生体データの保護

ICT・コンテンツ産業コンサルティング部　コンサルタント　片寄　良菜

1　はじめに

このたびの個人情報保護法（以下、法という）の「いわゆる３年ごと見直し」で示された改正テーマの一つに「本人が関知しないうちに容易に取得することが可能であり、一意性・不変性が高いため、本人の行動を長期にわたり追跡することに利用できる身体的特徴に係るデータ（顔特徴データ等）」（以下、顔特徴データ等という）の取扱いが挙げられている※1。

「身体的特徴に係るデータ」とは、いわゆる生体データのことで、法において「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」と定義され、さらに施行令において、具体的な対象が規定されている（図表１）。なお、単なる顔写真や動画、音声は該当しない。

現行法では、これらの生体データの取扱いに係る義務は、他の個人情報と同様で、特別の規定は設けられていない。しかし、「いわゆる３年ごと見直し」において、生体データのうち顔特徴データ等については、侵害の防止と適正な利活用の促進に向けて、上乗せの義務を課すことが検討されている。本稿では、顔特徴データ等に関する規律の方向性と、それらを取り扱う事業者に求められる対応について述べる。

2　顔特徴データ等に関する規律の方向性

顔特徴データ等に関する規律が検討されている背景と、現時点で想定されている規律の方向性を紹介する。なお、どの生体データが新たな規律の対象になるか、どのような義務が課されるかは、本稿執筆時点（2026 年２月）で明らかにされている範囲のものであり、今後の情勢によって、見直される可能性のあることに留意してもらいたい。

1）　規律が検討されている背景

規律の対象になりうる生体データとして、個人情報保護委員会が公表した文書では、顔特徴データが挙げられ「カメラ等の計測機器を複数の地点に設置して顔特徴データ等を入手し、これを名寄せに利用することで、本人が関知し得ないまま、半永久的・網羅的に当該本人の行動を追跡」できるおそれが指摘されている。

また、個人情報保護委員会が、犯罪予防や安全確保のための顔識別機能付きカメラシステムの利用について公表した資料※2 において、顔識別機能付きカメラシステムは、犯罪防止や行方不明者の捜索に有効である一方で、ア . 不変性と追跡性、イ . 自動的、無差別かつ大量の取得、ウ . 利用目的の予測困難性、エ . 差別的効果、オ . 行動の委縮効果といった懸念点が指摘されている。

パスポートの有効期限が５年や 10 年になっていることが示唆するように、顔特徴データは生体データの中でも不変性が高い（ア）。街中の至るところにある監視カメラで取得できることから、追跡性が高く（ア）、自動的、無差別かつ大量の取得が可能

※１　個人情報保護委員会「個人情報保護法 いわゆる３年ごと見直しの制度改正方針」2026 年１月９日
※２　個人情報保護委員会「犯罪予防や安全確保のための顔識別機能付きカメラシステムの利用について」2023 年３月

図表 1　個人情報保護法における生体データ

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（一般的には「**DNA**」として言及）
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（一般的には「**顔特徴データ**」として言及）
ハ	虹彩の表面の起伏により形成される線状の模様（一般的には「**虹彩データ**」として言及）
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（一般的には「**声紋データ**」として言及）
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（一般的には「**歩容データ**」として言及）
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（一般的には「**静脈データ**」として言及）
ト	**指紋又は掌紋**

出所）個人情報の保護に関する法律施行令第1条第1号よりNRI作成

（イ）である。さらに、カメラから取得された情報が、どのように活用され、どのような情報と照合されているのかが分からない、という利用目的の予測困難性（ウ）も指摘されている。例えば、個人認証・識別のために顔特徴データだけを抽出しているのか、マーケティングのために顔画像から性年代を読み取り、顔画像データまで保存しているのかは、カメラの外観だけでは読み取ることができない。そのほかに、特定の人種や肌の色によって誤検知の発生率に偏りが生じてしまうといった差別的効果（エ）や、自らの顔画像・顔特徴データ等がどのように利用されているのか不安になり、行動を委縮してしまう効果（オ）が言及されている。

以上のように、顔特徴データは本人のプライバシーなどの侵害につながりやすいことから、特別の規律が検討されているのである。

2）義務の概要

顔特徴データ等が規律の対象となった場合、どのような義務が新たに課されるのかについて、制度改正方針[※3]で示された内容を基に論じる。制度改正方針では（1）一定事項の周知の義務化、および（2）利用停止等請求の要件の緩和、（3）オプトアウト制度に基づく第三者提供の禁止が挙げられている。

