北九州市立大学法政論集第 49 巻第 1・2 合併号（2021年10月）抜刷

論　　説

顔認証技術を用いた捜査手法に対する規制方法

―― EU、ドイツにおける議論を参考に ――

水　野　陽　一

北九州市立大学法政論集第49巻第１・２合併号（2021年10月）

論　　説

顔認証技術を用いた捜査手法に対する規制方法
――EU、ドイツにおける議論を参考に――

水　野　陽　一*

はじめに

わが国における監視カメラ設置は設置主体を問わず都市部を中心に急速に広がっており、そこから人の顔画像を含む膨大な映像が日々取得されている(1)。入手された映像を、日夜進化を続けるAIによる顔認証技術を用いて処理・解析することで、広範囲かつ容易に正確に人物特定を行うことが可能になる。顔認証技術とは、映像や画像の中から人を判断する技術であり、画像中から「顔がどこにあるか」を検出し、瞳、鼻、口など、「その

* 本学法学部准教授。

(1) この様な状況に危機感を抱き、適切な規制、統制を求めるものとして、例えば日本弁護士連合会による顔認証システムに対する法的規制に関する意見書「顔認証システムに対する法的規制に関する意見書」2016年9月15日がある。
https://www.nichibenren.or.jp/library/ja/opinion/report/data/2016/opinion_160915_2.pdf

人の顔の特徴的なポイントがどこにあるか」を見つけ（顔特徴量データの検出）、検出された顔の特徴点から「誰であるか」を判定するものをいう(2)。

近年、顔認証技術を用いた捜査方法が注目されている。日本の警察では顔認証システムのことを「3 次元顔形状データベース」と表記しており、警視庁は逮捕した全被疑者の顔のデータベース化を進めている。この顔認証データベースと民間事業者の監視カメラと連動するための非常時映像伝送システムが用意されており、事業者の持つ監視カメラの映像を警察がリアルタイムで一元監視し、顔認証できるようになっている。事業者とは具体的には公共交通機関（東京メトロ、JR 東日本、都営地下鉄）を指す。警察の顔認証システムの利用については 2014 年の段階で警視庁、茨城県警、群馬県警、岐阜県警、福岡県警に「可搬型顔画像検出照合装置」が導入されていたことがわかっている(3)。その後、民間の監視カメラの活用するための非常時映像伝送システムができた。これらのシステムに加え、民間が設置した顔認証データベースは、裁判所の判断に拠らず捜査事項照会書の提示で閲覧しているものと考えられる(4)。

以上のように、顔認証技術を用いた捜査手法は、幅広く警察捜査において導入されているものと考えられるが、顔認証技術を含め AI 技術等先端技術を用いたわが国の警察捜査において個人情報保護に配慮した対応が十分に行われているとはいいがたい実情がある。本稿では、EU における AI とデータ保護に関する議論及びドイツにおける顔認証技術を用いた捜査についての議論を参照し、わが国においても十分な個人保護に配慮しつつ AI を用いて個人情報を処理することを通じた個人特定を行う捜査手法統制のあり方が議論される必要があることを示す。

⑵ 顔認証技術の説明について、日本電気株式会社ホームページを参照した。
https://jpn.nec.com/biometrics/face/history.html

⑶ 日本弁護士連合会・前掲註⑴・3 頁。

⑷ 我が国の警察における顔認証技術の利用状況について、一田和樹「日本の警察は世界でも類を見ない巨大な顔認証監視網を持つことになるのか？」を参照した。Newsweek 日本版 2020 年 9 月 8 日 18:00 配信。
https://www.newsweekjapan.jp/ichida/2020/09/post-7.php

