すると判断される場合には、PDPA における規定が適用される。

PDPA の第 2 条では、「真実であるか否かを問わず、個人識別が可能となるデータを指す」と規定している。ただし、個人の公開情報（ビジネス上の連絡先を含む）（第 2 条）や 100 年以上存在する個人データまたは 10 年以上前に死亡した人の個人データ（第 4 条第 4 項 b）は除外される。

---

[32] http://laws-lois.justice.gc.ca/eng/acts/H-5.7/page-1.html

[33] 社会保険番号規則の上位の「法」として雇用及び社会開発省法が明示されている（同規則第 1 条）。

[34] Government of Canada, “The Social Insurance Number Code of Practice Annex 2 - Authorized federal uses of the SIN”, https://www.canada.ca/en/employment-social-development/services/sin/reports/code-of-practice/annex-2.html.

[35] https://sso.agc.gov.sg/Act/PDPA2012

また、PDPA に関するガイドライン（“ADVISORY GUIDELINES ON KEY CONCEPTS IN THE PERSONAL DATA PROTECTION ACT2017”[36]）では具体的な例や解釈が記載されている。（注：以下で〔 〕内はガイドラインの節番号）

- フルネーム、ID 番号、個人の携帯番号、旅券番号、個人識別可能な録音、指紋、虹彩、DNA 等が列挙されている〔5.10〕が、個人データに該当するか否かは「個人識別可能性」に鑑み判断すると強調されている。
- 住所に関しては複数人が該当する可能性があるので、一律に個人データとは判断しない〔5.5〕。
- 「個人データ」の形と種類に関する制限はない〔5.3〕。
- データの組み合わせによって個人の識別が可能となる場合は、データセット（datasets）として個人データとなる〔5.12、5.13〕。

(2) その他の規定

個人データの収集・利用・開示についても「合理性」基準に照らし合わせて判断され、「合理性」の基準は進化していくものであるとしている〔ADVISORY GUIDELINES 9.5〕。

PDPA では個人データの取扱について合理的なセキュリティ対策を講ずることを要求している〔第 24 条〕。データの性質、収集された形式等に鑑み、幾つかの例を示しているが〔ADVISORY GUIDELINES 17.5〕、一律に規定するのではなく「合理的なセキュリティ対策」と規定している〔ADVISORY GUIDELINES 17.2〕。

(3) ID

PDPA 第 2 条[37]によれば、個人識別可能情報（Personally Identifiable Information: PII）は個人データ（personal data）に含まれると解される。

他方、PII に関する明文規定はないが、シンガポールの個人データ保護委員会（Personal Data Protection Commission: PDPC）が発行した「電子媒体における個人データ保護に関するガイド（GUIDE TO SECURING PERSONAL DATA IN ELECTRONIC MEDIUM）」[38]では、クラウドサービスにおける PII の保護に関して、クラウドサービス異業者が提供する各種のセキュリティ機能に加えて、PII に関する国際規格 ISO/IEC 27018[39]に言及し、同ガイドの脚注 9 でその概要を紹介している。すなわち、法規制面で PII の保護等に関する明文規定はな

---

[36] ガイドラインは以下から参照可能。https://www.pdpc.gov.sg/Legislation-and-Guidelines/Guidelines/Main-Advisory-Guidelines#AG1
また、ここで引用している部分は以下にある。https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/important-terms-in-pdpa---ch-3-9-(270717).pdf

[37] 個人データ保護法（Personal Data Protection Act 2012、PDPA）第 2 条によると、「個人データとは、真実であろうとなかろうと、識別可能な個人に関するデータを意味する。（“personal data” means data, whether true or not, about an individual who can be identified）」

[38] https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/guidetosecuringpersonaldatainelectronicmedium0903178d4749c8844062038829ff0000d98b0f.pdf

[39] ISO/IEC 27018 は、ISO/IEC 29100 のプライバシー原則に従い、パブリッククラウドコンピューティング環境における個人識別可能情報（PII）に関するガイドラインである。

いが、技術面では PII の保護に関して、とくにクラウドサービスを利用する事業者に対して注意喚起や情報提供を行っている状況と解される。

一方、シンガポールには日本のマイナンバーと類似する国民登録制度がある。PDPC は、国民登録番号証（National Registration Identification Card: NRIC）[40]に関する個人データ保護について、法改正に関する提案[41]「PROPOSED ADVISORY GUIDELINES ON THE PERSONAL DATA PROTECTION ACT FOR NRIC NUMBERS」[42]を 2017 年 11 月に公表した。同提案では、以下が提示されている。

- NRIC 番号は、個人を特定することができる一意の数字及び文字の列であり、個人情報に該当する
- したがって、NRIC 番号を収集する事業者は PDPA の規定に従う義務を負う
- NRIC 番号を取得・使用・開示してよい条件（法令に基づく場合、または個人について厳密に認証する必要がある場合に限る）
- 同意の要否（法令に基づく場合であれば同意は不要）
- 法令に基づき NRIC 番号を取得・使用・開示することが認められるサンプルケース
- 法令に基づかないが個人について厳密に認証することが必要と考えられる場合については、各事業者等が認証に求められる厳密性等に基づいて検討する
- 法令に基づかないが個人について厳密に認証することが必要と考えられる場合のサンプルケース
- NRIC 番号が使用できない場合の代替となるものについては PDPC は具体的に指定しない（事業者等は、事業内容や運用条件に基づいて代替となる ID 等について検討するとともに、代替となる ID が個人情報の過剰な取得等を招かないよう注意する）
- 上記のサンプルケース
- 事業者が NRIC（物理的な IC カード）またはそのコピーを保持する場合、事業者は NRIC の物理的カードに記録されている全ての個人情報を取得したことになり、PDPA の関連規定を遵守する義務を負うことの確認
- したがって、法により要求されない限り、一般論として事業者は NRIC の物理的カードを保持すべきでない（ただし、特定の条件において、事業者が本ン確認のために NRIC の物理的カードの券面をコピーすることは認められうる）
- 個人情報保護ポリシー等の定期的な見直しの必要性
- 事業者が守るべき義務の再確認（公開性、保護、保持期間の制限、その他）

また、NRIC 番号と同様の一意の識別子または身分証明書（例：旅券番号）について同様の扱いが適用される可能性についても示されている。

---

[40] NRIC に対しては NRIC 番号が出生時に付与され、さまざまな場面で ID として利用されている。また NRIC 番号を用いてオンラインの各行政サービスを利用する際に、共通のパスワードを設定することができ、これを SingPass という。https://www.singpass.gov.sg/spauth/login/loginpage?URL=%2F&TAM_OP=login
（参考）http://www.clair.or.jp/j/forum/c_mailmagazine/20150804/124-2.pdf

[41] パブリックコンサルテーションという位置づけで公表されている。

[42] https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Legislation-and-Guidelines/proposed-nric-advisory-guidelines---071117.pdf

3.4 欧州連合（EU）

3.4.1 GDPR における定義と規制の概要

(1) 生体情報及び DNA の定義

2018 年 5 月から施行される General Data Protection Regulation (GDPR)では、第 1 章でも記載したとおり、生体データ及び遺伝データが明確に定義づけられている。

第 4 条 定義

(13) 「遺伝データ」とは、自然人の生理機能又は健康に関する固有の情報を与え、特に当該自然人からの生物的サンプルの分析から得られる、継承又は獲得した自然人の遺伝的特性に関わる個人データをいう。

(14) 「生体データ」とは、顔画像又は指紋確証データのように、当該自然人に特有の識別性を認められる又は確かめられる、自然人の身体的、生理的又は行動的特性に関する特定の技術的処理 から得られる個人データをいう。

Article 4 Definition

(13) 'genetic data' means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;

(14) 'biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

(2) 生体情報及び DNA に関する規制の概要

生体情報及び DNA を取扱う際に直接関係する規制としては、第 9 条（特別な種類の個人データの取扱い）及び第 35 条（データ保護影響評価）が挙げられる。

第 9 条第 1 項では、特別な種類の個人データの一つとして、個人の一意な識別を目的とした生体データや遺伝データの取扱いが禁じられている。ただし、第 2 項では、同項に記載された(a)～(j)のいずれかに該当する場合には適用されないという免除規定が定められている。

第 9 条　特別な種類の個人データの取扱い

1. 人種若しくは民族的素性、政治的思想、宗教的若しくは哲学的信条、又は労働組合員資格に関する個人データの取扱い、及び遺伝データ、自然人の一意な識別を目的とした生体データ、健康に関するデータ又は自然人の性生活若しくは性的嗜好に関するデータの取扱いは禁止する。

2. 第 1 項は次に掲げる場合には適用されない。
   (a) データ主体が、一つ又は複数の特定された目的のために当該個人データの適用に対して明示的な同意を与えた場合。ただし、EU 法又は加盟国の国内法が、第 1 項で定める禁止事項がデータ主体によって解除されるべきではないと定めている場合を除く。
   (b) 雇用及び社会保障並びに社会的保護に関する法の分野における管理者又はデータ主体の義務の履行及び特定の権利を行使する目的で取扱いが必要な場合。ただし、当該法が、EU 法若しくは加盟国の国内法又は基本的権利及びデータ主体の利益に対する適切な保護を定めた加盟国の国内法による労働協約によって認められている場合に限る。
   (c) データ主体が物理的又は法的に同意を与えることができないとき、データ主体又は他の自然人の重要な利益を保護するために取扱いが必要な場合。
   (d) 政治、哲学、宗教若しくは労働組合の目的を持つ財団、組織又はあらゆる他の非営利団体による適切な保護措置を備えた適法な活動において取扱いが実行される場合。ただし、その取扱いは、メンバー、団体の前メンバー、又はその目的において団体と定期的に接触をしている人々に関する取扱いであり、データ主体の同意なく団体外に個人データが開示されないことを条件とする。
   (e) 取扱いがデータ主体によって明白に公開された個人データに関する場合。
   (f) 法的主張時の立証、行使若しくは抗弁又は裁判所がその法的資格に基づいて決定するために取扱いが必要な場合。
   (g) 実質的な公共の利益を理由として取扱いが必要な場合。ただし、求められた目的と比例し、データ保護の権利の本質を尊重し、データ主体の利益及び基本的権利を保護するための適切かつ特定の対策を規定した EU 法又は加盟国の国内法に基づく。
   (h) 予防的な若しくは職務上の医療目的、従業員の業務能力の評価、医療診断、又はヘルスケアや処置若しくはソーシャルケアや処置の提供にとって取扱いが必要な場合。又は、EU 法若しくは加盟国の国内法に基づくか、医療専門家との契約でかつ第 3 項で定める条件並びに保護措置に服する契約に依拠したヘルスケア若しくはソーシャルケアの制度及びサービスにとって取扱いが必要な場合。
   (i) 公衆衛生の分野における公共の利益を理由として取扱いが必要な場合。例えば、重大な越境衛生脅威に対する保護、ヘルスケア並びに医療製品又は医療機器の質及び安全性の高水準の保証といった理由。ただし、データ主体の権利若しくは自由、特に秘密保持を保護するため適切かつ具体的対策を規定する EU 法又は加盟国の国内法に基づく。
   (j) 公共の利益、第 89 条第 1 項による科学的若しくは歴史的研究目的又は統計目的の達成のために取扱いが必要な場合。ただし、求められた目的と比例し、データ保護の権利の策を規定する EU 法又は加盟国の国内法に基づく。

Article 9 Processing of special categories of personal data

1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

2. Paragraph 1 shall not apply if one of the following applies:
   (a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;
   (b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;
   (c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
   (d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or tradeunion aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;
   (e) processing relates to personal data which are manifestly made public by the data subject;
   (f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
   (g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;
   (h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;
   (i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy; or
   (j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

また、生体情報及び遺伝データを取扱う場合には、第 35 条第 3 項(b)により、第 1 項に定めるデータ保護影響評価を行うことが義務づけられている。また、公共空間を対象にカメラによる大規模な監視を行う場合には第(c)項により実施が要求されることが考えられる。他方、第 5 項に規定されている一覧に該当する場合には義務づけられない。データ保護影響評価が含むべき内容については第 7 項に記載されている。

第 35 条 データ保護影響評価

1. 特に新たな技術を用いるなどのある種の取扱いが、その性質、範囲、文脈及び取扱いの目的を考慮して、自然人の権利や自由に高リスクを生じさせる可能性がある場合、管理者は、取扱いの前に、予定された取扱い作業の個人データ保護への影響評価を実施しなければならない。独立した評価は同様の高リスクを示す同様の取扱い作業の集合で用いることができる。

3. 第 1 項で定めるデータ保護影響評価は特に次に掲げる場合に要求されるものである。
   (a) プロファイリングを含めた自動処理に基づいて自然人に関する個人的側面を体系的かつ広範囲に評価され、その評価に基づいて決定がなされ、その決定が自然人に関する法的効果を生じさせるか又は同様に自然人に重大な影響を与える場合。
   (b) 第 9 条第 1 項で定める特別な種類のデータ、又は第 10 条で定める有罪判決及び犯罪に関する個人データを大規模に取扱う場合。
   (c) 誰でも立ち入ることの出来る場所において大規模な体系的監視を行う場合。

5. 監督機関はデータ保護影響評価が求められない取扱い作業の種類の一覧を発行し、公開することができる。監督機関は欧州データ保護会議に当該一覧を通知しなければならない。

7. 評価は少なくとも次に掲げる事項を含むものとする。
   (a) 予想された取扱い作業及び取扱いの目的の体系的記述。該当する場合、管理者によって追求される正当な利益を含む。
   (b) 目的に関する取扱い作業の必要性及び比例性の評価。
   (c) 第 1 項で定めるデータ主体の権利及び自由に関するリスクの評価。
   (d) リスクに対処するために予定された対策。データ主体及び関連する他者の権利及び正当な利益を考慮し、個人データの保護を確実にし、本規則の遵守を証明するための保護措置、安全対策及び安全メカニズムを含む。

Article 35 Data protection impact assessment

1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

3. A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:
   (a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
   (b) processing on a large scale of special categories of data referred to in Article 9(1), or of

personal data relating to criminal convictions and offences referred to in Article 10; or
(c) a systematic monitoring of a publicly accessible area on a large scale.

