

# 万引き対策で顔認証システムの利用は許されるのか

松本七海<sup>†1</sup>

**概要**：映像技術の向上によって生み出された高精細映像と人工知能を組み合わせることにより、以前と比べてはるかに優れた正確性を持つ顔認証システムがあらゆる面で利用されている。しかし万引き対策における利用においては、十分な法的議論がなされないままである。本稿は個人情報保護法や民法上の観点から、顔認証システムの在り方について検討する。

**キーワード**：人工知能、顔認証システム、万引き対策、個人情報保護法、民法、監視社会

## Is it permitted what the face recognition system uses as shoplifting measures ?

NANAMI MATSUMOTO<sup>†1</sup>

**Abstract**: A face recognition system of the much superior accuracy is used with every aspect than before by putting high-definition picture and artificial intelligence produced by improvement of the imaging technique together. However, about the use for shoplifting measures, there is it without enough legal arguments being accomplished. From viewpoint of Personal Informational Law and Civil Law, this study examines the role of face recognition system.

**Keywords**: AI, Face recognition system, Shoplifting measures, Personal Informational Law, Civil Law, Mass surveillance

### 1. はじめに

顔認証システムの利用においては数年前から様々な問題が各マスコミで取り上げられている。2014年にJR大阪駅の駅ビルにおいて、人流統計を目的として顔認証技術を使って通行人を無差別にカメラで撮影し追跡する実験を試みたが、プライバシー侵害等を理由に市民から批判が寄せられ実験が中止になった事例がある[1]。また、同年初めて万引き対策での顔認証システムの利用による問題点が新聞報道等によって露わになった。スーパーやコンビニ等の防犯カメラで自動的に撮影された客の顔が顔認証で解析され、客の知らないまま、顔データが他の店舗と共有されていることが明らかになった[2]。この問題については、日本だけでなく米国においても同様のテクノロジーの利用がなされている[3]。その他本人確認やマーケティング等による顔認証システムの導入が次々になされることで、我々の生活が便利になっていく反面、プライバシー侵害に対する懸念が高まっている。

平成27年の我が国の個人情報保護法の改正により、顔認証により得られる身体的な識別情報が、新たに「個人識別符号」(2条1項2号)として明確化された。また今年1月には総務省からこれからの監視カメラの利活用につき、事前告知を含む配慮事項をまとめた「カメラ画像の利活用ガイドブック」が出されており、わが国ではまさに顔認証に対する規制が明確化され、民間事業者が顔認証システムの

利活用を推し進めている最中であるといえる。法務省では、審査の円滑化とテロ対策の強化を目的として、今年10月中旬から羽田空港の入国審査に「顔認証ゲート」を導入することを発表した[4]。

しかし顔認証においては、権利侵害の危険性の高さや監視社会への懸念等も考えられるため、個別の事案ごとに十分な法的議論がなされる必要がある。本稿では、万引き対策における顔認証システムの在り方を現行個人情報保護法や権利侵害の場合に被害者が求められる法的救済との側面から検討を行う。

### 2. 顔認証システム

#### 2.1 顔認証技術

顔認証技術は、「顔検出技術」、「特徴点検出技術」、「顔照合技術」から成り立っている。「顔検出技術」では、一般化学習ベクトル量子化方法を用いて、矩形領域が顔か非顔かを識別する。「特徴点検出技術」では、多点特徴点検出法により、顔矩形領域から瞳中心、鼻翼、口端等の特徴点の位置を探索する。「顔照合技術」では、多元特徴識別法を用いて、顔の中から目鼻の凹凸や傾き等の様々な特徴を抽出した後、これらの特徴の中から個人を識別するために最適な特徴を選択することにより、経年変化の影響を受けにくくなるなど、様々な変動に対応可能な個人識別が実現できる[5]。

