資料3

顔識別機能付き防犯カメラの利用に関する国内外動向

令和4年1月28日

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

顔識別カメラを用いた国内における取組等

①大阪ステーションシティ「ICT技術の利用実証実験」

- 2014年情報通信研究機構（NICT)はJR大阪駅一帯の商業ビル・公共空間において、監視カメラから取得する画像データと顔識別技術をもとに人流解析を行う実証実験を予定。準公共空間でのデータ取得や不正取得、実証実験の回避等の市民からの懸念を理由に延期となった。

②札幌市「札幌市ICT活用戦略」

- 札幌市が行う実証事業（2016～18年度）にて、個人の特徴や希望に合った情報を発信することにより効果的なマーケティングまたは防災、防犯対策等を目的として、顔識別カメラや人感センサー・デジタルサイネージ等のICT機器の設置を検討。顔識別カメラのプライバシー侵害や情報流出等の市民の不安が高まったことから、顔識別カメラは設置しない計画となった。

③渋谷書店万引対策共同プロジェクト

- 渋谷駅周辺の3書店が2019年7月より、書店内において発生する万引き、盗撮、器物損壊、暴行・傷害、公然わいせつに当たる犯罪の防止を目的として、個人情報保護法の「共同利用」に基づいて、参加店舗間で万引き等を実行した対象者等に関する情報を共有。

④JR東日本「不審者・不審物検知機能を有した防犯カメラの導入」

- JR東日本が東京オリンピック・パラリンピックを控えた2021年7月よりセキュリティ向上の取組として、首都圏の一部の駅に、不審者等の検知機能（うろつきなどの行動解析、顔識別技術）を有した防犯カメラを導入。

カメラ画像利活用ガイドブック

- **「カメラ画像利活用ガイドブック」は総務省及び経済産業省が検討を推進。**
- **商用利用を目的（ただし、特定の個人を識別して個人向けに何らかの具体的なサービスを返す目的は対象外）としたカメラ画像の取扱いに関して、事業者自らのリスクベースでの判断を可能とすべく、プライバシー侵害のリスク要因について注意喚起し、共通的なリスク対策部分を配慮事項として整理。**
- **2017年1月にカメラ画像利活用ガイドブック「ver.1.0」を公表。**
- **2018年3月には同一人物が来店した際に、来店履歴や購入履歴等を分析する『リピート分析』をユースケースとして追加し、ガイドブック「ver.2.0」を公表。**

【適用ケース（ver2.0時点）】
1) 店舗内設置カメラ（属性の推定）
2) 店舗内設置カメラ（人の行動履歴の生成）
3) 店舗内設置カメラ（リピート分析）
4) 屋外に向けたカメラ（人物形状の計測）
5) 屋外に向けたカメラ（写り込みが発生し得る風景画像の取得）
6) 駅構内設置カメラ（人物の滞留状況把握）

※現在、改正個人情報保護法との関係から対応すべき点や、国内外の動向を踏まえ、個人情報保護・プライバシー保護について注意喚起すべき点などを追加検討し、ver3.0の改定作業中。
今後パブリック・コメントを経て公表予定。

日弁連の意見書等

2021年に日本弁護士連合会が顔認証システムに関する２つの意見書等を公表。
公共性の高い空間における防犯目的での顔認証システムの利用について、本人同意、又は必要性及び相当性を慎重に検討した上での立法化を主張。

①行政及び民間等で利用される顔認証システムに対する法的規制に関する意見書（2021年9月16日）

- 不特定多数に対する顔認証システムに対して、明示的同意や、対象者の権利保護を盛り込んだ法律の制定。
- 特定の人に対する顔認証システムの場合についても、明確な要件の策定。
- 重大組織犯罪の捜査の場合に限定した法律を定めることなく実施される、顔認証システムを利用した捜査等の、顔認証システムを使用する３つの政策を中止するべき。
- 行政一般については、顔認証データの収集及び照合利用は必要性がないなら許されるべきではない。

②鉄道事業者における顔認証システムの利用中止を求める会長声明（2021年11月25日）

- 駅構内という公共性の高い空間であり、店舗の場合における顔認証システムを導入していない他の店舗を選択するなどの他の選択肢は必ずしも容易ではなく、プライバシー権を著しく損なう。
- 警察の犯罪捜査体制に日常的に組み込まれている関係になり、警察が顔認証システムを令状なく利用しているに等しい。
- 民間事業者の場合も含め、顔認証システムの利用は、必要性及び相当性を慎重に検討した厳格な法律の定めに基づき行われるべきである。また他の方法を選択することが困難である公共性の高い空間における顔認証システムは、利用者が同意しない場合、立法により容易に正当化されがたい事を考え、鉄道事業者における利用は中止されるべき。

