資料1

顔識別機能付きカメラの特性に関する国内外の評価

令和4年3月9日

個人情報保護委員会
Personal Information Protection Commission

調査の目的及び方法

（調査の目的及び方法）

- 顔識別機能付きカメラシステムの特性について、国内外でどのような評価がなされているかを把握するため、国内外の関連文書から関係する記述を抽出し、利点と懸念点に分けて一覧化した。

（対象文書）

- カメラ画像利活用ガイドブックver.2.0（2018年３月：総務省、経済産業省）「カメラ画像」
- 空港での顔認証技術を活用したOne IDサービスにおける個人データの取扱いに関するガイドブック（2020年３月：国土交通省）「One ID」
- ビデオ機器を通じた個人データ処理に関するガイドライン（2020年１月：欧州データ保護会議）「EDPB」
- 顔認証技術に関する決議（2020年10月：世界プライバシー会議）「GPA」
- 英情報コミッショナー意見書「公共の場所でのライブ顔認証技術の使用」（2021年６月：英情報コミッショナーオフィス）「ICO」

主な評価

- **利点**
  - セキュリティと公共の安全に利益をもたらす可能性がある。（ICO、GPA）
  - 生活をより簡単、効率的で便利にする。（One ID、ICO）

- **懸念点**

【取り扱われる個人情報の性質に由来する問題】
- 顔特徴量は不変性が高いため、顔特徴量をキーとして長期にわたって特定の個人が追跡されたり、様々な場面の情報が紐づけられたりする可能性がある。（カメラ画像、One ID、ICO、GPA）
- 本人がカメラによる顔画像の取得を認識、選択、コントロールしていない状況で、自動的かつ無差別に取得される。（カメラ画像、ICO、GPA）
- ウォッチリストの作成過程にも偏見や差別が含まれる可能性がある。（ICO）
- 年齢、性別、ジェンダー、民族などの特徴を推定又は推論するために利用できる。また、今後予期しない情報が、解析・プロファイリング技術の進歩により明らかになる可能性がある。（カメラ画像、ICO）

【顔識別機能付き防犯カメラシステムの技術的特徴や性能に由来する問題】
- 利用目的の範囲が一見して分からず、本人が予期する範囲を超えた取扱いが行われる可能性がある。（カメラ画像、EDPB、GPA）
- 装置の誤動作やそれにより引き起こされかねないバイアスによるリスクがある。（EDPB）

【上記による影響】
- 匿名による行動が制限される可能性があり、表現の自由等に対する萎縮効果も生じ得る。（EDPB、ICO）
- 差別的効果を伴う。（GPA）

(参考1)カメラ画像利活用ガイドブックVer.2.0

- カメラ画像の取扱いに関しては、以下のような特徴に留意が必要であると示している。
  - 撮影範囲内への写り込みや、設備利用上避けられない経路等があり、**被写体本人が常に事前の通知を受け、個人情報の取得への暗黙の同意を行っているとは限らない状況で、個人情報の取得が行われる**。そのため、可能な限りの誠実な通知を行うことを前提としても、常に「撮影されたくない者への配慮」を行うことが求められる。
  - 被写体本人にとっては、様々な利用形態のカメラであっても、カメラそのものは全て同じものに見えるため、**カメラで取得された情報がどの範囲で利用されるのか、カメラ本体を目視しただけでは想像・把握できない**。
  - 被写体本人にとっての意図的な行動だけでなく、無意識の行動等も含む膨大な情報が取得されるため、**本人が希望・意図する範囲を超えた情報の取得が行われ、本人の想像しない情報が後日開示されたり、漏えいする可能性がある**。
  - **取得時点では撮影側すら予想しなかった情報が、解析・プロファイリング技術の進歩により後日明らかになる可能性がある**。
  - **顔や容貌は容易に変更できず、また、外部から容易に観察可能**であるために、被写体本人の写り込むカメラ画像や、そこから抽出される特徴量データ（個人識別符号）をID として、**長期にわたって特定の個人が追跡されたり、様々な場面の情報が紐づけられる可能性がある**。※本内容のみVer.3.0パブリックコメント版より抜粋

(参考2)空港での顔認証技術を活用した One ID サービスにおける個人データの取扱いに関するガイドブック

- 以下の点が指摘されている。
  - 近年では顔認証技術が比較的身近な技術となり、**便利で豊かな生活の実現に貢献**してきている一方で、顔画像情報の取得が強い拒否感を招いた事例も存在する。
  - 顔画像情報が、**不変性が高く本人の意思によらない取得が容易な識別子であるため、強い追跡機能を有する**。