<sup>†1</sup> 新潟大学法学部(情報法ゼミ)115a228h@mail.cc.niigata-u.ac.jp

## 2.2 情報処理の機序の例

映像情報は、店舗内に設置したカメラにおいて撮影され、同施設内の装置において映像解析処理を受け、特徴量情報等(特徴量情報及び撮影された時刻、場所、判定された対象者の性別と年齢)が生成された後、消去される。映像情報は、同施設内のパソコン上にも記録され、存続期間が過ぎると消去される。また、映像情報が解析処理される際、1台のカメラフレーム内で撮影された個人ごとにIDである識別子が付与される。この識別子は、同一人物を識別して特徴量情報を作成するために用いられ、特徴量情報の生成とともに削除される[6]。

## 2.3 データ共有の構想

NPO法人全国万引犯罪防止機構は、警察などとも連携して、犯人の顔写真の共同利用を目指している。加盟する書店に関しては、顔認証と連動して当該人物が入店した際に自動的にわかる仕組みを既に取り入れているが、書店で「確保した犯人情報」、「取り逃がした犯人情報」等を管理組織に随時登録していくことで、データベースを構築していく。更に、書店は確保した犯人の前歴や組織犯罪との関係をデータベースと照会し、回答を受け取ることもできる[7]。

## 3. 現行個人情報保護法の適用

### 3.1 個人情報該当性

#### (1) 瞬間的な「映像情報」の「個人情報」該当性

「まず、カメラ画像が、そこに写る顔等により特定の個人を識別できるものであれば「個人情報」に該当する」[8]。しかし、数十秒で消去される場合においては、瞬間的に生成されるこうした中間データについて、法的観点から「個人情報」と評価すべきか否かについては、議論のありうところであり、判断材料として、利用者の不安や嫌悪感、また、「個人情報」の客観的該当性を考慮に入れる必要がある。

「利用者の不安や嫌悪感という点に関して、カメラの設置、撮影、記録に関する事実関係が被撮影者に事前に説明されることなく、またはその事実関係が外形上不明である場合は、カメラで撮影された情報は、「個人情報」として取り扱われるべき」だとする[9]。

また、我が国の個人情報保護法制において、「個人情報」の定義を定めるに際して、いわゆる情報プライバシー型ではなく、特定個人の識別情報型を採用している[10]点に着目すれば、個人の権利利益への影響の程度等といった実質的な評価に踏み込むことなく、外見から客観的に見て「個人情報」該当性を判断していると言える。

つまり、このような考え方を基礎として判断する場合には、カメラによる撮影により取得された「映像情報」は、「個人情報」に該当すると言える[11]。

#### (2) 「特徴量情報」の「個人情報」該当性

顔認証によって得られたデータは、個人情報保護法2条2項1号における「特定の個人の身体の一部を電子計算機の用に供するために変換した文字、番号、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」であるため、個人識別符号に該当する。

### 3.2 個人情報取扱事業者の義務

個人情報取扱事業者は、個人情報保護法の18条から23条で定められている、取得に際しての利用目的の通知や第三者提供の際に本人同意を得ること等の規定を遵守しなければならない。

### 3.3 本人の請求

個人情報保護法28条から30条の規定により、本人は、個人情報取扱事業者に対して、当該個人が識別される保有個人データの開示、訂正、利用停止などの措置を求めることが可能である。いずれも旧法案の「透明性の確保」原則に対応するものであり、平成27年度改正法により、裁判上の請求ができる権利であることが認められた[12]。

## 4. 民法上の違法性について

顔認証システムが個人情報取扱事業者によって個人情報保護法の規定通り行われていれば、違法性はないと判断できる。しかし、特徴量情報をみだりに取得されない自由等のプライバシー侵害におけるいくつかの問題点が考えられるため、それらの点について検討を行う。