１．わが国における個人情報保護の現状

(1) 古典的プライバシー保護と自己情報コントロール権

日本における個人情報保護の現状について、大要以下のようにまとめることができる[5]。わが国の個人情報保護について、まず重要となるのはいわゆる「宴のあと」判決である[6]。本判決において、「私生活をみだりに公開されない法的保障ないし権利」が承認され、これは古典的なプライバシーの先例であるとされる。その後、対象者の意思に反して個人情報を取得する場合、これをプライバシー侵害として捉える自己情報コントロール権説が主張されるに至る[7]。これは、プライバシーを「プライバシー固有情報」と「プライバシー外延情報」とに区別し、前者は対象者の意思に反して取得される場合全てプライバシー権侵害となるが、後者については正当な目的・方法により情報を取得・利用する限りにおいて、違法なプライバシー侵害は生じないとする。とはいえ、「プライバシー外延情報」についても、これが悪用または集積されるならば、個人の自律的生存に影響を及ぼすことになるため、情報の収集・管理・利用・開示・提供の全てについて、原則として対象者の同意が必要であるとされる。

自己情報コントロール権の意義は、単純な個人情報にまで憲法的保護を拡大したことにあるが、プライバシー外延情報の制約には必ずしも法律上の根拠が要求されないことに問題がある。これは、情報そのものの価値に着目して、保護の度合いを決める考え方であるが、近年の技術革新、特にコンピューター処理の高速化とそれに伴う AI を用いたビッグデータの活用を考慮した場合、重要な情報とそうではない情報に分けるという発想が

(5) わが国におけるプライバシー権の発展について、小山剛「転換点としての GPS 捜査判決？」法学研究 91 巻 1 号（2018 年）3-6 頁を参照した。

(6) 東京地判昭 39 年 9 月 28 日下民集 15 巻 9 号 2317 頁。

(7) 佐藤幸治「プライヴァシーの権利（その公法的側面）の憲法論的考察」『現代国家と人権』（有斐閣、2008 年）259 頁以下（初出 1970 年）。

最早過去のものとなっており、情報それ自体の価値はもちろんだが、情報の扱われ方が如何なるものであるかが問われなければならない。

(2) 写真・映像撮影とプライバシー

写真・映像撮影とプライバシーを考える際に重要となるのが、いわゆる「京都府学連事件」判決である[8]。ここでは、憲法 13 条を引用し、個人に対して「みだりに容ぼう等を撮影されない自由」があることを認めつつ、一方で警察等国家活動にとって必要な範囲で、当該自由が制約されることが明言されている。更に、本判決を受け大阪地裁平成 6 年判決は、防犯目的での監視カメラ設置の許容性判断について、①目的の正当性、②客観的・具体的必要性の検討、③設置状況の妥当性、④設置使用による効果の存在、⑤使用方法の相当性があるか、という基準を示した[9]。街頭に設置されるカメラの多くは、「犯罪の予防、鎮圧」という警察の職務の遂行を目的とする（警察法 2 条、警察官職務執行法 1 条 1 項）[10]。ここでは行政警察活動と司法警察活動の区別が問題となる。わが国において、前者には法律の留保と比例原則に則った統制が、後者には強制処分法定主義と令状主義による統制が行われると説明されるのが一般的である。警察による監視カメラの設置及び利用につき、判例、裁判例において利用目的と対象者の権利保障に配慮しつつ許容性判断が行われる旨判示されたが、わが国において写真撮影、映像記録を行う捜査手法に関する刑事訴訟法上の規定は存在しておらず、司法警察活動としての監視カメラ設置及び利用に対する統制が十分に働かない現状にある。行政警察活動としての監視カメラ設置について、個人情報保護法による統制が行われてはいるが[11]、ここでも監視カメラ設置及びその利用についての個別法は存在していない。

警察の捜査及び犯罪予防目的での、従来的な監視カメラの設置及び利用、

---

(8) 最大判昭和 44 年 12 月 24 日刑集 23 巻 12 号 1625 頁。

(9) 大阪地判平成 6 年 4 月 27 日判時 1515 号 116 頁。

(10) 星周一郎「防犯カメラ・ドライブレコーダー等による撮影の許容性と犯罪捜査・刑事司法における適法性の判断」警察学論集 70 巻 11 号（2017 年）47 頁。