(参考3)EDPB ビデオ機器を通じた個人データ処理に関するガイドライン

- ビデオ機器を通じた個人データの処理について以下のとおり述べている（「1 Introduction」）。
  - ビデオ装置の集中的な使用は、市民の行動に影響を及ぼしている。このようなツールが個人の生活の多くの領域に大規模に導入されたことは、**本来であれば異常だと思われるものが発見されることを防ぐために、個人への圧力を更に高める**ことになる。事実上、これらの技術は、**匿名による移動及びサービスの匿名での利用の可能性を制限し得る**ものであり、一般的には気づかれずに済む可能性を制限し得る。
  - セキュリティ目的で構築されたビデオ監視は、ある個人にとっては快適かもしれないが、データ主体が予期しない目的に不正利用されないように保証する必要がある。さらに、現在では、撮影した画像を利用するために多くのツールが導入されており、従来のカメラがスマート・カメラに切り替わりつつある。ビデオによって生成されるデータ量は、これらのツール及び技術との組み合わさることで、**二次利用のリスク（システムに当初割り当てられた目的に関連するものであるかどうかにかかわらず）、あるいは、不正利用のリスクを増加**させる。
  - プライバシーの問題に加え、これらの**装置の誤動作やそれにより引き起こされかねないバイアスの可能性に伴うリスク**も存在する。
  - ビデオ監視は、根本的な目的を達成するために、他の手段が存在する場合、デフォルトで行う必要はない。そうでなければ、文化的規範が変化して、**プライバシーの欠如が一般的に受け入れられるようになる可能性**がある。

(参考４)世界プライバシー会議(GPA) 顔認証技術に関する決議

- 決議前文において、以下のとおり述べている（一部抜粋）。
  - 顔認証技術の能力は重要であり、その潜在的な応用が**セキュリティと公共の安全に利益をもたらす**可能性がある。
  - 顔認証技術は、**広範な監視**を可能にし、**侵入的**で、**偏った結果を提供**し、データ保護、プライバシー及び人権を侵害する可能性がある。
  - 顔認証技術は**ユニークで永続的なセンシティブな生体情報に依存**しており、個人に関する決定は潜在的に**本人の認識や同意なく行われる**ため、適切な救済手段がなければ不利益をもたらす可能性がある。
  - **個人を誤って識別又は認証する可能性若しくは識別又は認証できない可能性**がある。
  - 顔認証技術の利用が進化し、**予期せぬ方法で利用されたり、他の技術的能力と結びつき、個人や社会の信頼に危害を加える可能性がある**。
  - **本人の認識又は同意なく様々な公開又は非公開ソースから情報が集められた大規模データセットが作成**され、**新しい又は予期せぬ文脈で商業的に利用することが可能**である。
  - 顔認証技術の広範な使用は、**差別的効果**を伴い、**表現の自由や結社の自由といった基本的人権の行使に影響を与える**可能性がある。

(参考５)英情報コミッショナー意見書「公共の場所でのライブ顔認証技術の使用」

- 以下のとおり述べている。（「2.Introduction」等）。
  - 顔認証技術は私たちの生活を**より簡単に、より効率的に、より安全にすることに役立つ**。
  - ライブ顔認証技術は、多くの場合生体情報の**自動収集**を伴う。
  - ライブ顔認証技術は、特定の個人ではなく、**特定のエリアにいる全ての人を対象とし、カメラの範囲を通過する全ての人の生体情報を自動的かつ無差別に取得することができる**。その情報はリアルタイムに取得され、大量に収集される可能性がある。この処理にはしばしば**個人の認識、選択、コントロールが欠如**している。
  - 生体情報は他の個人データよりも、**永久的で変化しにくく、容易に変更することはできない。顔画像から抽出された生体情報は様々な文脈で個人を一意に識別するために利用でき、年齢、性別、ジェンダー、民族などの特徴を推定又は推論するために利用することができる**。
  - 公共の場でライブ顔認証技術を利用することを決定するために、データ保護影響評価を行わなければならないが、その際は**個人データ保護権や、表現、結社、集会の自由などのより広範な人権に対する直接的又は間接的な影響**も含まれる。

(参考５)英情報コミッショナー意見書「公共の場所でのライブ顔認証技術の使用」

- さらに、以下のデータ保護の重要な問題を特定したと述べる（「3.1.4 Key data protection issues」）。
  - **明確な正当化根拠のないスピード及び規模の生体情報の自動収集**が行われる。
  - 個人やコミュニティの**コントロールの欠如**
  - **透明性の欠如**
    - ✓ 本人に対し、ライブ顔認証技術がいつ、どこで使用されているか、どのよう、なぜデータが処理されているか、どのように権利を行使できるかが明確になっていない。
    - ✓ 透明性の欠如によりデータ保護権の行使への影響を及ぼしかねない。
  - **ライブ顔認証システムの技術的有効性と統計的正確性**
    - ✓ ライブ顔認証システムの統計的精度が十分正確でない場合、「偽陽性」又は「偽陰性」が発生する。誤判定による追加的監視、施設からの退去、法執行当局への問い合わせや拘束の可能性がある。
    - ✓ システムをメーカーから購入する際の、デューデリジェンスが欠如している。
  - **偏見と差別の可能性**
    - ✓ 顔認証技術の機能のほか、**ウォッチリストの作成過程にも偏見や差別のリスクがある**。
  - **ウォッチリストが合法的、公正かつ透明性のある方法で作成、維持されていない**場合がありうる。
  - **顔認証技術で何者かが識別された場合のエスカレーション過程が明確でない**。