### 4.1 肖像権侵害

#### (1) 裁判例に見る肖像権侵害の違法性基準

肖像権についての最初の裁判例である京都府学連事件では、警察官が集団先頭の進行状況を写真撮影した行為が問題となった。最高裁判所大法廷は、「個人の私生活上の自由の一つとして、何人も、その承諾なしに、みだりにその容ぼう・姿態(以下「容ぼう等」という。)を撮影されない自由を有するものというべきである。これを肖像権と称するかどうかは別として、少なくとも、警察官が、正当な理由もないのに、個人の容ぼう等を撮影することは、憲法13条の趣旨に反し、許されないものといわなければならない」と判示したが、公共の福祉の観点から、「現に犯罪が行われ、もしくは行われたのち間がないと認められる場合であって、しかも証拠保全の必要性及び緊急性があり、かつその撮影が一般的に限度をこえない相当な方法をもって行われるとき」であれば、対象者の中に犯人やその周辺にいる第三者の容貌等を含む写真撮影であっても、許されると判示した[12]。また、下級審判決としては、自宅キッチン内の姿を塀の上に設置したカメラで撮影・公表した事案[13]、銀座の公道を歩く一般人の写真を容貌も含めて大写して撮影し、ウェブサイトに掲載した事案[14]において違法性が認められた。一方、公道を歩行中の者の上半身を撮影・公表した事案[15]、自宅玄関前での背広姿の全身を撮影・公表した事案[16]においては、違法性は否定された。

「諸判決の判断基準を概観すると、特定人に焦点を当てて撮影していれば違法性が認められる傾向にある一方で、公道に準ずる公共性のある場所で撮影された場合、記事の掲載についての公共の利害や公益目的がある場合、写真撮影の態様や写真の内容が私生活をのぞき見るようなものではない場合、写真撮影および掲載が表現の自由の正当な行使であると認められる場合の違法性は否定されている[17]。

**(2) 当てはめ**

「上記裁判例の傾向に照らし検討すると、何人も、その承諾なしに、みだりにその容貌・姿態を撮影されない自由を有し、この自由は私人間においても保護されるべき法的権利と解される」ところ、万引き対策における顔認証システムの利用においては、店舗内に設置された入口に設置されたカメラによって、個人を撮影し、その画像を生成するものであるから、肖像権を侵害するものであると解することができることも考えられる。しかし、「上記最高裁判所判決にいう「撮影」は、映像情報をフィルムだけでなくSDカード等に記録する行為も含むと解されるものの、揮発性メモリ上に、ごく短時間映像データが存在するだけの機械的プロセスが、法規範的にみて、「撮影」に該当するかについては、疑問が残る。また、肖像権とは、人の画像(写真・絵画等)に表出される人格を保護法益とする権利であるから、画像から抽出された情報であっても、特徴量情報のように、人格が表出されていないものに対しては、肖像権の問題ではなく、プライバシー権の問題と考えるべきである」[18].

**4.2 プライバシー権侵害**

**(1) 裁判例に見るプライバシー侵害の違法性基準**

わが国において、プライバシーの権利は、まず、私生活の平穩に着目して展開され、「宴のあと」事件において「私生活をみだりに公開されないという法的保障ないし権利」というように定義されていた[19]. 早稲田大学江沢民講演会名簿提出事件では、大学学生の学籍番号・氏名・住所・電話番号といったような「秘匿されるべき必要性が必ずしも高いものではない」個人情報であっても、「本人が、自己が欲しない他者にはみだりにこれを開示されたくないと考えることは当然のことであり、そのことへの期待は保護されるべきものである」とし、このような個人情報をプライバシーにかかる情報として法的保護の対象にするとし[20], プライバシーの対象となる情報は拡大傾向にある。

**(2) 当てはめ**

**① 画像の取得**

短時間で画像が消去される場合においては、誰の目にも触れることはないため、画像撮影におけるプライバシー侵害はないか、あるとしても些細なものであって、社会生活を営むうえで容認される範囲に属すると解される。しかし、短期間では画像が消去されない場合は、第三者に閲覧される危険性があり、また、映像情報が蓄積していくことにより、日常の行動履歴を把握できる可能性も考え得るため、プライバシー侵害がないとはいえない。

**② 特徴量情報生成**

高度なデジタル技術とインターネットが広く普及した現代社会において、全身や顔の画像などから当該個人固有の情報を抽出することは、承諾なき行動履歴の収集や記録を可能とし、これを通じて、平穩な生活を害する潜在的危険性を有するため、「個人識別符号」を第三者によってみだ

りに取得されない自由は、プライバシー権によって保護される法的利益と認められる[21].