すなわち人の手による記録映像と人物特定についての個別法すら存在しない状況で、AI アルゴリズムを用いた顔認証ソフトウェアを用いたより広範囲かつ正確性の高い監視行動を許容することが許されるのだろうか。確かに、監視カメラによる映像の記録及び当該映像を用いた監視は、目に見えるプライヴァシー侵害を惹起するわけではないし、逮捕、捜索・差押、身体検査・鑑定処分等及び、職務質問や所持品検査などの警察の行動によって侵害される情報：プライヴァシーに比して、侵害の程度が低いと判断される場合もあるのかもしれない[12]。しかしながら、ここで問題とされるべきは侵害される情報の価値だけではなく、情報の扱われ方なのである。なぜなら、従来、必ずしも保護すべき価値の高くないとされた情報であっても、対象者への侵害が積み重なっていくことで結果的に個人のプライヴァシーに対して看過し得ない侵害となることが認識されなければならないからである[13]。これは、情報通信手段の飛躍的な発達によって情報収集手段が発展しビッグデータとよばれる膨大な情報が容易に収集されることになったこと、更に高度に発達したコンピューターにより AI アルゴリズムを用いてビッグデータを処理・解析することで、人間の気づき得なかった相関関係までをも明らかにすることができるようになった現代においては、より一層意識されなければならないことである。この問題について、ドイツにおける個人情報保護の議論が参考になる。

⑾ 我が国における監視カメラに関する法整備及び現行法解釈について、拙稿「刑事手続における AI 実装と個人情報保護に関する諸問題―刑事捜査・訴追機関の情報収集・処理に関するものを中心に」北九州市立大学法政論集 47 巻 1/2 号（2019 年）90-92 頁参照。

⑿ その意味で、監視カメラを用いた人の手（目）による「監視だけを行う」のであれば、個人情報保護の一般的規定と人権保障に配慮した解釈運用でこれを最低限適切に統制することができる可能性はある。

⒀ 山本龍彦『プライバシーの権利を考える』（信山社、2017 年）48 頁以下参照。

２．ドイツにおける個人情報保護と顔認証技術の統制に関する議論

(1) ドイツにおける個人情報保護の基本的な考え

ドイツにおける個人データの保護にとって法的に重要な意味をもつのは、データと情報を区別しそれ自体では意思決定の根拠になり得ないと考えられてきたデータ自体を保護対象とすべきであるというものである。ドイツ連邦憲法裁判所におけるいわゆる国勢調査判決において、「自動データ処理という条件の下で些細なデータは、最早存在しない」ことが認識された[14]。全てのデータ、情報は個人に専属するのだ、という情報自己決定権の尊重を前提として、個人のプライヴァシー領域への介入のためには比例原則に則った法的根拠を設ける必要があり（法律の留保）、データの利用範囲は当初定めた利用目的に限定される（目的外利用の禁止）ことになる。

(2) 情報自己決定権

個人は「自己の個人データの開示及び使用について、原則として自ら決定する権限」を有し、「いかなる者が、自己に関して何を知り、何を利用するかということを、各個人が広範囲に認識し、かつこれを自ら決定する」ことが認められている（情報自己決定権：基本法 2 条 1 項、1 条 1 項、欧州基本権憲章 8 条）。また、データ取得の目的が何かということ、取得されたデータがいかなる結合可能性及び利用可能性を有しているのかが明らかになって初めて、情報自己決定権の制限がどこまで許容されるのかがわかるとされる[15]。

情報自己決定権は、他者との関係において無制限に認められるわけではない。個人には、自らに関するデータ、情報に関する権限が専属するのではあるが、個人の生活が社会共同体において他者との関係を前提とするも

---

⑭ BVerfGE 65,1.

⑮ 小山・前掲註(5)・7 頁

のである以上、個人に認められる情報自己決定権は公益による制限を甘受しなければならない。以上のことから、情報自己決定権とは、実質的に「優越的な公益によって要求されない限りにおいて、いつ、いかなる範囲内で個人の生活状況を明らかにするかを自ら決定する権限」であるといえよう。情報自己決定権の制限には、これに優越する公的な利益の存在が必要とされ、法律による根拠規定が求められる。ここでは、情報の重要性の程度という価値判断が行われることはないばかりか、基本権主体が実際に不利益を被るかどうかも基本権侵害の有無の評価には関係ないとされる。また、物理的強制力の有無も情報自己決定権に対する侵害が行われたか否かの判断に影響することはなく、重要なのは侵害の性質と、侵害のきっかけを作ったのが誰かということである[16]。国家が個人情報に対する介入を行う場合、リスクベースアプローチを前提とした立法による統制が行われる必要がある。これは原則として対象者に強い基本権侵害を与えることになりがちな刑事司法領域においては特に重要であり、刑事捜査・訴追機関が何らかの個人情報を対象として、処理、加工等を行い、これを捜査・訴追に用いる場合には、基本権侵害となる当該捜査・訴追手法が許容されるのかが議論され、許容されると判断された場合にも具体的な統制方法を定めた根拠規定が設けられなければならない。