（1）一定事項の周知の義務化

顔特徴データ等を取り扱うには、透明性を確保した上で本人の関与を強化する必要があるとし、データの取扱いに関する一定事項の周知の義務化が挙げられている。周知すべき項目には「個人情報取扱事業者の名称・住所・代表者の氏名や、顔特徴データ等を取り扱うこと、顔特徴データ等の利用目的、顔特徴データ等の元となった身体的特徴の内容、利用停止請求に応じる手続等」が示されている。

米国・イリノイ州のBiometric Information Privacy Act（BIPA）第15条（b）では、生体データを取り扱う際に、データ主体、またはその法的代理人に対して、生体データを取得・保管することや、取得・保管・使用する目的とその期間を書面で通知することが義務付けられている。制度改正方針では、イリノイ州BIPAのような通知ではなく、あくまでも「周知」の義務化が想定されているが、BIPAと同様の項目が周知の対象となる可能性がある。

※3　個人情報保護委員会「個人情報保護法 いわゆる3年ごと見直しの制度改正方針」2026年1月9日

(2) 利用停止等請求の要件の緩和

顔特徴データ等（保有個人データ※4に限る）は、違法行為の有無などを問わず、利用停止等請求への対応を義務付けることが示されている。現行法では、違法行為があった場合以外に、法第35条第5項にて「当該本人が識別される保有個人データを当該個人情報取扱事業者が利用する必要がなくなった場合」「当該本人が識別される保有個人データに係る第二十六条第一項本文に規定する事態（漏えい、滅失、毀損〔きそん〕その他の個人データの安全の確保に係る事態のこと）が生じた場合」「その他当該本人が識別される保有個人データの取扱いにより当該本人の権利又は正当な利益が害されるおそれがある場合」に、利用停止等または第三者への提供の停止を請求できると定められている。請求時にそれらの理由があれば、個人情報取扱事業者は、利用停止等または第三者への提供の停止に応じる必要がある。一方、制度改正方針では、顔特徴データ等において、個人情報取扱事業者にとって利用の必要性がなくなったこと、漏えいや滅失などにより、本人の権利や正当な利益が害されるおそれがあること、といった理由を問わず、利用停止等請求への対応を義務付けることが示されている。

ただし「本人の同意を得て作成又は取得された顔特徴データ等である場合、要配慮個人情報の取得に係る例外要件※5と同種の要件に該当する場合等」は、利用停止等請求への対応義務の例外要件として定めることとされている。

(3) オプトアウト制度に基づく第三者提供の禁止

顔特徴データ等に関して、オプトアウト制度に基づく第三者提供を禁止することが想定されている。オプトアウト制度に基づく第三者提供とは、本人に通知し、または本人が容易に知り得る状態に置くとともに、個人情報保護委員会に届け出たときには、本人の同意取得や、人の生命、身体または財産の保護目的などといった条件を満たさずとも、個人データを第三者に提供できる仕組みのことである。

要配慮個人情報では、既にオプトアウト制度に基づく第三者提供が禁止されている。要配慮個人情報とは、法第2条第3項にて「本人の人種、信条、社会的身分、病歴、犯罪の経歴、犯罪により害を被った事実その他本人に対する不当な差別、偏見その他の不利益が生じないようにその取扱いに特に配慮を要するものとして政令で定める記述等が含まれる個人情報」と定義されている。取扱いに特に配慮を要する要配慮個人情報と同じく、顔特徴データ等についても、オプトアウト制度に基づく第三者提供の禁止が検討されているのである。

先述したイリノイ州BIPA第15条（d）では、オプトアウト制度に基づく生体データの第三者提供が禁止されている。生体データの第三者提供は、データ主体またはその法的代理人による同意がある場合、金融取引の遂行が目的の場合、州法・連邦法・自治体の条例で定められている場合、令状または召喚状に基づいて要求される場合にのみ認められている。日本ではBIPAのように生体データ全般ではなく、顔特徴データ等のみに課される予定であるが、第三者提供時に、データ主体による同意などが義務付けられる可能性がある。

※4　個人データのうち、個人情報取扱事業者が、開示、内容の訂正、追加又は削除、利用の停止、消去及び第三者への提供の停止を行うことのできる権限を有するもの。委託を受けて取り扱っている個人データや、個人情報のうち体系的に整理されていないものについては、「保有個人データ」には該当しない（個人情報保護委員会ウェブサイトFAQ　Q2－1）

※5　現行法第20条第2項にて「法令に基づく場合」「人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき」「公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって、本人の同意を得ることが困難であるとき」「国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき」などが例外要件として定められている