「個人識別符号」は、特定個人の身体の一部を記号化や暗号に置き換えただけのものであるため、プライバシー権侵害の可能性は否定できない。

**③ 第三者提供**

万引き対策を目的としていることから、万引き犯の情報を加盟店同士で共有することは当然に考えられ、このことが利用者のプライバシーを侵害する可能性は大いに考えられる。

**(3) プライバシー侵害における法的責任**

憲法 13 条にその基礎を有する人格権は、人間の尊厳に由来し、①人格の自由な展開の保証、②個人の私生活領域の平穩の保護を目的とする権利である。プライバシー権は人格権としてとらえられ、プライバシーを侵害された者には以下の効果が及ぶと解されている[22].

**① 損害賠償**

民法 709 条によれば、故意又は過失によって他人の権利又は法律上保護される利益を侵害することは不法行為であり、損害賠償責任を負わなければならない。

**② 差止請求**

北方ジャーナル事件において、名誉を侵害されたものは、「人格権としての名誉権」に基づき、現に行われている侵害行為を排除し、または将来生ずべき損害を予防するために、侵害行為の差止めを求めることができる[23]. プライバシーの侵害を理由とする差止めについても、通説はこれを否定しない。ここでは、侵害状態が継続する場合に、この状態を将来に向かって解消するための物理的行為を命じる特定の救済が肯定されることとなるであろう[24].

**③ 現状回復**

他人の名誉を毀損したものに対して、裁判所は、被害者の請求により、損害賠償に代え、または損害賠償とともに、民法 723 条に基づいて、名誉を回復するのに適当な処分(低下した社会評価の回復のために適当な処分)を命じることができる[25].

**5. カメラ画像利活用ガイドブックの適用**

生活者のプライバシー侵害や、生活者が望まない形でデータが利用されることに対する漠然とした不安等の課題に対し、個人情報保護法により守られるべき範囲だけでなく、プライバシー保護の観点から配慮が必要な範囲を適用対象としたガイドブックを今年 1 月に総務省が発表した。下の表は、店舗内設置カメラの導入例において好ましいとされる事業者の対応である[26].

分類	配慮事項	配慮事項に基づき、実施する対応例
基本原則	1. リスク分析の適切な実施 一元的な連絡先の設置	・データのライフサイクル等を分析し、システム管理者等を定めた運用体制を実施している。 ・問い合わせ窓口を設置した。

事前告知時の配慮	2. 事前告知の実施	・ 自社 HP 上でのリリースを実施した。 ・ 新聞等メディアへの掲載を促した。
	3. 事前告知内容	・ 運営全体趣旨として「当社が店舗を対象に実施する」旨を明記した。 ・ 個人特定にはつながらないことを明記した。
	4. 多言語化	・ 英語, 中国語, 韓国語による自社 HP での発信を行った
	5. 通知の実施	・ ポスターに掲示 ・ 自社 HP へ掲載している
取得時の配慮	6. 通知内容	・ 運用実施主体の主語を「株式会社〇〇」として記載した。 ・ 特定個人にはつながらないことを明記した。
	7. 多言語化	・ 英語, 中国語, 韓国語による HP 上での情報発信を行った。
	8. 画像の破棄	・ カメラ画像はシステムメモリ上で処理され, 保存されることなく破棄する。
取扱時の配慮	9. 処理方法の明確化	・ 「お客様を個々に特定できないデータ」に処理している。
	10. 処理データの保存	・ 推定した属性情報から生成した混雑予想値を統計情報として保存する。
	11. 適切な安全管理措置	・ 撮影したカメラ画像データは特微量データ抽出後, 直ちに破棄している。 ・ 特微量データは, 属性情報を指定した時点で, 直ちに破棄している。
管理時の配慮	12. 利用範囲, アクセス権	・ データの利活用は自社グループ内に限定している。 ・ データアクセスをシステム管理者のみに限定している。
	13. 第三者提供時の適切な契約締結	・ 他社へ提供しないことを自社の HP 上に明記した。
	14. 契約変更時の事前告知	-