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

- EUの個人データ保護に関する諮問委員会であるEDPB（欧州データ保護会議）は2019年7月10日に、「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（案）」を公表し、パブコメ後、2020年1月29日に正式版を公表。
- これはGDPR（一般データ保護規則）の下でのカメラ画像や顔識別技術等の取扱いに関する指針であり、EU各国のデータ保護機関がGDPRの執行を行う際の根拠となる。（EDPBはEU各国のデータ保護機関から構成。）
- 本ガイドラインにおいても、ビデオ監視システムで特別な種類のデータ※を取得する場合については、データ管理者は、第9条に基づく特別な種類のデータを取扱うための例外（データ主体の明確な同意など）と第6条に基づく法的根拠の両方を特定しなければならないという一般的な記述にとどまる。（本ガイドラインは顔識別システムのみならず、従来型のCCTVも適用範囲としている）

※人種的若しくは民族的な出自、政治的な意見、宗教上若しくは思想上の信条、又は、労働組合への加入を明らかにする個人データの取扱い、並びに、遺伝子データ、自然人を一意に識別することを目的とする生体データ、健康に関するデータ、又は、自然人の性生活若しくは性的指向に関するデータ

ガイドライン項目

1　はじめに
2　適用範囲
3　取扱いの適法性
4　第三者へのビデオ映像の開示
5　特別な種類のデータの取扱い
6　データ主体の権利
7　透明性と情報に関する義務
8　保存期間と消去義務
9　技術的及び組織的な措置
10　データ保護影響評価

（参考）GDPR（General Data Protection Regulation：一般データ保護規則）（抄）

第9条 特別な種類の個人データの取扱い

1. 人種的若しくは民族的な出自、政治的な意見、宗教上若しくは思想上の信条、又は、労働組合への加入を明らかにする個人データの取扱い、並びに、遺伝子データ、自然人を一意に識別することを目的とする生体データ、健康に関するデータ、又は、自然人の性生活若しくは性的指向に関するデータの取扱いは、禁止される。

2. 第1 項は、以下のいずれかの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のその個人データの取扱いに関し、明確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 項に定める禁止をデータ主体が解除できないことを定めている場合を除く。

(b) （略）

(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場合で、データ主体又はその他の自然人の生命に関する利益を保護するために取扱いが必要となるとき。

(d)～ (f)（略）

(g) 求められる目的と比例的であり、データ保護の権利の本質的部分を尊重し、また、データ主体の基本的な権利及び利益の安全性を確保するための適切かつ個別の措置を定めるEU 法又は加盟国の国内法に基づき、重要な公共の利益を理由とする取扱いが必要となる場合。

(h) ～ (j) （略）

3. （略）

4. 加盟国は、遺伝子データ、生体データ又は健康に関するデータの取扱いに関し、その制限を含め、付加的な条件を維持又は導入することができる。

EUのAI規則案

- **欧州委員会は2021年４月21日付でAI規則案を公表。**
- **同規則案は、AIを①受容できないAI、②ハイリスクAI、③透明性義務を伴うAI、④極小リスク／リスクなしAIの４つのカテゴリーに分類した上で、使用方法について規定するものであり、①は原則禁止、②は要件と事前適合性評価の準拠を条件に許可、③は情報／透明性の義務を条件に許可、④は制限なし、という原則を規定している。**
- **法執行の目的により公の場所において遠隔地からのリアルタイム生体識別システムを使用する行為は①として、一定の例外の除いて禁止されている。これ以外の遠隔地からの生体識別に使用することを目的としたAIシステムは②として、要件と事前適合性評価の準拠を条件に許可されている。**

- 法執行の目的により、公の場所において、遠隔から「リアルタイム」生体識別システムを使用する行為は原則として禁止される。ただし、行方不明の子供を含む、犯罪の特定の潜在的な被害者を対象とした捜索、実質的かつ差し迫った脅威またはテロ攻撃の防止、一定の犯罪の犯罪者・容疑者の検出、特定、起訴のために厳密に必要な場合には例外としている。
- ハイリスクAIとして、自然人の生体識別及び分類（リアルタイムで行うか否かを問わず、遠隔からの生体識別に使用することを目的としたAIシステム）を挙げている。ハイリスクAIに対しては、リスク管理プロセスを確立して実装、高品質な学習・検証・テストデータの利用、文書化の確立・ログ機能の設計、適切な透明性確保・ユーザーへの情報提供、人間による監視、堅牢性・正確性・サイバーセキュリティ確保等が要求されている。