5. The supervisory authority may also establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. The supervisory authority shall communicate those lists to the Board.

7. The assessment shall contain at least:
(a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
(b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
(c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and
(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

データ保護影響評価（DPIA）が含むべき評価基準については、GDPR に関するガイドラインのうち DPIA に関するもの（WP248 rev.01）[43]でも Annex-2 にて記載されているが、いずれも最低限含むべき項目ないし基準として示されているもので、具体的なフレームワークについては同ガイドラインにていくつかの例（加盟国における共通及び分野別の PIA（Privacy Impact Assessment）フレームワーク及び国際標準（ISO/IEC 29134: Guidelines for privacy Impact assessment））が示されている。実際に DPIA を実施する場合にはこれらのフレームワーク・国際標準等に即して行うことになるのではないかと予想される。

(3) ID の定義

GDPR では、ID は個人データの一般的定義の中に含まれており、個人データとして扱われる。

第 4 条 定義

(1) 「個人データ」とは、識別された又は識別され得る自然人（以下「データ主体」という。）に関するあらゆる情報を意味する。識別され得る自然人は、特に、氏名、識別番号、位置データ、オンライン識別子のような識別子、又は当該自然人に関する物理的、生理的、遺伝子的、精神的、経済的、文化的若しくは社会的アイデンティティに特有な一つ若しくは複数の要素を参照することによって、直接的に又は間接的に、識別され得る者をいう。

[43] "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679" (Adopted on 4 April 2017, As last Revised and Adopted on 4 October 2017)

Article 4 Definition

(1) 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

(4) ID に関する規制の概要

上記の定義から、EU においては、ID は個人情報として GDPR に記載されている各規定に基づき取り扱われるものと解される。

他方、GDPR 第 87 条では、「加盟国は国民識別番号又は一般に用いられるあらゆる識別子の取扱い関する具体的条件を定めることができる。その場合、国民識別番号又は一般に用いられるあらゆる識別子は、本規則によるデータ主体の権利及び自由のため、適切な保護措置下でのみ、利用されなければならない。」と定めており、具体的な規定については加盟国に委ねられている。

3.4.2 経緯

(1) 生体情報全般

生体データについて、Directive 95/46/EC（データ保護指令）では明確には定義されていなかった。同指令では、第 2 条(a)項において、個人情報は'any information relating to an identified or identifiable natural person.'（識別された又は識別され得る自然人に関するすべての情報[44]）として幅広に定義されていた。

これに対し、同指令の Article 29 Working Party (第 29 条作業部会 WP29) は、2003 年に公表した"Working Document on biometrics" (12168/02/EN WP80, Adopted on 1 August 2003)[45]において、「データ保護指令の（個人データの）定義に従って、生体認証手段またはそのデジタルデータはたいていの場合は個人データである」[46]との見解を示し、データ保護指令の主要な原則・規定の適用について整理している。

また、WP29 が 2012 年に出した「意見」（"Opinion 3/2012 on developments in biometric technologies" (WP193, Adopted on 27th April 2012)）[47]では、"[b]iometric systems are tightly linked to a person because they can use a certain unique property of an individual for identification and/or authentication….biometric data, by their very nature, are directly linked to an individual."と記載され、個人に関する特定のユニークな特徴を用いて個人の識別ないし照合を行っているため、

---

44 堀部政男研究室「EU データ保護指令仮訳」より引用。
http://www.soumu.go.jp/main_content/000196313.pdf

45 http://www.statewatch.org/news/2004/feb/biometric-wp80_en.pdf

46 ただし、個人（データ主体）を識別するための合理的な手段として使用されていない場合には、個人データに該当しないとの注記が付されている。（上記 Working Document の脚注 11 参照。）

47 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf

生体情報システムと個人とが緊密に関係していることを指摘している。

当該「意見」（WP193）は、2003 年に出された WP80 以降の状況の変化を受けて出されており、生体データに関する課題について整理した上で、欧州及び各国の立法機関及び生体情報を用いたシステムを提供する産業とそのユーザーを対象として、生体情報を利用する際のプライバシー・データ保護原則に関する統合的なガイドライン・提言を改訂している。

以下にその概要を示す。

a. 背景と目的

- 2003 年の Opinion 公表後、状況が大きく変化した。
  - 生体情報利用が公的分野・民間分野でともに普及してきており、新たなサービスも開発されている
  - 生体情報を利用するために必要な技術リソースとコストが劇的に進化した（安く、速くなった）
  - 顔、静脈などの認証技術は成熟した
- 生体情報は個人の特定の特徴と深く関係しており、その一部は、センシティブ情報を暴くために利用されうる。
- 加えて、生体情報の多くは個人の自動的な追跡（tracking, tracing）やプロファイリングを可能にするものであり、プライバシーやデータ保護に対する潜在的なリスクが高い。

b. 法的な視点からの分析

- 直接的に関係する法的枠組みはデータ保護指令（95/46/EC）である。また、すでに、2003 年の WP80 にて、生体情報はほとんどの場合に個人情報であると述べられている。
- 目的の限定、生体情報利用のメリットとプライバシーリスクの釣り合い、生体情報取扱いの正確性、データの最少化（生体情報は多様な情報を含むことにも留意）、保持期間などの原則を遵守することが重要である。

c. 新たな状況

- 生体情報は、従来は主に政府機関において利用されていたが、近年は商業的組織による利用や開発が増えつつある。技術面での成熟により、生体認証が既存の認証手段を置換または補完するようになっていることが理由の一つである。
- また、生体情報の利用は、従来からの用途である認証・識別にとどまらず、行動分析、監視、不正防止などに広まりつつある。コンピューター技術とネットワークの発展により、生体情報技術の用途は広がってきている。（典型的には、身体的な特徴の遠隔取得によるプロファイリング、遠隔監視、あるいはさらに複雑なタスク（例えば環境知能等）。）

d. プライバシーへの影響

- 生体情報の利用の発展に伴い、プライバシー侵害に対する懸念も高まっている：生体情報が密かに取得、蓄積、処理されることに加え、センシティブな情報が収集されることなどが懸念されている。
- 生体情報を密かに取扱う技術により、個人に気づかれずに識別することが可能になり、その場合、プライバシーや個人データの保護に対する重大な脅威となる。
- 生体情報によりプロファイリングやターゲティングが可能になり、区別する、烙印を押す、望まない情報を知る、といったことにつながりうる。

e. ガイドライン・提言

一般的原則	生体情報について変更できないことから、セキュリティが第一の懸念点であり、生体情報の取扱いに際して、最新の高いレベルの技術的な保護を施すことを推奨する。
プライバシー・バイ・デザイン	生体情報を扱う場合には、システムのバリューチェーン全体について、プライバシーバイデザインの考え・手法を含む開発ライフサイクルを適用することを推奨する。
PIA フレームワーク	生体情報の特徴（ID 不正、生体情報の利用目的の拡大、生体情報の侵害）を踏まえた PIA を行うことが重要である。
技術的手段	・生体情報テンプレートの使用 ・生体情報の保管場所（中央記憶装置よりもローカル端末が望ましい） ・情報の更新・変更が可能（同じ生体情報に対し、複数かつ独立のテンプレートを用いて、認証のための情報を更新できるようにする） ・暗号化、偽造された生体情報への対抗 ・バイオメトリック暗号化・復号化（生体情報を暗号化・復号化に用いる） ・生体情報自動消去 ・大規模データベースではなく弱い結合によるデータベースの使用
組織的手段	生体情報を扱う組織におけるデータ取扱規則等の策定と運用。

(2) 顔認証

WP193 では生体認証全体を対象としているが、オンラインサービス・モバイルサービスにおける顔認証に焦点を絞った Opinion（'Opinion02/2012 on facial recognition in online and mobile services" (WP192)）[48]も出されている。WP192 ではオンラインサービス（例：SNS 等）やモバイルサービス（例：スマートフォンを介して提供されるサービス等）について、想

[48] http://www.pdpjournals.com/docs/87997.pdf

定されるリスクと提言を示している。提言の内容自体は従来からあるものであるが、オンラインまたはモバイルサービスにおけるリスクを整理した点が注目される。

a. 対象とする顔認証技術

WP192 では、対象とするデジタル画像として、2D による顔画像に加え、技術進歩に伴う 3D 画像も含めた、静止画及び動画を挙げている。

また、顔認識技術としては以下を挙げている。

- 画像取得（顔を含む画像の取得・デジタル化：オンラインサービスの場合、デジタルカメラで撮影してアップロードする形態もある。）
- 顔検出（デジタル画像から顔を検出し、対応する画像領域にマーキングする。）
- 正規化（検出された顔画像領域についてのサイズ統一、傾き修正、色分布調整等を行う。）
- 特徴抽出（デジタル画像から再現性のある特徴を抽出するプロセス。顔の全体的な特徴量を算出する”holistic”法と、顔の個々の要素の位置に注目する”Feature-based”法、及びそれらの組合せがある。抽出された特徴は以降の比較に用いるためにテンプレート[49]として保存される。）
- 登録（初めてのユーザーの場合、画像及び/または参照テンプレートを登録し、以後の比較に用いる。）
- 比較（ユーザーの顔・特徴と、予め登録されたものの類似度を計測するプロセス。主たる目的は「識別」、「照合」だが、第三の目的として「分類」がある。顔画像を用いて年齢、性別、服装の色などを分類するもので、この場合には登録プロセスは不要になる。）

b. オンライン及びモバイルサービスにおける顔認証の事例

オンライン及びモバイルサービスにおける顔認証は、その目的により異なった方法で行われるとして、法的検討のために 4 つの典型的事例を示している。

表 3-4　オンライン及びモバイルサービスにおける顔認証の事例

分類	事例
分類 1： 識別（1:n 認証）の手段としての顔認証	**事例 1：** SNS サービスにおいて、ユーザーが自らのプロフィールに画像を付ける、写真をアップロードして他のユーザーと共有する、といったことができる。アップロードした画像について他の個人を識別してタグ付けすることができ、タグは他のユーザーにも共有される。 SNS サービスは、タグ付けされた画像を用いて、個々の登録ユーザーの参照テンプレートを作成したり、ユーザーがアップロードした画像

[49] ここでは、元の画像から抽出された特徴を現すデータ（群）を「テンプレート」と呼んでいる。WP193 にて「生体情報の生データから抽出した、キーとなる特徴」という説明がなされている。

分類	事例
	に対して顔認証システムにより新たなタグを自動的に推奨したりすることができる。 これらの画像は公開されているため、検索エンジンによりキャッシュされる。検索エンジンはサービス内容を充実させるために、スマートフォンで撮影された画像について、類似した画像を探し、SNS サービスのプロフィルページへのリンクを示すような機能を提供する可能性がある。
分類 2： 照合（1:1 認証）の手段としての顔認証	**事例 2：** オンラインサービスやモバイルサービス・デバイスへのアクセス制御において、ユーザー名/パスワードの代わりに顔認証システムを用いる。登録時にはカメラによりユーザーの顔画像が撮影され、対応するテンプレートの作成と記録（デバイスまたはサービスのサーバに保管）が行われる。 認証時には、端末やサービスにアクセスしようとする個人の顔画像が撮影され、登録されているデータと照合の結果、一致しているという判断がシステムによってなされれば、アクセスが認められる。
分類 3： 分類の手段としての顔認証	**事例 3：** 事例 1 の SNS サービスが、保有する画像ライブラリーへのアクセスについて、オンラインでの顔認証サービスを提供する第三者に認める可能性がある。 第三者の提供するサービスの顧客は、顔認証技術を他の製品に組み込むことができる。この機能により、それらの製品は、ユーザーの顔画像の検出と予め設定された基準（例：年齢、性別、気分）に基づく分類を行うことができる。
	事例 4： ゲーム端末で、ユーザーの動き（ジェスチャー）を検出して制御するシステムが用いられている。ジェスチャーによる「制御システムのカメラが撮影した個人の画像は顔認証システムと共有され、ゲームプレイヤーの年齢、性別、気分が推測される。ユーザー体験を高めるため、あるいはユーザーの状況に応じてゲームの状況を変えるために、他の要素も加えたデータに基づいてゲームプレイが制御されている。 同様の方法により、ユーザーの年齢を推定して、年齢制限のあるコンテンツの許可/拒否、広告の表示/非表示を制御している。

c. 顔認証に特有のプライバシーリスク及び提言

以上の事例を想定した上で、顔認証において特に考えられるプライバシーリスクとその対策の提言を行っている。下記に示すとおり、基本的には、オンライン及びモバイルサービスにおける顔認証で典型的に見られる状況・条件を想定して、生体情報としての顔画像及びテンプレートの取得・処理・保管に関して注意すべき事項が示されている。