図表 配慮事項の対応例  
 出典: カメラ利活用ガイドブック

さらに総務省は, 今後も事業者のユースケースに合わせてガイドブックの改訂を行っていく旨の記述を残し, 生活者の権利保護を念頭に, これから更なるカメラの安全な利活用が期待できる。

## 6. 問題点

上記で触れてきた万引き対策における顔認証システムの利用は, 個人情報取扱事業者が主体であることを前提として検討を行ってきたものであるが, 前述 2.3 において全国万引き防止委員会が構想として発表していたように, 「警察と連携して犯人のデータ共有をする場合」においては, 警察のデータベースの取り扱い方によっては問題が起り得る。

刑法学において, 強制処分や任意処分の場合, 情報を「取る」という瞬間に焦点を当てて(取得時中心主義[28])その正当性を論じてきたために, 取得後の情報の管理・利用の在り方について, 警察実務では指紋データベースや DNA 型データベースが法律上の根拠なく構築・運用されて

しまっている[29].

しかし, 情報の管理・利用の侵害性を刑事訴訟において問題とすることには困難を伴う。なぜなら, 情報の取得時点や利用時点よりも時間的に後に当該情報の具体的な管理・利用の状況が確定することになるため, 「当該情報の具体的な取得・管理・利用の状況を考慮した侵害性の測定」は, 刑事手続の進行過程では行得ない場合も少なくないと考えられるからである[30]。他方, 判例では, 梱包内容をエックス線検査することの適法性において「その射影によって…, 内容物によってはその品目等を相当程度具体的に特定することも可能」[31]であることを問題とし, 「品目等の具体的な特定が相当程度可能な場合もあればそうでない場合もあるけれども, 可能な場合のあることが, 本件 X 線検査の強制処分性を肯定する根拠になる」[32]としている。このように「『宅配便荷物の X 線検査』という限度で操作行為を抽象化一般化し典型的に把握」[33]する方法であれば, 取得中心主義から脱却することも可能である[34].

いずれにせよ, 万引き犯またはその他の犯罪者のデータベースを管理する際に, 個人情報保護法制の一般的拘束から逃れる, 警察による個人情報の管理・利用を法的に聖域化してしまう恐れがあると考えられる。

## 7. 今後の課題

以上の通り, 諸法との関係から万引き対策における顔認証システムの在り方を検討したが, 特に 6 で触れた問題点においては, 万引き犯に対してだけではなく, テロ対策等のナショナルセキュリティを考える上でも避けては通れない論点である。そのため, 今後人権保障の観点から, 警察の情報の管理・利用に際しては, 侵害概念の査定を考慮に入れた議論を重ねていくことが求められる。