ドイツ刑事訴訟法 160 条 4 項は、ドイツ連邦法及び州法に適合しない捜査手法を用いることは許されないと規定する。本条の規定からもドイツ警察は刑事訴訟法のみならず個人情報保護に関する一般的規定であるドイツ連邦データ保護法及び EU 法に適合した行動を行うことが求められることになる。近年、EU 域内において国内法のみに依拠して国家的活動を行うことはもはや現実的ではない。EU 加盟国の国内法は、全て EU が示すミニマムスタンダートを満たすものである必要がある[17]。この点について、AI をはじめとする情報技術革新を背景に、EU における個人情報保護関連立法が

⑯　以上、情報自己決定権に関する議論として、玉蟲由樹『人間の尊厳保障の法理―人間の尊厳条項の規範的意義と動態』281 頁以下（尚学社、2013 年）、小山・前掲註(5)・6 頁以下を参照した。

盛んに行われており、EU データ保護一般規則（GDPR）が代表的である[18]。更に、AI の人間中心原則に根ざした円滑な利活用を行うため[19]、ヨーロッパ委員会における AI 白書が示され、本稿において問題とする顔認証技術を用いた警察の捜査活動もこれに沿った運用が求められることになる。

⑶ EU における AI 規制とデータ保護政策

① AI に関する白書

2020 年 2 月 EU 委員会は、データ戦略、セキュリティと責任の問題に関する報告書、AI に関する白書からなるデジタル戦略を発表した[20]。白書で EU 委員会は、高リスクのアプリケーションに対する拘束力のある法的要件を提案、EU 全体で AI 開発者やユーザーが満たすべき AI の要件を示した。これは、AI の特殊性に適応した規制の枠組みを作り、AI が提供する可能性に対する社会の信頼を高めることを目的とする。白書におけるステークホルダーとして、AI の開発者や事業者、AI を利用している企業や個人、または AI に影響を受けている人など、おおよそ AI に関係する全ての人間が想定される。

白書の特徴として、リスクベースアプローチの提案がある。これは、AI 利用者への潜在的な影響は、AI アルゴリズムとそれが使用されている場面に依存するとし、AI には内在的なリスクが存在することを前提とする。具体的な規制方法として、高リスクの AI アプリケーションに対しては法的規制、低リスクの AI アプリケーションに対しては自主的な規制が求め

---

⑰ 拙稿「ヨーロッパ連合における刑事訴訟の共通基準について－被疑者・被告人の防御権保障に関するものを中心に－」広島法学 35 巻 2 号（2011 年）87-122 頁。

⑱ GDPR について、拙稿・前掲註⑪・77 頁以下参照。

⑲ 2019 年 4 月 8 日、EU 委員会によって信頼できる AI のための倫理ガイドライン（AI 原則）が示された。以下のホームページから、EU 加盟国各言語で参照可。https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

⑳ 2020 年 2 月 19 日、EU 委員会は信頼できる AI 利活用の方針を示す、AI 白書を公表した。以下のホームページから参照可。https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf

られる。「高リスク、低リスク」の定義は曖昧であるが、本稿で問題とする顔認証技術を含む生体認証技術の利用は原則高リスクありとされている。

② EU 委員会のモラトリアムの見送り

以上のリスクベースアプローチを用いた効果的な AI 規制の実現のため、EU 委員会は、官民を問わず利用されている顔認証技術を一時的に禁止する措置を検討していた（モラトリアム）。公共空間における民間または公的な主体による顔認証技術の使用は、一定期間（例えば 3 年から 5 年）は禁止し、この技術の影響を評価するための健全な方法論と、可能なリスク管理方法の開発等を行う計画があったが、これは結局のところ見送られた。モラトリアム措置の見送りは、ドイツを含む EU の AI 戦略に大きな影響があるとされている。