表 3-5　顔認証に特有の主なプライバシーリスク及び提言

主なリスク	提言
<u>顔認証を目的とした不法な取扱い</u> オンラインでは、データ管理者はさまざまな方法で画像を取得する（例：オンライン及びモバイルサービスのユーザーによる提供、友人や同僚、第三者による提供）。画像にはユーザー自身や、他の登録/非登録ユーザー、画像を取られているという認識のないユーザーの顔が含まれている。取得方法によらず、画像の取扱には法的根拠が必要。	**<u>提言 1：</u>** データ管理者が画像を直接取得する場合（事例 2、4 など）は、データ管理者は、データ主体の有効な同意を事前に得ること、顔認証のためにカメラがいつ動作しているかに関し十分な情報を提供すること、を確実に行わなければならない。
	<u>提言 2：</u> 個人が画像を取得して、顔認証のためにオンライン及びモバイルサービスにアップロードする場合は、データ管理者は、顔認証で生じうる画像処理について、データをアップロードする個人が確実に同意するようにしなければならない。
	<u>提言 3：</u> データ管理者が個人のデジタル画像を第三者から取得する場合（例：Web サイトから複製する、他のデータ管理者から購入する）は、データ管理者は、オリジナル画像のソース及び取得・処理された状況（データ主体が処理について同意している場合に限る）について注意深く考慮しなければならない。
	<u>提言 4：</u> データ管理者は、提供されたデジタル画像及びテンプレートが指定された目的にのみ用いられることが確実になるように対応しなければならない。データ管理者は、デジタル画像が、データ主体が同意していない目的のために第三者によって処理されるリスクを低減するため、技術的な制御を設けるべきである。
	<u>提言 5：</u> データ主体は、登録されていない個人や、そのような処理に同意していない個人のデジタル画像が、データ管理者が正当な利益を有している限りにおいて取扱われるようにしなければならない。 例えば事例 1 では、マッチする画像がない場合には、処理を中止しすべてのデータを削除する。
<u>転送時のセキュリティ侵害</u> 画像取得とその他のプロセスとの間で画像データの転送（例：撮影した画像データのアップロー	**<u>提言 6：</u>** データ管理者は、データ転送におけるセキュリティを確保するために、適切な対策を施さなければならない。これには暗号通信チャネルや取得した画像自

主なリスク	提言
ド）が行われる可能性が高い。	体の暗号化も含まれうる。とくに照合（1:1 認証）の場合には、可能であれば、ローカル（端末）での処理が望ましい。
<u>データ最少化</u> 顔認証により作成されたテンプレートには、指定された目的のために必要な以上のデータが含まれる可能性がある。	<u>**提言 7：**</u> データ主体は、テンプレート作成のためにデジタル画像から抽出されたデータが、過度でなく、指定された目的に必要なデータのみを含み、それによって、さらなる処理が避けられるようにしなければならない。テンプレートは、顔認証システム間で転送できないようにすべきである。
<u>保管時のセキュリティ侵害</u> 識別や照合を行う場合には、テンプレートの保管が必要になる可能性が高い。	<u>**提言 8：**</u> データ管理者は、データの保管に最も適した立地について考慮しなければならない。ユーザーのデバイス、あるいはデータ管理者のシステム内部、もこれに含まれうる。 データ管理者は、保管されているデータのセキュリティを確保するために適切な措置をとらなければならない。テンプレートの暗号化も含まれうる。 テンプレートやデータ保管ロケーションへの不正アクセスが可能となるべきではない。 とくに照合を目的とする顔認証の場合には、生体情報の暗号化技術を用いるべきである：この技術により、暗号鍵は生体データと直接結びつき、照合に際して生きた正しい生体データが提示されたときにのみ、再生性されるため、画像やテンプレートは保存されない（したがって、”追跡不能な生体情報”となる）。
<u>データ主体のアクセス</u>	<u>**提言 9：**</u> データ管理者は、データ主体に対し、適切な仕組みにより、アクセス権を提供しなければならない。可能な場合には、オリジナル画像及び顔認証のために生成されたテンプレートの両方について、アクセスを提供しなければならない。

なお前述のとおり、WP192 はオンライン・モバイルサービスにおける顔認証を対象としているが、それ以外の用途における顔認証、例えば監視カメラにおける顔認証については WP193 にて議論されている。WP193 では、監視カメラに顔認証機能が備わった場合にどのようなデータ保護リスクが考えられるかなどについて、以下を示している[50]。

・ 正確性：顔画像の品質が低い場合（例：髪型や帽子、ポーズや照明の影響）、認証

[50] WP193 の 4.4.3 節（pp.21-23）参照。

の正確性に影響する

- 影響：顔認証システムの影響は、その目的や使用条件により異なる（例：来場者の属性分析システムと捜査機関による問題人物の識別システム）
- 同意と透明性：顔認識の場合、他の生体認証と比較して、幅広い地点や環境条件での観測が可能、データ主体に気づかれずに観測が可能、という特徴をもつが、データ主体が気づかない場合、同意を取得したとはいえない（単に監視カメラが作動していることがわかるだけでは、顔認証に気づいているとはいえない）
- 他の用途での顔画像の利用：取得された顔画像は、適法・違法を問わず、他の用途・システムに容易に共有・複製される（例：SNS サービスでユーザによりアップロードされた画像）
- 連関性：多くのオンラインサービスではユーザのプロフィールに顔画像をアップロードすることが可能になっているが、これらの顔画像はオンラインサービスの間だけでなく、監視カメラなどオフラインで取得された顔画像とも照合することが可能な場合があり、リアルタイムに、いつ・どこに誰がいるかが検出されてしまう可能性もある
- 追跡・プロファイリング：商業施設や公的空間では、来訪者の動線分析を行って、売り場の検討や行列の管理などに役立てているが、この技術を用いて、特定の個人に対してターゲット広告やその他のサービスを届けることも可能である
- センシティブデータの取扱い：顔認証に用いる画像により、センシティブ情報（例：人種、民族、健康状態など）を推知することが可能である
- 取消し可能性：個人は顔の“見た目”（髭、眼鏡、帽子など）を容易に変更することができ、そのことにより顔認証システムを欺くことが可能である一方、顔の主たる特徴は安定しており、認証システムは、異なる多くの画像を収集することで認証能力を向上させることが可能である
- 成りすまし対策：多くの顔認証システムでは成りすましによる認証が容易であり、認証システムのメーカーは 3D 画像や動画などを用いた成りすまし対策に取り組んでいるが、公的用途で用いられている最も基本的な認証システムではこの機能は取り入れられていない

3.5 EU 加盟国

EU 加盟国については、2018 年 5 月の GDPR 発効後は GDPR の規定が直接適用されるが、ここではそれ以前の状況、あるいは各国が独自に行っている取組について記載する。

(1) イギリス

a. データ保護法

イギリスにおける個人情報保護に関する現行法は、公的部門と民間部門に適用されるデ

ータ保護法（The Data Protection Act 1998：以下「1998 年法」）[51]である。それ以前は 1984 年データ保護法が自動処理データのみを対象として制定されていたが、データ保護指令（Directive 95/46/EC）に対応して改正された。

生体情報については、1998 年法においては明示的な規定はないが、情報コミッショナーオフィス（Information Commissioner's Office: ICO）が、生体データが個人情報に当たることを認めていた[52]。

なお、2017 年 9 月に、1998 年法を改正する法案（Data Protection Bill 2017）[53]が議会に提出されている。同法案にはバイオメトリクスの定義も明記されている[54]が、その内容は GDPR の定義と同じである[55]。また、主な規制内容として以下が挙げられる。

- データの取扱いについては GDPR の基準を導入している
- センシティブな健康、ソーシャルケア、教育に関するデータに関して機密性が保護されること
- 国家の安全を含む公共政策で強い正当性がある場合には、アクセス権、削除権について適切な制限がされること
- オンラインでのデータの取扱いについて、親の同意が必要ない年齢を 13 歳に定める[56]

b. 監視カメラに関する行動規範

イギリスでは監視カメラの設置･利用が進んでいたことから、GDPR 策定以前から、監視カメラに関する規制が検討されている。監視カメラに関する第三者機関としては、個人データ保護全般を所管する ICO に加え、監視カメラコミッショナー（Surveillance Camera Commissioner: SCC）が設置されている。SCC は 2013 年にカメラ設置・利用に関する Code of Practice（行動規範）[57]を定めている。この行動規範は 2012 年自由保護法（Protection of Freedoms Act 2012）[58]の第 30 条に基づき定められたもので、イングランド及びウェールズの関連当局（第 33 条で規定）に対して、適切かつ効果的な監視カメラの利用に関するガイ

---

[51] 女王の裁可：1998 年 7 月 16 日、施行：2000 年 3 月 1 日。
http://www.legislation.gov.uk/ukpga/1998/29/contents

[52] https://ico.org.uk/media/about-the-ico/documents/1042564/ico-proposed-dp-regulation-analysis-paper-20130212.pdf

[53] https://services.parliament.uk/bills/2017-19/dataprotection.html
https://publications.parliament.uk/pa/bills/cbill/2017-2019/0190/18190.pdf

[54] 法案第 196 条(1)の冒頭に記載されている。

[55] 法案の概要（Overview）を記載した文書では、' Set new standards for protecting general data, in accordance with the GDPR,(略) 'とあり、GDPR の内容と基本的に同じである旨の記載がある。（以下の文書の' How are we going to do it?'の項。）
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/685647/2018-03-05_Factsheet01_Bill_overview.pdf

[56] オンラインでの個人情報の取得とは別に、学校での生体情報（指紋）の利用（各種の本人認証や、図書館での貸し出しで使われている）についても、ICO によりガイドライン等が従前より定められている。以下等を参照。https://ico.org.uk/for-the-public/schools/fingerprinting/
http://www.statewatch.org/news/2007/jul/uk-biometrics-in-schools.pdf

[57] https://www.gov.uk/government/publications/surveillance-camera-code-of-practice

[58] http://www.legislation.gov.uk/ukpga/2012/9/contents

ダンスを提供するものである。イングランド及びウェールズにおける、他の監視カメラ運用者・利用者に対しては、この行動規範を自発的に採用することが奨励されている。

行動規範では以下の 12 の原則が定められている。

＜監視カメラシステムの開発または使用＞

原則 1 : 監視カメラシステムは、常に、適法な目的を実現するために、かつ明確な緊急の必要性のために必要な範囲において、指定された目的のために使用されなければならない。

原則 2 : 監視カメラシステムの使用に際しては、その使用が正当であることを確保するための定期的な検査により、個人に対する効果とプライバシーが考慮されなければならない。

原則 3 : 監視カメラの使用においては、情報へのアクセスや苦情に関する公表された連絡先を含む形で、可能な限りの透明性が確保されなければならない。

原則 4 : 監視カメラシステムの全ての活動（収集・保管・使用された画像及び情報を含む）について、明確な責任及び説明義務が存在しなければならない。

＜監視カメラシステムにより得られる画像または他の情報の使用または処理＞

原則 5 : 監視カメラシステムの使用に先立ち、明確なルール、方針、手順が設けられ、かつ、それらに従うべき全ての者に伝えられなければならない。

原則 6 : 監視カメラシステムに関する記載された目的のために厳密に必要な以上の画像及び情報は蓄積されるべきではない。また目的が解除された時点で、それらの画像及び情報は削除されるべきである。

原則 7 : 保持されている画像及び情報へのアクセスは制限されるべきである。また、誰がどのような目的でアクセスできるのかについての明確な規定が必要である : 画像及び情報の開示は、それらの目的のために必要な場合、あるいは法執行目的の場合に限るべきである。