## 参考文献

- [1] 映像センサー使用大規模実証実験検討委員会 「調査報告書」 <https://www.nict.go.jp/nrh/iinkai/report.pdf>, (参照 2017-08-10).
- [2] 読売新聞 「客の顔情報「万引き対策」115 店が無断共有」 2014.4.5 朝刊.
- [3] LP Magazine 「Facial Recognition: A Game-Changing Technology for Retailers」 <http://losspreventionmedia.com/feature-articles/item/2482-facial-recognition-a-game-changing-technology-for-trtailers.html>, (参照 2017-08-12).
- [4] 毎日新聞 「羽田で導入 10 月から, 帰国の日本人対象」 2017.7.4.
- [5] NEC 「顔認証技術」 <http://jpn.nec.com/rd/research/DataAcquition/face.html>, (参照 2017-08-12).
- [6] 映像センサー使用大規模実証実験検討委員会・前掲[1], (参照 2017-08-12).
- [7] 新文化通信社 「万引き犯のデータベースを書店と共有 翻万防止機構・竹花氏が構想発表」 <https://www.shinbunka.co.jp/news2017/02/170215-01.htm>, (参照 2017-08-12).
- [8] 総務省「カメラ画像利活用ガイドブック ver.1.0」 [https://www.soumu.go.jp/main\\_content/000462242.pdf](https://www.soumu.go.jp/main_content/000462242.pdf), (参照 2017-08-12)

- [9] 映像センサー使用大規模実証実験検討委員会・前掲[1], (参照 2017-08-12).
- [10] 大西達夫「情報公開条例における非公開個人情報該当性の解釈について」判例タイムズ No.1025(2000.5.15)53 頁
- [11] 映像センサー使用大規模実証実験検討委員会・前掲[1], (参照 2017-08-12).
- [12] 宇賀克也『個人情報保護法の逐条解説 第五版』(有斐閣,2016).
- [13] 最判昭和 44 年 12 月 24 日刑集 23 卷 12 号 1625 頁.
- [14] 東京高裁平成 2 年 7 月 24 日判時 1356 号 90 頁.
- [15] 東京地判平成 17 年 9 月 27 日判時 1917 号 101 頁.
- [16] 岡山地判平成 3 年 9 月 3 日判時 1408 号 107 頁.
- [17] 東京地判平成 13 年 12 月 6 日判時 1801 号 83 頁.
- [18] 映像センサー使用大規模実証実験検討委員会・前掲[1], (参照 2017-08-12).
- [19] 映像センサー使用大規模実証実験検討委員会・前掲[1], (参照 2017-08-12).
- [20] 東京地判昭和 39 年 9 月 28 日下民集 15 卷 9 号 2317 頁.
- [21] 最判平成 15 年 9 月 12 日民集 57 卷 8 号 973 頁.
- [22] 映像センサー使用大規模実証実験検討委員会・前掲[1], (参照 2017-08-12).
- [23] 潮見佳男『債権各論Ⅱ 不法行為法 第 2 版増補版』(新世社, 2016),211 頁.
- [24] 最大判昭和 61 年 6 月 11 日民集 40 卷 4 号 872 頁.
- [25] 潮見・前掲[21],217 頁.
- [26] 潮見・前掲[21],218 頁.
- [27] 総務省「カメラ画像利活用ガイドブック ver.1.0」  
[https://www.soumu.go.jp/main\\_content/000462242.pdf](https://www.soumu.go.jp/main_content/000462242.pdf), (参照 2017-08-12)
- [28] 山本龍彦「警察による情報の収集・保存と憲法」警察学論集 63 卷 8 号(2010)111 頁以下, 星野周一郎『防犯カメラと刑事手続き』(弘文堂,2012)81 頁
- [29] 捜査手法,取り調べの高度化を図るための研究会「最終報告」(2012)29 頁,  
<http://www.npa.go.jp/shintyaku/keiki/saisyuu.pdf>, (参照 2017-8-14)
- [30] 亀井源太郎「基調報告 憲法と刑事法の交錯」宍戸常寿ら『憲法学のゆくえ』(日本評論社,2016) 11 頁以下.
- [31] 最決平成 21 年 9 月 28 日刑集 63 卷 7 号 868 頁.
- [32] 笹倉宏紀「判批」平成 21 年度重要判例解説(2010)209 頁.
- [33] 笹倉・前掲[32]209 頁
- [34] 亀井・前掲[30]12 頁