③白書に対するドイツ政府の反応

ドイツ連邦政府内では、労働、経済、教育の 3 つの省庁と内務省、法務省が白書の受け入れプロセスに関与している。AI 規制の枠組みのための EU 域内に共通する概念が合意され、保護目標や保護されるべき対象を明確化、透明性やトレーサビリティの確保、最終的な決定プロセスへの人間の関与を必須化するための措置が講じられる予定。自然科学、社会科学など、分野に限定されず、横断的な共通の法的枠組みを作る必要性の認識が表明された[21]。

④顔認証技術の規制方法と問題点

現状の規制方法として個人識別符号を有するデータとそうではないデータとに区別して、前者の保護に重きを置いた規制方法が採られるのが一般的である。

---

[21] ドイツ政府の AI 白書対応について、ドイツ法務省ホームページを参照した。https://www.bmjv.de/SharedDocs/Artikel/DE/2020/062920_BReg_Weissbuch_KI.html

これには、一定の効果があると思われるが、AI 関係技術の急速な発展により、様々な問題点が浮上している。例えば、個人識別符号を有さないデータが大量に蓄積され、AI を用いた解析を行うことで、個人の再特定が可能となるとの指摘がされており、個人識別符号の有無に着目した発想が古くなっているとの指摘がある。以上に関連して、顔認証技術に特化した法規制の必要性が認識されている。EU レヴェルでは、生体データ全般に対する法規制が明文化されているものの、顔認証に特化した明文の規定が存在しない。これは、ドイツ国内においても同様であり、顔認証に特化した規定を創設するべくドイツ連邦データ保護法及び、刑事訴訟法の規定を改正する必要があるとの指摘がされている[22]。

以上の情報自己決定権及び、EU におけるデータ保護に関する最近の動向を踏まえ、以下では、ドイツの裁判所で初めて問題とされた警察による大規模な顔認証システムを用いた捜査活動について概観し、争われた法的問題について検討していく。

⑷ ドイツ刑事手続における顔認証技術

①ハンブルク G20 サミット警備の事例[23]

問題となった事件は、これまでドイツ警察が行った顔認証技術を用いた捜査活動で最も大規模なものである。2017 年ハンブルクで行われた G20 サミットの警備に際して、15157 件の映像データ及び 16480 件の写真データ、計 17 テラバイトに及ぶデータがハンブルク警察によって取得された（第一段階）。これらは、警察が独自に撮影・録画したもの、警察に提供された私的録画、G20 サミット前後の 5 日間に 8 つの異なる都市高速鉄道（S-Bahn）の駅で撮影されたすべての監視カメラの映像から成る。警察や個人の録音は、データベースに入力する前にスクリーニングされた

⑵ 例えば、*Heckmann*, Editorial16/2020- Gesichtserkennung muss streng reguliert warden, jurisPR-ITR 16/2020 Anm. 1.

⑵ 本事例の検討に際して、*Mysegades*, NVwZ 2020, 852ff. が紹介する事実の概要、ハンブルク行政裁判所の示す問題点を参照した。

が、S-Bahn の監視カメラの映像はフィルターをかけずに入力された。この基本ファイルをもとに、警察は民間が開発した顔認証ソフトを使って照合元となるデータベースを作成した（第二段階）。これは、取得された写真・映像に含まれる顔特徴量データを抽出し作成されたものである。警察は、抽出された顔特徴量データの正確な総数を認識していないが、作成された照合元データベースに含まれる顔特徴量データは 10 万件を超えるだろうと述べている。この照合元となるデータベースを用いて、警察は、捜査手続において、被疑者の顔画像を個別に検索した（第三段階）[24]。534 件の具体的な顔画像の検索が行われ、2018 年 9 月までに 32 件の捜査の端緒となる結果が得られ、最終的に 9 件で捜査手続が開始された。ハンブルクデータ保護監督官は、これらの警察の顔認証技術の利用を禁止する命令を出したが、ハンブルク警察はこの命令に対して異議申立てを行った。結果、ハンブルク行政裁判所は、禁止命令が違法であると判断し、ハンブルク警察の捜査活動を適法であるとした。