原則 8 : 監視カメラシステムの運営者は、システム及びその目的と関連のある、運営、技術、権限に関する承認されたいかなる標準についても考慮すべきである。また、それらの基準を満たし維持するよう努めるべきである。

原則 9 : 監視カメラシステムの画像及び情報は、許可されていないアクセス及び使用を防ぐための適切なセキュリティ対策に従うべきである。

原則 10 : 法的要件、方針、基準が現実と適合しているかに関する検査及び監査の効果的なしくみが設けられるべきである。また定期的な報告が公表されるべきである。

原則 11 : 監視カメラシステムの使用が、適法な目的を実現するためであり、かつ明確な緊急の必要性が存在する場合に、公共の安全及び法執行のために、証拠の価値としての画像及び情報の処理を目的として、最も効果的な方法で使用されるべきである。

原則 12 : 監視カメラシステムにおいて、照合を目的として参照用データベースと比較するために用いられるいかなる情報も、正確でありかつ最新であるべきである。

これらの原則のうち、原則 2、8、12 については、顔認証システムについても言及されており、監視カメラシステムによる安全の確保と、個人のプライバシーとのバランスに留意すべきことが上記行動規範において説明述されている。

なお、GDPR の第 9 条において生体情報を含む「特別な種類の個人データの取扱い（Processing of special categories of personal data）について規定されているが[59]、第 4 項では「加盟国は、制限を含め、遺伝データ、生体データ又は健康に関するデータに係る追加的規定を維持又は導入することができる。」[60]と規定されており、これらの法制度は GDPR 発効後も有効になると考えることができる。

c. 監視カメラの利用動向

英国では、空港（例：ヒースロー空港における電子パスポートゲート、ビザ写真の照合、犯罪者データベースとの照合）、警察（拘留者データベースにおける顔画像による識別）、地下鉄（ロンドン地下鉄は乗降客の行動検知による事故防止、駅施設の運行管理、乗降客数カウントなどを内務省、警察、大学研究者、システムベンダーと共に検討）など公共部門での利用に加え、小売業店舗など商業施設、住宅地域でも顔認証を用いた監視カメラの利用が進んでいる[61]。

d. 監視カメラに関する認証制度

SCC は、監視カメラシステムの透明性を高めるために、2015 年 11 月に第三者認証制度を設けた[62]。上記の行動規範の適用対象とされている関連当局のほか、民間企業が自主的に申請することも認められている。具体的には、上記の行動規範の 12 原則を遵守していることについて、最初に自己評価ツール[63]による評価を行い、次に独立した認証機関による審査を実施して、認証を行う[64]。

2016 年 11 月時点で、警察、小売事業者、大学、病院等約 40 の組織が認証を取得しているといわれる[65]。

(2) フランス

フランスでは職場における生体認証に関する規則が定められている。2016 年 9 月 27 日に、フランスのデータ保護機関の CNIL（Commission nationale de l'informatique et des libertés: 情報処理及び自由に関する国家委員会）は、職場における全ての生体認証制御システム（施

---

[59] 第 3.4.1 節(2)では第 9 条第 1 項及び第 2 項について記載したが、同条には第 3 項（特別な種類の個人データの利用目的の制限に関する例外）及び第 4 項もある。

[60] 原文は” Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health.”

[61] 小泉雄介「英国・米国におけるカメラ画像と顔認識に関する動向」（2017 年 10 月 5 日）https://www.i-ise.com/jp/information/report/20171010_koizumi.pdf

[62] https://www.gov.uk/government/publications/surveillance-camera-code-of-practice-third-party-certification-scheme

[63] https://www.gov.uk/government/publications/surveillance-camera-code-of-practice-self-assessment-tool

[64] https://www.gov.uk/government/publications/complying-with-surveillance-camera-code-of-practice-self-assessment-and-third-party-certification/complying-with-surveillance-camera-code-of-practice-self-assessment-and-third-party-certification

[65] 小泉 雄介「英国・米国におけるカメラ画像と顔認識に関する動向」（2017 年 10 月）https://www.i-ise.com/jp/information/report/20171010_koizumi.pdf

設、ソフトウェアアプリケーション及びデバイスへのアクセス）を対象とする 2 つの認可 "Single Authorizations AU-052[66] 及び AU-053[67]"を発表した。これらの規則では、規則が対象とする主体（民間組織及び公的組織で、それぞれ条件に該当するもの）、生体情報の利用が認められる目的、取扱われる個人データ（生体情報も含む）。データ保持期間、データの利用が許される者、データ主体に通知すべき内容、セキュリティ及び信頼性に関する要件などが定められている。またそれに伴い、従来からあった規則である Single Authorizations AU-007[68], AU-008[69], AU-019[70], AU-027[71]を廃止した。

これらの決定は、2018 年 5 月に施行される GDPR に対応したものであり、プライバシーバイデザイン(PbD)とプライバシーバイデフォルトのプライバシー原則、データ保護影響評価を採用している。これらについて、データ管理者は 2018 年 5 月 25 日までに対応しなければならないとされている。なお、一般的に、生体情報システムについては CNIL の事前許可が必要とされているが、これらの Single Authorizations に規定されている要件を満たせば、簡易届出とすることが可能であった。従来の認可制度（簡易届出）により申請した事業者は 2 年以内（2018 年 9 月まで）に新しい認可制度に対応して新規に登録するか、または CNIL の監査を受ける必要がある。GDPR では、生体情報の取扱いについて加盟国が追加的な制限をすることを許可しており（第 9 条第 4 項）、フランスではより厳格な制限がされている。

a. 背景

2006 年以降、CNIL は、生体情報システムについて「追跡不能なもの」(traceless)と「追跡可能なもの」(traceable)という区別を行ってきた。

追跡可能な生体情報システム（例：指紋認証）では、個人（データ主体）が認識することなく、パーソナルデータを取得・利用することが可能である。他方、追跡不能なシステム（例：掌形認証や指の静脈パターン認証）では、個人の認識なしにデータを追跡することは困難である。そのため、CNIL は追跡可能な生体認証システムには、個人のプライバシーに対してより高いリスク（例：ID 窃盗等）があるとして、追跡不能な場合と比べ、より厳格なルールを課してきた。しかしながら、新技術の進展により、これらの区別はもはや意味がなく、全ての生体認証が「追跡可能」と考えるべきだとして、新しいルールを制定した。

b. ポイント

新しい制度では、データ主体が自己の情報についてコントロール可能か否かによって適用されるルールが異なる。

- 個人が生体テンプレートに対するコントロールを保持できる生体情報システムであ

[66] https://www.cnil.fr/fr/declaration/au-052-biometrie-controle-dacces-sur-les-lieux-de-travail-avec-maitrise-de-la-personne

[67] https://www.cnil.fr/fr/declaration/au-053-biometrie-controle-dacces-sur-les-lieux-de-travail-avec-conservation-des-gabarits

[68] 職場における手の輪郭・形状を用いたアクセスコントロールについて定めた規則。

[69] 職場における指紋の利用に関する規則。

[70] 職場における手の静脈の利用に関する規則。

[71] 職場における指紋を用いたアクセスコントロールについて定めた規則。

れば、AU-052 が適用される。具体的には、個人が保有しているデバイス（例：IC カードや USB キー等）又は個人の関与なしに利用できないようなデータベース（例：テンプレートの暗号を解除するための秘密鍵を個人のみが保有する場合）にテンプレートが保存されている場合などが該当する。なお後者は、前者の方法を選択することが不可能なことについて正当な理由がある場合に認められる。

- 個人が自己の生体情報テンプレートをコントロールできない生体情報システムについては、より厳格なルールである AU-053 が適用される。この場合、データ管理者はテンプレートを①個人の認証番号と関連づけられるデータベース、②認証時にサンプルとの比較を行う内部記憶装置で、データやテンプレートの抽出が可能な通信ポートを持たないもの、のいずれかにテンプレートを保管することができる。また、データ管理者は、その目的に関して（生体情報によらない方法ではなく）生体情報を用いる方法を選択したこと、ユーザーのコントロールが制限される方法でテンプレートを保存すること、の二点に関する正当な理由を書面で残すことが求められる。

CNIL は、データ主体が生体情報テンプレートをコントロールできる生体アクセス制御システムを使うことを事業者・組織に推奨しており、そうでないシステムを使う場合には、AU-053 が適用され、analysis　grid と呼ばれるチェックリスト[72]への記入が必要になる。

(3) ドイツ

ドイツには、公的機関及び民間に適用される連邦法として、連邦個人データ保護法（Bundesdatenschutzgesetz in German: BDSG）[73]が存在する。

ドイツにおいては、個人データ保護に関する概念は、憲法上の人間の尊厳と人格の保障（GG（ドイツ憲法）第 1 条第 1 項、第 2 条第 1 項）から派生したこともあり、データ主体の同意を得た場合（BDSG 第 4 条）にのみ、個人データの処理が許可されるとされている（いわゆる情報の自己決定権）。

IP アドレスやクッキー等の電子通信データは基本的に「個人データ」として認められているが、重大な犯罪やテロ等の捜査のために電子通信プロバイダが保持する必要がある。また、匿名化・仮名化した後の利用は認められている。

BDSG における個人情報の定義は以下のとおり整理される。

・ 特定または識別可能な個人的または物的環境に関するすべての情報を指す。（第 3

[72] https://www.huntonprivacyblog.com/wp-content/uploads/sites/18/2016/09/au-053-grille_danalyse_des_risques_0.pdf

[73] BDSG は 1978 年に制定され、当初は、「個人データ」の範囲（特に、電子通信関連）に関する議論が多く行われたが、最近は、2018 年に施行予定の GDPR との関連で技術ベースの監視問題とプロファイリングが主な論点となっている。BDSG では、特定の公務利用、研究、メディア利用等の「個人データ」取扱いについては特別の規定を設けている。また BDSG は、国境を越えるデータ転送に関し、「信頼できる国」とその他の国を分けて、それぞれに対し異なる規定を設けている。他方、クラウドサービスにおいては、クラウド内のデータの物理的な場所を特定の国の特定のサーバに固定的に対応づけることが困難なため、複数の管轄区域をまたぐデータの転送が必然となる。したがって、当該規定に対し、クラウドサービスを提供する企業から異議が出されている。さらに、データ保護責任者（DPO）の設置を要求することも規定されている（第 4f 条）。

条第 1 項）
・ 人種や民族的起源、政治的意見、宗教的または哲学的信念、所属団体、健康または性生活に関する情報は要配慮個人データとして指定される。（第 3 条第 9 項）

また具体的な規制内容の概略は以下のとおりである。
・ 事前登録義務 : 自動化処理を運用する前に、管轄機関に登録しなければならない。（第 4d 条）
・ 匿名化以外に、仮名化（Aliasing）を通じて処理することは認められる。（第 3 条第 6a 項）
・ 公の場におけるビデオ監視も個人データとして規制される。（第 6b 条）
・ モバイルにおける自動処理に関する規定がある。（第 6c 条）
・ 「個人データ」の範囲は、基本的に EU 全体での認識と違わないが、プライバシーと技術実現可能性等に鑑み、比例原則によって判断する。例えば、仮名化されたデータを市場調査や広告等のために使うことは認められている（TMA (Telemedia Act 2007)、第 15 条 3 項〕。

3.6 小括・補足

各国における法制度や議論の状況についてのまとめ及び補足は以下のとおりである。

①生体情報・DNA
- 生体情報のプライバシーについての議論や法制度化は、2000 年代前半から行われており、ガイドライン策定やオピニオン公表なども行われてきた。
- 2010 年代に入り、生体情報利用の拡大（とくに民間分野）をふまえ、米国、カナダ、EU では、新たな議論が行われた。
  ・ 米国、カナダでは生体情報利用に関するガイドが政府機関により策定・公表された。
  ・ EU では、新たなオピニオンが公表されるとともに、GDPR においても生体情報や個人識別符号が明示的に定義された。
- 2010 年代の議論では、生体情報の漏えいや不正利用といった従来の論点に加えて、①データ主体が認識できない状況での取得、②利用目的以外での利用（クロスマッチングや二次情報）、③不特定多数からの個人の識別やプロファイリング、遠隔監視等に関する懸念、などがそれぞれの国・地域において示されている。
- 立法化については、EU では GDPR にて明文化されたが、米国やカナダでは既存のプライバシー法の枠組みに上記ガイド等を組み合わせる形で規制している。
  ・ 米国では州法において規制しようとする動きが 2008 年からあるものの、事業者の激しい抵抗にあって立法化されないか、立法化されても表面的なものにとどまっている。
  ・ Google, Facebook, Amazon.com Inc., Wal-Mart Stores Inc.等の事業者は、マーケティングとセキュリティのために顔面認証技術を使うことに実務的な利便性があると指摘。厳格な法律は（高精度な本人認証技術の使用を妨げることになり）逆に詐欺を招く、生体情報を使って詐欺やセキュリティ面での検知を行うことができると