3　顔特徴データ等を取り扱う事業者に求められる対応

顔特徴データ等を取り扱う際に、事業者がどのような点に留意すべきかを述べる。

1）一定事項の周知の徹底

制度改正方針では、顔特徴データ等を有する本人への通知ではなく、周知の義務が示されている。ただし、透明性を確保することが重要とされており、周知に当たっては、本人の目に入る形で、一定の事項を明瞭に伝える必要があるだろう。周知の方法としては、顔特徴データ等が取得されるエリアに入る前の入り口に大きなポスター等を掲示したり、自社のホームページやアプリのトップ画面に表示したりすることなどが考えられる。

例えば、2019 年から渋谷の書店が共同で実施している「渋谷書店万引対策共同プロジェクト」では、店頭のポスターおよびホームページにて（1）共同利用する個人データの項目、（2）共同利用する者の範囲（プロジェクトに参加している書店名）、（3）利用する者の利用目的、（4）個人データの管理について責任を有する者の名称（連絡先・代表者の氏名含めて記載）が掲載されている[※6]。このプロジェクトは、万引や盗撮などの犯罪事犯の顔特徴データを書店間で共有し、データが登録された顔識別システムと防犯カメラを突合することで、犯罪事犯の入店を防ぐ取り組みである。書店内のカメラで顔特徴データが取得されているため、入り口のポスターでそのことが分かるように周知されている。今後は他の取り組みにおいても、法的な拘束力がある形で、店頭やホームページでの明瞭な周知が義務付けられる可能性がある。

2）生体データとその他の情報の分別管理

先に述べた通り、生体データとは、単なる顔写真や動画、音声ではなく「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」のことである。身体の特徴を特徴量化するアルゴリズムは、システムの開発ベンダーによって異なるため、特徴量が流出しただけでは、個人を特定できるリスクは低いとされている。一方で、特徴量と共に、氏名などの個人情報や、特徴量の基となった身体の特徴が流出した場合には、個人を特定できる確率が高まる。顔特徴データ等は、一意性・不変性が高く、本人の行動を長期にわたり追跡できるリスクがあるため、個人を特定できる形での特徴量の流出には、厳重に注意する必要がある。

そのためには、特徴量データと、氏名などの個人情報や、特徴量の基となった写真や身体の情報をひもづけられない形で管理することが重要である。例えば、米国の HID Global 社が提供している「HID® Amico™ Biometric Facial Recognition Readers」では、個人が保有する物理的カードに特徴量データを保存しておき、カードをかざした上で、その場のカメラに写し出される顔画像と、カード内の特徴量データを照合する機能を搭載している。特徴量データをカードに分別して保存することで、漏えい時のリスクを低減している事例といえる。

3）最低限のデータ保存

一部の事業者では、身体の情報を特徴量化した時点で、特徴量の基となった身体の情報（顔画像や声紋抽出前の音声データなど）をその場で削除している。例えば、「Microsoft Azure Face API」の利用規約では「顔画像は保存されず、抽出された顔の特徴量のみがサーバーに保存される」と記載がある[※7]。

また、現時点で特徴量から元の身体の特徴を復元する技術（テンプレート反転技術）は、個人を特定できるレベルで成熟しているわけではないものの、生成 AI やディープラーニングの進化により、

※6　渋谷書店万引対策共同プロジェクトウェブサイト「店頭告知内容」2026 年 2 月 25 日改定第 4 版
※7　Microsoft Azure AI Services ウェブサイト「Face Detection Operations - Detect」

特徴量単体が流出したときのリスクも高まりつつある。日立製作所では「公開型生体認証基盤（PBI：Public Biometric Infrastructure）」を用いて、生体データ情報を秘密鍵へと変える一方向性変換を行っている。身体の情報に加えて特徴量までも保存しないことで、漏えい時のリスクを低減しているのである。

このように、特徴量データとその他のデータを分別して管理するだけでなく、特徴量の基となった身体の特徴に係るデータや、特徴量データをそもそも保存しない方法も、セキュリティーの向上につながるであろう。これらのデータの保存は、必要な範囲にのみとどめることが重要である。

4　おわりに

本稿では法の「いわゆる３年ごと見直し」において、顔特徴データ等に新たに課される義務の概要と、顔特徴データ等を取り扱う事業者に求められる対応について述べた。規律の対象として、顔特徴データが想定されているが、ほかにも生体データの中には一意性・不変性が高いものが多いため、取扱いには注意が必要である。そうしたデータの取得前に一定の事項を周知したり、特徴量データとその他のデータを分別して管理したり、最低限の保存にとどめたりするなど、データ利用の透明性を確保すること、また漏えい時のリスクを抑えることが重要であろう。

（監修：小林　慎太郎）

筆者

片寄　良菜（かたよせ　らな）
株式会社 野村総合研究所
ICT・コンテンツ産業コンサルティング部
コンサルタント
専門は、情報通信業界、コンテンツ業界における事業戦略立案、実行支援
E-mail: r2-katayose@nri.co.jp