②ハンブルク行政裁判所の判断の概要

ハンブルク行政裁判所の判断は 3 つの前提に基づいている。まず、データ保護監督官の削除命令は、認められた法的権限から逸脱しているとする。更に、ドイツ連邦データ保護法 48 条 1 項が、本件における警察の行動全体を根拠付けるために十分であるとし、当該行動は、本条にいう「絶対的に必要」という要件を満たしているとする。

ハンブルク行政裁判所は、ハンブルクデータ保護監督官が「具体的」なデータ保護違反を立証できていないことを問題としており、法律違反を指摘するのみならず、データの具体的な不正利用、そこから生じた損害を摘示していないとする。そして、本件における警察の行動を先に示した三段階の個別のものとは考えず、共通した目的のために行われる総合的行動、統合されたプロセスであると見ている。

---

[24] 本件における一連の個人情報の収集及び処理についての三段階におけるステップに分類することにについて、*Mysegades* (Fn.23), 852. を参照。

更に、ハンブルクデータ保護監督官には、連邦憲法裁判所が求める情報自己決定権に対する侵害を肯定するに足る規律の密度がドイツ連邦データ保護法 48 条 1 項に備わっているかを判断することはできないとし、憲法的な検討を行う権限がないとしている。更に、ドイツ連邦データ保護法 48 条は、ドイツ国内における生体データの処理に関する基準として設けられたのであるから、データ保護監督官もこのような立法者意思に従う必要があるとしている。そして、本件における一連の警察の行動を達するためには、顔認証システムの利用が絶対的に必要であったと結論づけている。

③ハンブルク行政裁判所の判断の法的な問題点

データ保護に関する憲法上の基準と比較すると、今回のハンブルク行政裁判所の判断に対していくつかの疑義が指摘される。まず、データ保護監督官には警察の行動につき憲法的な問題に関する審査権限がないとしているがこれは誤りである。更に、ハンブルク行政裁判所が訴訟の対象となっている顔認証の実際上の効果と危険性を過小評価していることも問題であるとされる。

第一の問題について、データ保護監督官がデータ保護に関する個別法についてのみ審査権限を有するという理解は、EU 法的観点からも疑問がある。

第二の問題について、EU 裁判所と連邦憲法裁判所は、情報主体の自己決定を無視した個人データの処理は、情報主体の基本的権利の侵害にあたるとしている（欧州基本権憲章 8 条）。実際に不利益が生ずるか否かは、情報自己決定権に対する侵害の有無の評価には関係しない。これは、データベースを用いた照合を行う際に、不一致であった比較対象者に対しても基本権侵害が肯定されることを意味し、この場合でも法的根拠が必要とされる。具体性を欠く一般規定では法的根拠たり得ない場合が多く存在し、特に警察法における警察の一般的な行動原則、指針などを根拠として、個人の情報自己決定権に対する侵害を肯定することはできない。この点について、EU 裁判所及び連邦憲法裁判所の判断によれば、問題とされる規定が、措置の範囲と適用に関する明確かつ性格な規則を設けており、かつ濫用の

リスクから自らのデータを効果的に保護することを可能にする十分な保護手段を備えている場合にはじめて、情報自己決定権を制限する法的根拠たり得るとしている[25]。

本質性理論に基づけば、立法者によって基本権侵害が明確に統制されなければならず、統制の対象となる行動の基本権に対する侵害が強ければ強いほど、当該行動の根拠となる規定はより正確かつ具体的であることが求められる。行政機関は、具体性を欠く一般権限に基づいて個人に対して強力な侵害を伴う行動を行うことはできないし、行政機関自身で事前に法的根拠が備わっているかを判断しなければならないとされる。