主張。特に詳細な通知や同意を義務づける要件は、生体情報の利用に賛成するユーザーから同意を得にくくすると主張した[74]。

- EU からの離脱を決めたイギリスでは、2017 年 9 月に新法案 Data Protection Bill 2017 が出されている。

- DNA については、国家による蓄積についての懸念が示されている例もある。
  - イギリスでは、世界最大規模の国家 DNA データベースがあり、容疑者および遺留資料から採取したものが収容されている[75]。
  - これに対して、EU 市民のプライバシー権利に関わる事案を扱う最高位の裁判所である欧州人権裁判所（European Court of Human Rights: ECHR）は 2008 年に、無罪になった者（又は逮捕されたが起訴されていない者）の DNA サンプルを保持することは、ヨーロッパ人権条約（EU's Convention for the Human Rights and Fundamental Freedoms (the "Convention")）に違反すると判示した。
  - これにより当該データベースは 520 万人の DNA を持っていたところ、850,000 程度のデータ（容疑者であったが無罪となった者の DNA サンプルの数と考えられる）を削除することになるのではないかとみられている(注：2008 年当時の状況）[76]。なお、米国でも同様の議論がある[77]。

②ID

- ID については、各国・地域とも個人情報保護・プライバシー保護に関する法律において規定されており、それぞれの法律が定めるところにより規制されている。
  - 米国では PII (Personally identifiable information)がプライバシー法において規定されている他、HIPPA（医療保険の携行性と責任に関する法律）でも個人が特定可能な保健情報の取扱いについて定めている。州レベルでもカリフォルニア州法が PII の取扱いを規定している。また標準化機関である NIST も PII の定義や望ましい取扱いについて定めるなど、さまざまな階層にて規制が定められている。
  - カナダ、シンガポールでも個人情報保護に関する法律にて規定されている。
  - EU では、GDPR において、「個人データ」として「識別番号」や「オンライン識別子のような識別子」が挙げられており（第 4 条(1)）、GDPR における各規定が適用される。また GDPR 第 87 条では、「加盟国は国民識別番号又は一般に用いられるあらゆる識別子の取扱い関する具体的条件を定めることができる。その場合、国民識別番号又は一般に用いられるあらゆる識別子は、本規則によるデータ主体の権利及び自由のため、適切な保護措置下でのみ、利用されなければならない。」と定めており、具体的な規定については加盟国に委ねられている。

---

74 https://www.bloomberg.com/news/articles/2017-07-20/tech-companies-are-pushing-back-against-biometric-privacy-laws

75 http://www.ndl.go.jp/jp/diet/publication/refer/200601_660/066002.pdf

76 http://www.ndl.go.jp/jp/diet/publication/refer/200601_660/066002.pdf

77 https://privacylaw.proskauer.com/2008/12/articles/european-union/eu-high-court-strikes-down-uk-dna-database-on-privacy-grounds/

4. 利用動向・技術動向

第 4 章では、個人識別符合の利用動向、技術動向について整理する。

4.1 現在の主な利用事例

4.1.1 全体動向

国内における個人識別符号の利用事例について、典型的または特徴的なものを以下に示す。

表 4-1　国内における個人識別符号の利用事例

	個人認証	その他
顔	NEC：「顔認証エンジン NeoFace」 http://jpn.nec.com/pcserver/appliance/faceset/index.html 東芝インフラシステムズ：「顔照合技術」 https://www.toshiba.co.jp/sis/scd/face/index_j.htm オムロン：「顔認証」 https://plus-sensing.omron.co.jp/function/face-authentication/	オムロン：「画像センシング技術 OKAO Vision」 http://plus-sensing.omron.co.jp/technology/detail/
虹彩	サムスン：「Galaxy S8 虹彩認証」 http://www.galaxymobile.jp/galaxy-s8/security/	
声紋	鹿児島銀行：「声紋認証機能」 http://www.kagin.co.jp/library/pdf_release/newsh291016_022.pdf	
歩容	大阪大学：「深層学習モデルによる歩容認証」 http://www.sanken.osaka-u.ac.jp/toppage/hot_topics/topics_20171108/	大阪大学：「歩容における性別・年齢の分類と特徴解析」
静脈（手のひら、手の甲、指）	富士通：「手のひら静脈認証 PalmSecure」 http://www.fujitsu.com/jp/solutions/business-technology/security/palmsecure/ 日立製作所：「指静脈ソリューション」 http://www.hitachi.co.jp/products/it/veinid/index.html	
指紋・掌紋	NEC：「指紋認証・指静脈認証」 https://jpn.nec.com/biometrics/fingerprint/index.html Liquid 他：「Touch&Pay」	

	個人認証	その他
	http://miqip-info.jp/jp/service10/ KDDI 研究所:「掌紋認証アプリ『てアロ』・アルゴリズム」 http://www.kddi-research.jp/newsrelease/2012/100101.html	
DNA	法科学鑑定研究所：「民間 DNA 鑑定サービス」 http://alfs-inc.com/	京都大学：「またいとこがわかる血縁判定法」 http://www.kyoto-u.ac.jp/ja/research/research_results/2016/documents/160729_2/01.pdf
ID（番号）	徳島県：「マイナンバーカードを用いた認証システム」 http://jpn.nec.com/press/201706/20170621_05.html	

国内では、顔認証、指紋・掌紋、静脈などについて、製品・ソリューション提供や導入が進んでいる。とくに静脈については認証精度が高く、またユーザーが自覚的に生体情報を提示する必要があり（遠隔等での取得ができない）、また体内の情報であることから偽造が難しい等の理由で、金融機関での導入が多くみられる。

虹彩については、従来は専用センサ・機器が必要であったが、スマートフォンに搭載可能なセンサの実現により、今後普及するのではないかと期待されている。

声紋、歩容については、ディープラーニングの導入により認証精度が著しく向上しているとされるが、現在はまだ研究開発段階にある。他方、スマートフォンや AI スピーカーなど音声を入力する機器の普及（声紋）、あるいは遠隔で低精細度の画像でも識別可能といった技術的特徴（歩容）などから、今後の実用化・利用が期待されている。

4.1.2 事例

上記のうち、必ずしも代表的な事例ではないが、いくつかの事例を示す。

(1) 指紋認証による各種サービスの提供プラットフォーム

最初に、生体認証（指紋認証）を用いて各種のオンラインサービスを提供する取り組みである Touch&Pay を示す。これは、さまざまなサービスの提供、予約、決済などを指紋認証により本人確認を行うことで提供するものである。指紋認証はスマートフォンでのロック解除に導入されたことで急速に普及しているが、オンラインでのサービス提供や決済等のプラットフォーム的な位置づけで用いられているという点が注目される。

サービス概要		サービスイメージ
事業社名	Liquid、JTB、日本観光振興協会 等	  出典URL：http://miqip-info.jp/jp/service10/
サービス名	Touch&Pay	
サービス内容	➢ 主に訪日外国人をターゲットとした、指紋認証の活用により様々なサービスを享受できる次世代プラットフォーム。 ➢ 指紋認証により、電子決済やイベント会場への入場手続き等を行うことが可能。 ➢ 経済産業省の「IoT推進のための新ビジネス創出基盤整備事業」の一環として2016年10月より関東地区を中心にサービスを展開。2017年10月からサービス範囲を全国に拡大し、本格導入を開始する。	

背景・目的	実績	課題と今後の展望	個人情報保護上の論点（例）
➢ 指紋認証を活用した多様なおもてなしサービスを提供することで、ストレスフリー観光を実現し、サービス事業者の生産性の向上と消費の促進を目的としている。	➢ 2016年より関東地区を中心に200を越える施設でサービス実証を実施済み。	➢ 今後はホテルのチェックインや免税手続きの簡略化サービス等を展開予定。	➢ 指紋情報が電子決済を含むあらゆるサービスと紐付くため、偽造指紋等により個人が様々な不利益を被るリスクがある。

図 4-1　Touch&Pay の概要

(2) 民間 DNA 鑑定サービス

次に、民間 DNA 鑑定サービスの事例を示す。

捜査や医学などの専門家を中心に利用されてきた DNA 鑑定が、この事例では広く一般企業・個人にも提供されており、今後の普及が期待される一方、プライバシーリスクとしてどのような問題が生じうるのかという点も注目される。

サービス概要		サービスイメージ
事業社名	法科学鑑定研究所	 出典URL：http://alfs-inc.com/
サービス名	民間DNA鑑定サービス	
サービス内容	➢ DNA分析による個人識別鑑定、血縁鑑定、企業向けDNAバンクの構築サービスを展開。 ➢ 口内粘膜、血液（以上は細胞そのもの）、歯ブラシ、吸い殻（以上は残っている細胞片）等、様々な資料を用いた鑑定が可能。 ➢ 99%以上の高精度な鑑定を実現。 ➢ 官公庁・公的機関から個人まで幅広い依頼に対応。	

背景・目的	実績	課題と今後の展望	個人情報保護上の論点（例）
➢ 一般企業や個人が安心して依頼できる中立、公平な民間の法科学鑑定機関を目指している。	鑑定実績例： ➢ 警察庁、防衛省 ➢ 東京高等裁判所 ➢ 東京大学、京都大学 ➢ 弁護士・法律事務所 ➢ テレビ局、新聞社 等	➢ 鑑定技術の向上、裁判を有利に進める理解しやすい鑑定書の実現。	➢ DNA鑑定に使用する試料が本人の同意なしに持ち込まれる可能性がある。

図 4-2　民間 DNA 鑑定サービスの概要

(3) マイナンバーカードを用いた認証システム

ID を用いた認証システムとして、マイナンバーカードを県庁の職員証として使用している例を示す。マイナンバーカードの空き領域に利用者用 ID を追加し、これと職員情報を紐付けることで入退室や PC へのログオンに用いている。

実際にはマイナンバーカードに記載されているマイナンバー（ID）そのものを用いるわけではなく、IC カードという媒体を用いていることになるが、他方で公的な身分証明書類等を他のサービスの認証に用いることはハードルが高いため、ここではその前段階という位置づけで示した。なお、1.2 節に記載したとおり、ドイツでは、本人の同意に基づき、新国民 ID カード(eID)に対応する個人属性情報を事業者が取得することが可能となっている。

サービス概要		サービスイメージ
事業社名	徳島県	
サービス名	マイナンバーカードを用いた認証システム	
サービス内容	➢ マイナンバーカードを職員証として利用する「利用者ID登録システム」を導入。 ➢ 職員は、職員証とマイナンバーカードを重ね合わせて挿入可能な専用のカードケースを携帯。 ➢ マイナンバーカードのICチップ内の空き領域に追加した利用者識別用IDと職員情報を紐付けることで、入退室管理やPCログインなどの際に、マイナンバーカードをカードリーダにかざすことで本人認証を実現。	

背景・目的	実績	課題と今後の展望	個人情報保護上の論点（例）
➢ 情報セキュリティの確保と行政事務の効率化、職員の利便性向上を目的に導入。	➢ 2017年6月に稼動を開始し、マイナンバーカードによる入退室管理やPCログインを実現。	➢ 更なるマイナンバーカードの利用拡大と職員業務の効率化を推進する予定。	－

図 4-3　マイナンバーカードを用いた認証システムの概要

4.1.3 海外における利用動向の整理例

生体認証技術を提供する企業の団体である IBIA（International Biometrics + Identity Association）は、各生体認証技術の主な用途として以下を挙げている。

最も幅広く使われている認証方式は指紋で、次いで顔となっている。他の生体データは、その特徴に応じた利用分野の傾向がややみられる。

用途についてみると、法執行、出入国管理、防衛・テロ対策、アクセス管理においてはさまざまな生体データが利用されている。

他方、IBIA は米国のベンダが多く参加しているため、用途として「法執行」「出入国管理・旅客安全」「防衛・テロ対策」が多くなっている傾向があるが、指紋、掌紋、顔、虹彩は他の用途でも広く使われているとの指摘も有識者からあった。

表 4-2　IBIA（業界団体）が示す生体認証技術の利用事例

	法執行	出入国管理・旅客安全	防衛・テロ対策	反人身売買	災害犠牲者特定	教育	金融	ヘルスケア	サイバーセキュリティ	ゲーム	消費者サービス・決裁	人材	選挙	アクセス管理
指紋	●	●	●			●	●	●	●			●*1	●	●
掌紋	●	●	●											●
顔	●	●	●						●	●				●
眼（虹彩）	●	●	●					●	●					●
眼（強膜）							●	●	●					●
眼（網膜）							●							●
声紋	●								●		●			●
行動	●	●	●											
DNA	●		●	●	●									