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」

- **ICO（英国のデータ保護機関）は2021年6月18日付で「The use of live facial recognition technology in public places」（公共の場所でのライブ顔認証技術の使用）と題する文書を公表。**
- **同文書は、ライブ顔認証を複雑かつ斬新なタイプのデータ処理を行うものと位置付けた上で、ライブ顔認証に対して英国のデータ保護法制度がどのように適用されるかを説明するための意見として公表された。**
- **公共の場所におけるライブ顔認証技術の使用に関しては、英国GDPRが求める「特別な種類の個人データ」の処理を可能とする条件を満たす必要があるが、第9条(2)（g）の「重要な公共の利益」を理由とする取扱いの可能性を示唆。**

- 顔認証技術は、状況に応じて英国GDPRで定義される異なるタイプの個人データを処理することになり、そのタイプに従って英国GDPRの規制を遵守することが必要である。
- 英国GDPRにおいては、生体認証データ（顔画像は個人の一意の識別を可能又は確認するための特定の技術処理が実行されると生体認証データとなる）は自然人を一意に識別する目的で処理される場合には「特別な種類の個人データ」として規制しており、英国GDPR第９条に従う必要がある。また、犯罪データの処理を含む場合には、英国GDPR第10条に従う必要がある。
- 英国GDPR第9条(2)（g）を満たす例としては、違法行為の防止又は検出、危険にさらされている子どもや個人の保護等である。

欧州評議会　顔認証に関するガイドライン

- **欧州評議会（※）は2021年1月28日に、「Guidelines on Facial Recognition」（顔認証に関するガイドライン）を公表。**
- **顔認証は、管理された環境下でのみ行われるべきであり、マーケティング目的や私的なセキュリティ目的のために、ショッピングモールのような管理されていない環境では、顔認証技術を使用すべきではないとしている。**

（※）欧州評議会（Council of Europe, CoE）は、EU加盟27カ国を含む計47カ国から成る。日本は、米国、カナダなどと共にオブザーバー国。

（※※）本ガイドラインは、欧州評議会の「個人データの自動処理に係る個人の保護のための条約第108号」（108号条約。日本は未批准であり、同条約の諮問委員会にオブザーバー参加）の批准国向けのものだが、批准国を法的に拘束するものではない。

- 管理されていない環境でのライブ顔認証の使用、適切な保護措置なしで、肌の色/人種/性別/信条/年齢/健康ないし社会的状態を判断することのみを目的とした顔認証の使用は法律で厳しく制限すること
- デジタル画像が、他の目的で作成された場合、新たな処理のための法的根拠がないまま、生体情報テンプレートの抽出や生体システムへの統合が行われないようにするための仕組みを確保すること
- 民間部門が行う顔認証では、データ主体の明示的、具体的、自由かつ情報提供された上での同意を必要とする。したがって、顔認証は、管理された環境下でのみ行われるべきであり、マーケティング目的や私的なセキュリティ目的のために、ショッピングモールのような管理されていない環境では、顔認証技術を使用すべきではない。
- 顔認証は、データ主体の認識や協力なしに行われうるため、透明性と公正性の確保が最重要であり、そのために十分な情報が提供されるべきである。
- 顔認証技術の使用は、目的の限定/データの最小化/記録保存の制限/正確性の原則に服する。特にライブ顔認証の場合は、ウォッチリストと生体情報テンプレートは、目的達成時（照合完了時）に削除されなければならない。

世界プライバシー会議（GPA）　顔認証技術に関する決議

- **2020年10月13日～15日に開催された第42回世界プライバシー会議（※）においては、顔認証技術について、その導入によってもたらされる便益と、権利侵害の可能性等を踏まえながら議論が行われ、以下の決議が採択された。**
- **その後、「原則」について検討を進めるためのサブワーキンググループが組織され、日本も参加。当初予定より遅れてはいるものの、引き続き作業中。**

（※）世界プライバシー会議（GPA;Global Privacy Assembly）は、各国のデータ保護機関等130の機関等が参加し、国際的な個人データ・プライバシー保護の促進や強化等についての議論や情報交換を行う会議体。40年以上の歴史を持つ。当委員会は、2017年より正式メンバーとして参加。

- 以下の原則の重要性を再確認する。
  - データ保護及びプライバシー・バイ・デザイン
  - 必要性及び比例性
  - 透明性及び説明責任
  - 公正性
  - 倫理的アプローチ

- 顔認証技術に係る個人情報の適切な利用に関する原則及び期待事項を策定し、第43回世界プライバシー会議での採択を目指す。同原則等の策定に向け、傘下の国際執行協力WG及びAIにおける倫理とデータ保護に関するWGに対し、他の関係者と協議しつつ作業を行うよう要請する。