出所：IBIA Web サイト[78]より作成

[78] https://www.ibia.org/biometrics-and-identity/biometric-technologies

4.2 技術･標準化の動向

次に、個人識別符号（とくに生体情報）に関する技術動向について記載する。

4.2.1 生体情報の特徴及び比較

個人情報保護法･施行令にて提示されている生体情報について、その概要及び特徴を整理すると以下のようになる。

表 4-3　生体情報の特徴比較（1）全般

生体情報	対象とする情報	センサ	取得形態	認証精度	取得時の本人の認識
顔	顔の特徴（例：目鼻の凹凸、傾き、配置等）	カメラ	遠隔	○	知らずに取得される可能性あり（監視カメラ等）
虹彩	虹彩の画像パターン（同心円状の濃淡配列パターン）	カメラ(近赤外光)	近接/遠隔	◎	遠隔カメラでの取得では、本人が知らないうちに取得されることもある
声紋	音声信号のうち、話者の特徴を現す信号（因子分析による特徴抽出）	電話音声、マイク音声、無線傍受、インターネット映像に付随した音声	遠隔	△	知らずに取得される可能性あり（マイク等）
歩容	歩行動作のシルエット画像（以前は歩行モデルが主流だった）	画像センサ 深度センサ 加速度センサ	近接/遠隔	○	知らずに取得される可能性あり（監視カメラ等）
静脈	手指や手のひらの皮膚内部の静脈パターン	静脈センサ(画像センサ)	近接	◎	本人が知らずに取得することはできない（本人がセンサに手のひらまたは手指を当てることが必要）
掌紋	手のひら全体に見られる一定間隔に並んだ紋様の皮膚隆起線	カメラ	近接/遠隔	◎	動画にも対応しているので、認証エリアの位置決めができれば遠隔での取得も可能
指紋	指紋特徴点（端点・分岐点）群の配置（距離・角度、隆線方向）	指紋センサ(光学方式、静電容量方式、電解強度方式)	近接	◎	遺留物から指紋を収集する場合には、本人が知らずに収集される

出所：有識者（生体認証研究者）へのヒアリングに基づき作成

なお、認証精度については、さまざまな要素が関係するため単純に比較することはできないが、有識者へのヒアリングをふまえ、非常に大まかな相対的関係として記載している。

なお、実際に生体認証方式を選択する際には、上記のほかにも認証精度、耐ノイズ性、耐環境変動性、コスト、技術的成熟度等さまざまな要素や、認証規模（例：対象者の人数等）、環境・条件（例：認証場所の環境等）を考慮することになるが、それらはさまざまであり、上記はあくまでも概略的な傾向という位置づけで記載している。

次に、生体情報の個人識別性（どのような場合に個人識別が可能か、認証・識別の条件、特徴等）について整理したものを示す。

表 4-4　生体情報の特徴比較（2）個人識別性

生体情報	個人識別性
顔	● 【個人識別性がほぼ確かと判断できるケース】パスポート画像基準（ICAO[79]）で撮影された画像 ● 【個別の対応が必要なケース】ICAO 基準は満たさないが、顔として人が認識できる場合：姿勢・表情・照明、画質など ● 【個人識別性はほぼ無いと判断できるケース】顔が見えないぐらい低解像画像（モザイク画像、ぼかし）、目線を入れた場合
虹彩	● 万人不同・終生不変であり、認識精度も高い ● 疾病や薬物による変化、ストレスによる影響がある ● ピンボケ、ブレ、視線ずれ、めがねレンズの反射光、カラーコンタクト、顔の傾き等により認証精度低下
声紋	● 【個人識別性がほぼ確かと判断できるケース】明瞭な音声（静かな環境で等誤り率 2、3%程度） ● 【個別の対応が必要なケース】何らかの加工が加えられた音声（ボイスチェンジャー、声質変換など） ● 【個人識別性はほぼ無いと判断できるケース】不明瞭な音声（何を言っているかわからない） ● データ形式はベンダにより異なる
歩容	● 【個人識別性がほぼ確かと判断できるケース】自然な直線歩行をしていて、高精度なシルエットが得られ、一定の時空間解像度（高さ 30 画素以上、5fps 以上）で、条件変化（観測方向、速度、服装、鞄、靴、地面、経年変化）がないケース ● 【個別の対応が必要なケース】シルエットの品質が低下するケース、観測条件の一部が変化するケース ● 【個人識別性はほぼ無いと判断できるケース】一定の時空間解像度を満たさないケース、条件変化が極めて大きいケース
静脈	● 万人不同であり、経年変化はほとんどない ● 身体内部情報であり、偽造が困難

[79] International Civil Aviation Organization（国際民間航空機関）。国連専門機関として、ISO/IEC（JTC1 SV27/WG6）と連携しながら機械可読旅券（IC パスポート）の標準化を行っている。

生体情報	個人識別性
掌紋	● 紋様部分は終生不変・万人不同とされている（掌線、しわ部分は加齢により変化する場合あり） ● 照合には 75dpi が必要とされている（より低解像度でも認証可能という研究例もある） ● 照合に必要なサイズは、例として 50.4cm×50.4cm と算出されている
指紋	● 終生不変・万人不同とされている ● 認証に必要な最小指紋画像サイズは 12mm×16mm 程度 ● 照合精度は、特徴点抽出方式と照合エンジンの組合せに依存する ● 他人照合率とデータベースサイズ（登録件数）との相対的関係も照合精度に関係する

出所：有識者（生体認証研究者）へのヒアリングに基づき作成

なお、生体認証方式の比較を行っている文献はいくつかみられるものの、情報が古い、評価基準が明確でない、前提条件（例：認証規模）が一般的でない可能性がある、特定認証方式に偏っている可能性がある、等の点が懸念されること、また海外の文献については、その国における用途の特徴が評価にも反映される可能性がある（ある用途が非常に重要な場合、その用途に対応した評価項目が重視される傾向は否定できない）ことから、有識者ヒアリングにより上記の整理を行った[80]。

4.2.2 新用途が期待される生体認証技術の開発

次に、現在研究開発が行われている生体認証技術について、主なものを整理した。

表 4-5　新用途が期待される生体認証技術の例

分類	生体情報	事例	概要
身体的特徴	心臓	心臓スキャン認証（バッファロー大学） https://sctracy.github.io/chensong.github.io/pdf/mobicom17.pdf	ドップラーレーダーを用いて、心臓の形状・サイズ・動きを測定することで個人を認証する。最大約 30 メートル離れた場所からの認証が可能。
	耳穴	耳穴形状認識（NEC・長岡技術科学大学） http://jpn.nec.com/press/201603/20160307_01.html	イヤホンを装着し、耳穴の形状によって決まる音の反響特性によって個人を認証する。1 秒以内での高速認証が可能。

[80] さらに加えれば、前述のとおり、生体認証の精度やその他のパフォーマンスに影響を及ぼしうる要素は多数あり、比較を行った研究者等がどのような条件・前提を置いているかによっても結果が異なる可能性もある。

分類	生体情報	事例	概要
	顔画像	顔写真に基づく性的志向分析（スタンフォード大学） https://www.theguardian.com/technology/2017/sep/07/new-artificial-intelligence-can-tell-whether-youre-gay-or-straight-from-a-photograph https://www.washingtonpost.com/news/morning-mix/wp/2017/09/12/researchers-use-facial-recognition-tools-to-predict-sexuality-lgbt-groups-arent-happy/?utm_term=.fd38e00f47f1	顔写真から被験者の性的志向を推定する技術。
	顔画像	顔写真に基づく犯罪者識別技術（上海交通大学） Xiaolin Wu and Xi Zhang (2016), Automated Inference on Criminality using Face Images, arXiv	画像認識や AI を活用し、顔写真から犯罪歴のある人とそうでない人を識別する技術。実験では一定の傾向がみられた。
行動的特徴	まばたき	まばたき顔認証（Gemalto）： https://www.paymentnavi.com/paymentnews/61807.html クレジットカード認証（Master Card） https://newsroom.mastercard.com/eu/press-releases/mastercard-makes-fingerprint-and-selfie-payment-technology-a-reality/ 携帯電話認証(ドコモ：2006 年の事例) http://www.itmedia.co.jp/mobile/articles/0605/11/news102_2.html	まばたきが行われた場合のみ顔認証を行うことで、写真等によるなりすましを防止する技術。
	足裏・臀部	足裏圧力分布（産業技術大学院大学） https://aiit.ac.jp/master_program/ide/pbl/pdf/h21/h21-6.pdf 着座認証システム（産業技術大学院大学） https://shingi.jst.go.jp/past_abst/abst/p/11/1114/tmu3.pdf	足裏や臀部の接触面の圧力データを分析することで個人を認証する。自動車の運転座席への導入が検討されている。
	唇	リップムーブメント認証（香港浸会大学） https://www.helpnetsecurity.com/2017/03/16/lip-movement-authentication/	パスワードとなる単語とくちびるの動きをセットで分析し、個人を認証する。情報流出時は、別の単語で再登録を行うことが可能。
	歩容認証	深層学習モデルによる歩容認証（大阪大学）※前掲 http://www.sanken.osaka-u.ac.jp/toppage/hot_topics/topics_20171	深層学習モデルを用いることで、防犯カメラで撮影された人物の認証制度を向上させた。

分類	生体情報	事例	概要
		108/	
	ライフスタイル	ライフスタイル認証（東京大学） http://www.yamagula.ic.i.u-tokyo.ac.jp/	次世代個人認証技術として、各種センサで取得した行動情報（例：位置情報、購買情報、等）を組合せ、個人の生活行動上の癖や特徴に基づいて認証を行う。

次に、上記の中から特徴的なもの（従来とは方向性が異なるものなど）について示す。認証方式としての実用性等が不明なものもあるが、新たな用途や認証形態を示唆しうるものとして挙げている。

(1) 心臓スキャン認証

ユーザー負担が少なく、また偽造が困難な認証方法として開発されている。本格的な「手ぶら認証」は生体認証における大きなトレンドの一つであるが、これもそうした方向性をもって行われていると考えられる。

サービス概要		サービスイメージ
事業者／研究機関名	バッファロー大学	
サービス名	心臓スキャン認証	
サービス内容	➢ 低出力のドップラーレーダーを用いて、心臓の形状・サイズ・動きを測定し、個人認証を実現する技術。 ➢ 最大約30メートル離れた場所からの認証が可能。 ➢ 約8秒間でユーザーの心臓を認識し、その後は心臓認証が継続される。パソコンに設置し、ユーザーを継続認証することで、離席時の他者利用を防ぐシステムの実現を目指している。	出典URL：http://www.buffalo.edu/news/releases/2017/09/034.html https://sctracy.github.io/chensong.github.io/pdf/mobicom17.pdf

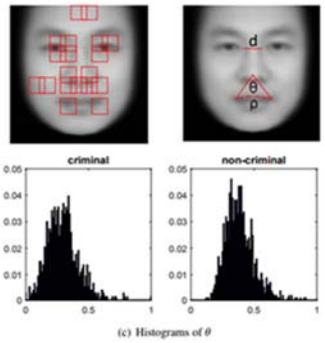
背景・目的	実績	課題と今後の展望	個人情報保護上の論点（例）
➢ ユーザー負担の少ない個人認証システムによるプライバシーの保護を目的としている。	➢ 検証実験における誤認識率は4.42%	➢ 他の生体認証と比べて認識精度が低い。 ➢ 将来的にはPCやスマートフォン、空港での利用を目指している。	➢ 非接触で離れた場所から測定することが可能であるため、本人の同意なしに個人識別が行われる可能性がある。

図 4-4　心臓スキャン認証の概要

(2) 顔写真に基づく犯罪者識別技術

次に顔画像を用いて何らかの分析・判定を行う例を挙げる。現在でも、カメラ画像から性別や年代を判定しているが、より深い分析を志向するものとして以下のような例がある。図に示したとおり、まだ認証精度が粗い（サンプルデータを用いても 10 人に 1 人ははずれる）が、画像解析自体の技術や、ビッグデータに基づくディープラーニング等により分析精度が

向上する可能性がある。他方、こうしたデータを多数収集し蓄積するハードルが高いという面もあり、プライバシーリスクについても留意・検討が必要と考えられる。

技術概要		技術イメージ
研究機関	上海交通大学	 出典：Xiaolin Wu and Xi Zhang (2016), Automated Inference on Criminality using Face Images, arXiv
技術名	顔写真に基づく犯罪者識別技術	
技術内容	➢ 画像認識やAIを活用し、顔写真から犯罪歴のある人とそうでない人を識別する技術。 ➢ 18～55歳の中国人男性1,856人（約半数が犯罪歴のある人）の身分証明書の写真を用いて、人工知能の学習及び実験を実施。 ➢ 検証の結果、特に「上唇の曲率」、「目と目の間の距離」、「鼻先と唇を結んだ線の角度」について、傾向差があることがわかった。 ➢ 89.5%の識別精度を実現。	

背景・目的	効果	課題と今後の展望	個人情報保護上の論点（例）
➢ 機械学習により、複雑かつ微妙な表情の違いを識別し、人間の内面を含めた表情理解を実現することを目的としている。	➢ 研究では、89.5%の精度で犯罪者と非犯罪者の識別を実現。	➢ 18~55歳の中国人男性に限定した検証であるため、対象者を広げた検証を行う必要がある。	➢ 比較的入手しやすい顔写真を用いた技術であるため、各企業が本技術を用いて、本人の同意を得ずに顧客や訪問者等の識別を行う可能性がある。

図 4-5　顔写真に基づく犯罪者識別技術の概要

(3) まばたき顔認証

顔認証では生体でない写真等をつかって認証をすり抜けられてしまうという場合も少なくなく、3D 画像モデルの導入をはじめさまざまな方法が試行されているが、これはまばたきにより生体であることを検知するというものである。またローカル端末上で認証情報を管理するため、生体情報への不正アクセスのリスクの低減も狙っている。

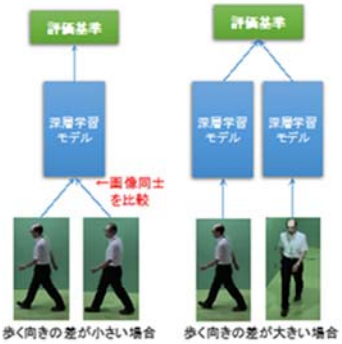
サービス概要		サービスイメージ
事業者／研究機関名	Gemalto	 出典URL: https://www.paymentnavi.com/paymentnews/61807.html
サービス名	まばたき顔認証	
サービス内容	➢ スマートフォンアプリに顔画像を登録し、まばたきを行うことで認証が行われるシステム。 ➢ まばたきが行われた場合のみ認証を行うことで、写真等によるなりすましを防止。 ➢ サーバーではなく、モバイル端末内で個人認証情報を管理しているため、ハッキングによる情報漏洩のリスクが低い。	

背景・目的	実績	課題と今後の展望	個人情報保護上の論点（例）
➢ 顔画像とまばたきと組み合わせることによる、顔認証サービスにおけるなりすまし防止。	➢ 各国の銀行やeコマース企業に対して、本技術を含む個人認証ソリューションを提供している。	➢ サービスの拡充による普及率の増加を目指している。日本では大日本印刷と提携し、生体認証クラウドサービスを展開。	➢ 個人識別符号としての位置づけ。（顔と別で定義する必要があるか等）

図 4-6　まばたき顔認証の概要

(4) 深層学習モデルによる歩容認証

歩容認証は他の例と異なり本格的実用化が非常に近い認証方式であるが、低精細度でも認証が可能なことから、遠隔から広域を対象に識別を行うことが可能であり、新たな用途が期待される。

技術概要		技術イメージ
研究機関	大阪大学 産業科学研究所	 出典URL：http://www.sanken.osaka-u.ac.jp/toppage/hot_topics/topics_20171108/
技術名	深層学習モデルによる歩容認証	
技術内容	➢ 深層学習を用いた歩容認証技術を開発。 ➢ 防犯カメラで撮影される人物の歩く向きは様々であるため、従来の画像認識技術では高精度な認証が困難であった。 ➢ 独自の深層学習モデルの適用により、歩く向きが異なる人物映像を用いた歩容認証性能の精度向上を実現。	

背景・目的	実績	課題と今後の展望	個人情報保護上の論点（例）
➢ カメラに対して人の歩く向きが異なる場合、従来の技術では歩容認証が困難であった。	➢ 従来技術では本人認証の誤り率が約40%であったのに対し、本技術では約4%（世界最高精度）まで低減。	➢ 犯罪捜索に加え、商業施設における同一人物の移動経路解析によるマーケティングや、顧客に応じたサービス提供等の活用が期待される。	➢ 歩容特徴は、遠方から撮影した低解像度の防犯カメラ映像からでも比較的容易に抽出することが可能であるため、本人の同意を得ずに識別が行われてしまう可能性がある。

図 4-7　まばたき顔認証の概要

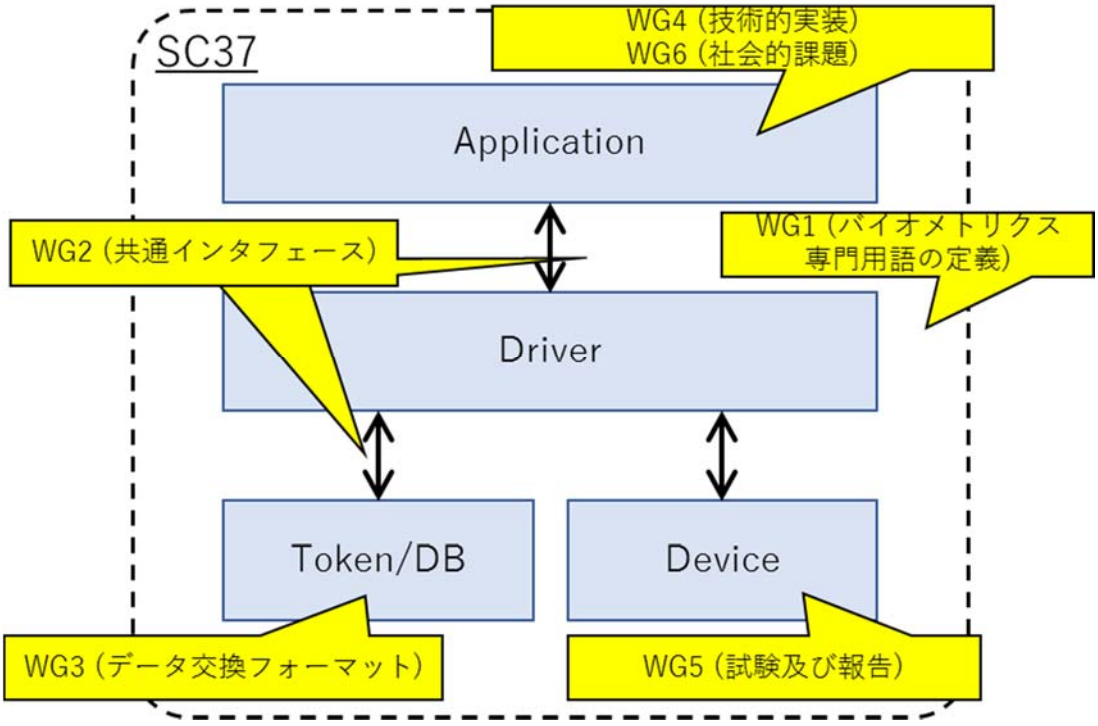
4.2.3 標準化動向

次に、生体認証に関連する標準化動向について記載する。

生体認証に関する標準化は非常に幅広く行われているが、ここでは今後の用途拡大に大きく関係すると思われるものから主なものを記載する。具体的には、生体認証に関する性能評価方法及び、生体認証に関するセキュリティに関連する規格について取り上げる。

(1) ISO/IEC における生体認証に関連する標準化動向

ISO/IEC では生体情報・生体認証に関して幅広い標準化活動が行われているが、主たる標準化は ISO/IEC JTC1 SC37 にて行われている。SC37 は生体認証（バイオメトリクス）の国際標準化を推進する専門委員会であり、下図に示すように WG1～WG6 のワーキンググループで構成されている。



出所：https://www.iso.org/committee/313770.html

図 4-8　ISO/IEC JTC1 SC37 の構成

各 WG では上記の標準化が実施されているが、ここでは、プライバシーとの関係で、生体情報の保護に関する標準化の動向について述べる。

生体情報の保護に関連する主な動向としては、WG5 の ISO/IEC 30136 の中で、登録された生体データが漏えいした際も、新しいデータを生成して再登録が可能な生体情報保護技術の性能評価指標が定義された。現在は FDIS 投票が行われ可決され、IS（国際標準）とし

ての発効を待つ状態である。

また、偽造物によるなりすましなどの入力攻撃検出に関する ISO/IEC 30107 シリーズについても標準化が行われている。

その他、ISO/IEC 19795 Information technology – Biometric performance testing and reporting（SC37）、ISO/IEC 24745:2011 Information technology – Security techniques — Biometric information protection（SC27）、ISO/IEC 19792:2009 Information technology -- Security techniques—Security evaluation of biometric（SC27）なども関連する標準として挙げられる。特に、24745 にはキャンセラブル・バイオメトリクスの規格も含まれており、静脈認証などによる「手ぶら認証」（例：ATM 等での各種操作が手ぶら（カード等が不要）でかつ安全にできる）などでの活用が期待されている。なお SC27 はセキュリティに関する標準化を進める専門委員会である。

表 4-6　生体認証に関連する国際標準（プライバシー関連）

規格	担当	標準化対象
ISO/IEC 30136:2018 Information technology -- Performance testing of biometric template protection schemes	SC37	生体情報保護技術の性能評価指標
SO/IEC 19795 Information technology – Biometric performance testing and reporting	SC37	バイオメトリック性能試験及び報告
ISO/IEC 24745:2011 Information technology – Security techniques — Biometric information protection	SC27	バイオメトリック情報の照合におけるセキュリティ（脅威分析、セキュリティ要件等）※キャンセラブル・バイオメトリクスに関する規格も含む
ISO/IEC 19792:2009 Information technology -- Security techniques—Security evaluation of biometric	SC27	バイオメトリクス製品固有のセキュリティ評価（評価要件、評価ガイド

出所：文献調査及び有識者ヒアリングにより作成

(2) FIDO における標準化動向

FIDO (Fast Identity Online) Alliance[81]によって、オンラインサービスにおいて、生体認証等の活用により、パスワード依存を軽減したシンプルで堅牢な認証を実現するための技術標準の策定が行われている。生体情報等の秘匿すべき情報をサーバに送信・登録しない（端末で検証を行い、検証結果をサーバに送信する）という特徴を有する。ローカル端末で認証を行い、生体情報をサーバに送らない、という方法は生体認証におけるセキュリティ対策のトレンドの一つであり、特にスマートフォンの活用により普及が期待されている。

2012 年に発足した FIDO Alliance には、Google, Microsoft, サムソン, PayPal, MasterCard 等大手企業が加盟しており、今後オンライン認証のデファクトスタンダードとなることも予想されている。

[81] https://fidoalliance.org/?lang=ja

FIDO にもいくつかの WG が設置されているが、Privacy and Public Policy Workgroup でプライバシー案件や各国の法制度とのすり合わせについて議論している。なお、日本からの参加企業が参加する FIDO Japan WG という WG も設置されており、参加メンバー（2016 年 12 月時点）は、NTT ドコモ、ヤフー、大日本印刷、富士通、楽天、三菱東京 UFJ 銀行、DDS、レノボ、Nok Nok Labs、NXP セミコンダクターズ、ISR である。

FIDO 認証の技術仕様には大きく 2 つのタイプがある[82]。

一つは「パスワードレス型」（UAF (Universal Authentication Framework) 1.1）で、スマホ備え付けの認証器で生体・所持認証（パスワードなし）を行うものである。

もう一つは「パスワード補完型」（U2F (Universal 2nd Factor) 1.1）で、主要ブラウザでのパスワード認証＋セキュリティキーなどの所持認証により認証を行うというものである。

前者はパスワードの代替、後者は補完（強化）という位置づけである。

次に、国内における FIDO の最新動向についてみると[83]、2017 年には、FIDO 仕様に準拠した金融機関サービスが進展している。例えば、みずほ銀行（富士通）、沖縄銀行（NEC）、ジャパンネット銀行（大日本印刷）が FIDO 認証を利用したサービスを開始している。

また、2017 年 12 月には、NTT ドコモの一部スマートフォン端末（Xperia シリーズ）が FIDO UAF 1.1 技術仕様に対応したことが発表された。これにより、通信キャリアや特定のサービス事業者のみならず、アプリの開発者が容易に指紋等の生体認証等を活用したアプリケーションを提供できるようになった。

[82] 五味秀仁「FIDO 認証と公開鍵暗号」: http://www.jnsa.org/seminar/pki-day/2017/data/170419_gomi.pdf

[83] Fido Alliance プレスリリース: https://prtimes.jp/main/html/rd/p/000000006.000029122.html

4.3 生体認証の現状及び今後の利用動向

4.3.1 生体認証の現状及び今後の動向

以上をまとめて、生体認証の現状及び今後の動向を整理する。生体情報のモダリティごとの現状と今後の動向を以下に示した。

表 4-7　生体認証の現状及び今後の利用動向

生体情報	現状及び今後の動向
顔	● 認証精度はまだ向上しており（データの蓄積と機械学習による）、新たな用途（例：ウォークスルー認証）も期待される ● 生体検知が難しい（写真や石膏像による認証等） ● 目視でも確認できるという意味で特殊 ● 従来は 1:n での識別が多かったが、スマートフォンのユーザー認証に使われたことで 1:1 認証（照合）も広がりつつある ● 認証速度は、認証精度を下げればいくらでも向上できるので、精度との組合せで考えることが重要 ● 顔と他の個人識別符号との組合せが効果的と考えられる
虹彩	● 一部スマートフォンに搭載されたため、コストダウンに加えて技術的にも伸びていくとみられ、民生分野での利用拡大が期待 ● 顔の一部が隠れていても認証可能（マスク、イスラム教徒、炭鉱夫、等）
声紋	● ディープラーニングにより認証精度が向上しているが、単独での話者認識の精度は高くない（ただし人間よりも高精度） ● 顔認証などと合わせることで認証精度も高まる ● データを取りやすい、デバイスが安価でハンディな一方、健康状態や環境、感情による影響を大きく受ける ● 電話での認証や残高照会などに用いられているが、スマートフォンや AI スピーカーの普及により用途が広がる可能性
歩容	● 低解像度でも特徴を抽出できること、遠隔で個人を識別できること、が大きな強み ● 歩き方は、体型と動きの両方似ている必要があり、真似するのが難しい ● ウォークスルー認証の場合は、方向を誘導するなどの運用が効果的 ● 基本的には研究開発段階だが、機械学習により性能が向上してきている
静脈	● 認証精度が高く、偽造にも強い ● 入退室やアクセス管理、金融や決済などの本人認証（照合）に広く用いられている ● ベンダにより部位やデータフォーマットが異なる
掌紋	● 技術的には成熟 ● 動画からの切り出しも可能 ● FIDO に対応することで用途が拡大しつつある ● 課題はカメラ特性による画像の違いが大きいこと、生体検知が難しいこと

生体情報	現状及び今後の動向
	● 大きな怪我でなければ認証には影響しない ● 静脈との組合せも考えられる
指紋	● Android 端末での汎用プラットフォームを Google がリリースしたため、より広く利用されることが期待される ● 数%の人が利用できないため、指紋を必須とすることには問題もある

出所：有識者（生体認証研究者）へのヒアリングに基づき作成

4.3.2 今後の動向に関するトレンド

以上から、3 つの大きな傾向を読み取ることができる。

a. スマートフォンを活用した、ローカル認証の普及の可能性

指紋だけでなく、顔、虹彩、掌紋についてはセンサがスマートフォンに搭載される、あるいは搭載可能となっており、生体情報をサーバに送信しない形でセキュリティを向上させた生体認証の普及が予想される。また、音声についてもスマートフォンで取得可能なため、顔などと組み合わせた認証も考えられる。手軽に手元の端末で認証できる一方、生体情報がローカルに保存されることによる安心感から、これまで以上に生体認証の導入や利用が進むことも期待される。

ローカル認証では、指紋、顔、虹彩、掌紋などのセンサがすでに開発されている他、電話機のマイクにより音声を入力することも可能であるため、単独または組合せにより生体認証を行うことができる。これにより、スマートフォンへのアクセス制御だけでなく、各種オンラインサービスでの生体認証も普及する可能性が考えられる。その場合、ユーザー体験や「手軽さ」を重視すると、サービスの内容や特徴と親和性の高い生体情報[84]が選ばれる可能性が高い。

b.「手ぶら」認証の普及

静脈認証により、金融機関のサービスを手ぶらで利用可能とした事例が複数出てきている。前述のとおり、静脈は認証精度が高く、経年変化が少ない、生体内部の情報であるため偽造が困難、ユーザーが意識的にセンサに読み取らせないと情報取得が難しい、等の特徴があり、今後、キャンセラブル・バイオメトリクスなどの生体情報保護技術と組合せることで、さらに普及が進むことが期待されている。他方、ベンダにより部位（手のひら、指）やデータフォーマット等が異なる点は、静脈認証が普及する上での課題と考えられる。

「手ぶら」認証の用途としては、すでに導入事例がみられるような、金融サービス、重要な施設・データへのアクセス制御などが中心になると考えられる。今後、ユーザー端末への

[84] 例えば、画像を用いるアプリであれば顔画像、音声通話やテレビ電話・会議アプリであれば、顔＋音声などが用いられる可能性が高いと考えられる。

静脈センサの内蔵[85]が実現した場合には、オンラインバンキング等での利用も期待される。

また顔や歩容を用いたウォークスルー認証についても、イベントや施設への入退場の管理、チケットの代わりなどの用途を中心に開発や導入が進められている。

c. 追跡・分析・判別などの新用途の開拓

顔画像や歩容などでは、個人の追跡、施設や公共空間での動線分析、属性（年齢、性別等）やその他の特徴分析などが実施または試行されている。個人を特定した形での追跡や解析は、そのメリットとプライバシーリスクについて慎重に検討する必要があると考えられるが、他方で個人を特定せずに動線だけを分析する、あるいは個人を特定せずに属性だけを解析しその挙動を解析する（例：年齢・性別ごとに、ショッピングモールでの動線を分析する等）といった利用方法も考えられる。この場合は、生体情報は使うが個人は特定しないことになるが、こうした場合に、個人情報保護法制、プライバシー法制においてどのような扱いになるのかといったことについても今後は検討が必要になると考えられる。

これらの傾向を図示すると次のようになる。図は生体情報の用途を、個人の特定を目的とするか、個人の追跡・分析・判別等を行うか、の 2 点から分類したもので、横軸、縦軸はそれぞれ以下を表している。

横軸：生体情報により、個人の特定を目的としているか否か

縦軸：生体情報を用いて、対象とする個人の属性・状況・挙動等を追跡・分析・判別を行うか否か

図の右下部分は生体情報を用いて個人の認証（照合または識別）を行うが、追跡・分析・判別等は行わないという領域であり、現在用いられている生体認証の多くはここに含まれる。本人であるかを確認するための生体認証では、上述のとおり、a. ローカル認証、b. 「手ぶら」認証、という大きな傾向がみられるが、いずれもユーザーにとっての手軽さとセキュリティ確保（ローカルでのみ生体情報を保持する、テンプレート暗号化などの生体情報保護技術を用いる、等）を重視した流れと考えることができる。

図の上半分は、c. 追跡・分析・判別などの新用途の開拓、に対応している。

右上部分は、生体情報を用いて個人の特定と追跡・分析・判別等を行う場合と、行動上の特徴（例：ライフログや歩容等）による照合・識別を行う場合の 2 パターンが考えられる。いずれの場合も、個人を特定する情報と、個人の行動や履歴に関する情報が素材することになる。ここでは普及の端緒としては 2 通りが考えられ、前者の場合には個人を特定した上で挙動の特徴等を分析し、マーケティング等に用いるなどが考えられる。後者の場合には特定の状況・目的における本人認証が導入されるケースが考えられる。特定の状況・目的とは、例えば広場や駅・空港の構内、スタジアムなど一定の広さのある公共空間における個人の認証や識別[86]、ウォークスルー認証などが考えられる。

---

[85] 有識者へのヒアリングによれば、現状では静脈センサはスマートフォンに搭載するには若干大きいとのことである。

[86] 例えば、予め歩容をスマートフォン等に登録しておき、監視カメラを用いて（スマートフォン等に登録しておいた歩容データを監視カメラ運営者に一時的に提出して照合する）、迷子や徘徊する認知症患者の

図の左上部分は、対象者の属性（例：年齢、性別、服装[87]）、状況（例：気分や感情[88]）に基づく分類結果・分布、あるいはそれにより分類されたセグメントごとの挙動分析（例：動線分析、購買行動分析）は行うが、個人の特定は行わないというものである[89]。なお、この場合は個人の特定は行わないが、追跡・分析・判別のためのデータを取得した時点では個人情報を保有していると考えられ、適切な取得と、処理・廃棄に関する透明性が重要と考えられる。また、将来的には行動による各種の入力（ジェスチャーによる端末やサービスの操作）などが普及する可能性も考えられるが、その際に取得される動作データなども場合によっては個人を識別することが可能になることも考えられる。また個人の識別は困難（実質的に不可能）であっても、姿勢や動作特性から性別、年齢等が判定される場合も考えられる。

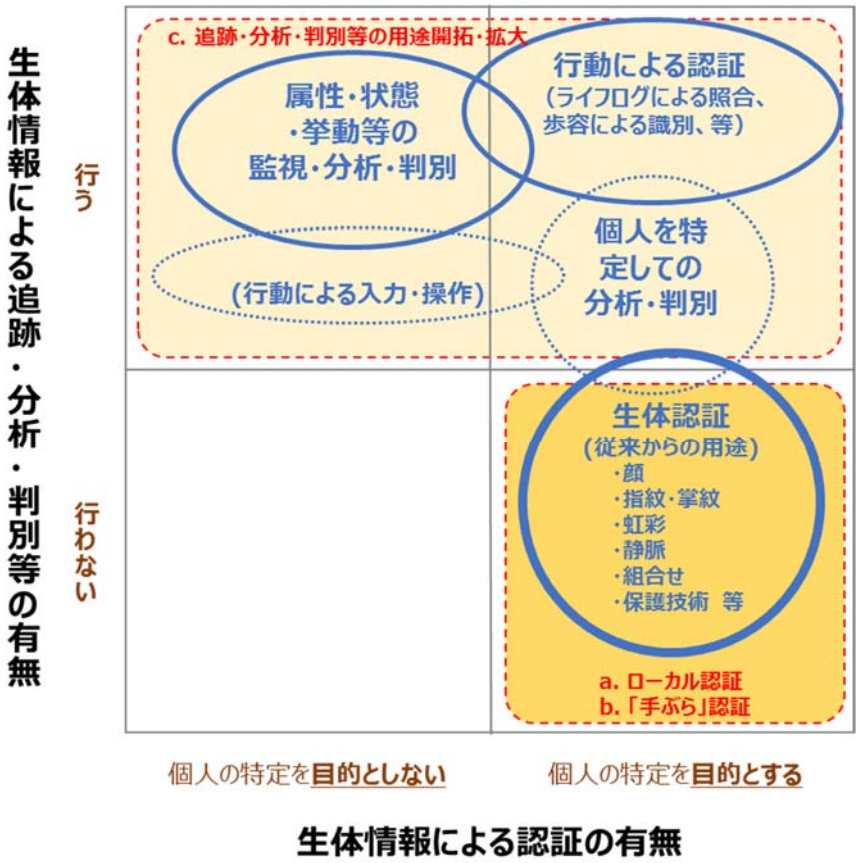


図 4-9　生体情報利用のトレンド

4.3.3 市場の展望

上述の 3 つのトレンドもふまえて市場の今後を展望すると、従来は生体認証機器やアル

探索に利用することも考えられる。

[87] 例えば、服装の色使いや特定のアイテム（例：ブーツ、ロングスカート等）による分類が考えられる。

[88] いずれも、特定のアルゴリズム等により推測・判定されたもの。

[89] 3.4.2 節(2)に記載した EU の Opinion (WP192)における事例 3、4 を参照。

ゴリズムなど、認証手段（ハードウェア、ソフトウェア等）が中心の市場が展開してきたが、今後は、センサの小型化・コストダウン（例：スマートフォンへの搭載を契機にセンサのコストは低下する）も含め、こうした機器市場よりもサービス市場が成長することが期待される。

例えば、上記 a.のトレンドについては、スマートフォン端末上の認証機能（センサ＋ソフトウェアにより実現される）を個々のアプリやサービスが利用する形になり、従来のような専用機器・システムの市場ではなくなる。この場合の生体認証自体は消費者から直接対価を得て提供するサービスではなく、サービスやアプリの提供者に対して提供されるプラットフォーム機能の一部ともいえ、このような生体認証の市場規模はある意味で「見えない」ものになるが、生体認証を利用するサービスや対象ユーザーという面では大きな普及が期待される。

同じく上記 b.については、従来と同様に専用機器・システムに対する需要が中心と想定され、またサービス提供サイドが主な顧客であり、数量規模としては堅調な成長が想定される。普及のポイントはセキュリティ面がユーザーおよび事業者（とくにユーザー）にどのように評価されるかであると考えられる。

上記 c.については、カメラ等の入力機器は既存の設備を利用することも考えられるため、主にソフトウェア・サービスが中心の市場になると想定される。主な顧客はサービス提供サイド（主に施設管理者、イベント運営者等）であり、数量規模でみると堅調な成長と予測される。他方、分析等の付加価値が大きいため、その面での市場規模の拡大も期待される。

以上から、まず、生体認証自体について一定の市場拡大・創出が期待される。それに加え、生体認証自体は直接消費者から対価を得て提供するサービスではなく、サービス事業者に対して提供されるプラットフォーム機能の一部という性格があることから、生体認証単体の市場規模が明示的ではなくてもそれを用いる他サービスの成長や普及とともに進む可能性がある。

他方で、生体認証を含む個人識別符号はひとたび漏えいすれば重大な人権侵害、経済的被害につながるリスクが存在することから、利用にあたっては、法令を遵守するとともにプライバシーへの配慮を含む適切な対応が不可欠である。

個人識別符号に関する海外・国内動向の調査研究　報告書

2018 年 3 月

株式会社三菱総合研究所
社会 ICT イノベーション本部