④法的根拠の欠如

ドイツ連邦データ保護法 48 条は、顔認証技術を用いた捜査の根拠規定としては不十分であり、ハンブルク行政裁判所の判断には問題がある。というのは、国家の監視措置が秘密裏に行われ、関係のない第三者を対象とする場合において、連邦憲法裁判所は、情報自己決定に関する基本権への重大な侵害を伴う規範の確定性及び正確性を厳格に要求しているからである。監視カメラの記録映像に顔認証ソフトウェアを用いることで、ビデオ監視による基本権に対する侵害はより深刻なものとなることが予想されるため、このような運用をデータ保護法の一般条項によって正当化することは困難である。以上に関して、連邦憲法裁判所は自動車ナンバー自動読み取り装置（日本での N システムに相当）をめぐる判決において、データ利用と監視に関する手続規定を含む個別の根拠規定が設けられることを求めた。また、本判決では、公共空間において取得された画像の利用は、侵害の実体的な重みを低減させるが、一方で情報収集手段の秘匿性、広範囲を対象としていることからくる監視されているという感覚は、侵害の実体的な重みを高めるとしている[26]。

警察が実際に顔認証システムを不正利用したか否かは、本件において重要

---

[25] *Mysegades* Fn (23), 853.

ではない。先に見たように、EU 加盟国は、リスクベースアプローチを採用して、データ保護政策、立法、法解釈を行う旨明言している。それ故、欧州基本権憲章 8 条及び情報自己決定権の中核要素は、データ濫用、登録、データベース化の危険から個人を保護することにあると理解されることになる。

ハンブルク行政裁判所は、警察が顔認証システムを使用するために行った 3 つのステップを、統合された個人情報に対する処理とみなす。確かに、ドイツ連邦データ保護法 46 条 2 項によれば、処理とは「収集、記録、整理、ファイリング、保管、適応、変更、検索、相談、使用、送信による開示、普及、その他利用可能な状態にすること、整列、結合、制限、消去または破壊など、自動化されているか否かにかかわらず、個人データに対して行われるあらゆる操作または一連の操作を意味する」とされる。ただし、情報自己決定権の理解に際して、単純な個人情報に対する様々な侵害が積み重なっていくことで成り立っているのが国家によるデータ処理の典型であることが前提とされなければならない。

すなわち、全てのデータの収集と比較は、原則として、各々が基本権の侵害を構成すると理解しなければならない。したがって、本件におけるような一連の手続の中の個々のステップは、技術的、組織的、時間的にステップが互いに明確に区別できる場合には特に、個別に基本権への侵害の程度が考慮され、それぞれ法的根拠に基づくものでなければならない。具体的には、第 1 段階（基本ファイルの作成）と第 2 段階（参照用データベースの作成）であっても、十分に正確な法的根拠とそれに対応する手続に基づいて実施されなければならないし、第三段階の措置が許容されるか否かの判断に至っては第一、第二段階における個人に対する侵害をも考慮して決定されなければならないだろう。

以上の判断に際して特に重要となるのはデータの利用目的の検討と目的

⑵⑹ BVerfGE 150, 244 = NJW 2019, 827

本判決に関する日本語文献として、實原隆志「判例研究 自動車ナンバー認証システムの合憲性：ドイツ連邦憲法裁判所・第二次「N システム」決定［連邦憲法裁判所 2018.12.18 決定］」福岡大學法學論叢 65 巻 1 号 175-194 頁（2020 年）。

外利用の禁止原則である。本件における第三段階における措置は、刑事捜査・訴追目的という個人の基本権に対する侵害度合いが特に強いものであり、先に示した連邦憲法裁判所の基準に基づけば、その根拠規定に求められる明確性、正確性は特に高いものとなることが予想される。特に、ドイツ連邦データ保護法48条にいうセンシティブデータの取扱いが問題となる場合、当局は、目的を正確に定義し、追求する具体的な警察の任務に照らし合わせ比例性を担保しなければならない。しかしながら、本件におけるように、データ保護の一般規定であるドイツ連邦データ保護法の規定を根拠に、データベース構築を目的としていると理解した上で第一段階における極めて広範囲かつ対象者の制限を行わない個人情報の収集を正当化すること、これを解析・処理しデータベースを構築した後、個人に対する侵害の度合いが最も強いと考えられる警察による捜査・訴追への利用を許容することは、個人の基本権侵害を肯定するに足る程度に規律された根拠規定に基づくものであるとはいいがたいように思われる。

本件における、ハンブルク行政裁判所の判断は、警察による明確な根拠規定に基づかない顔認証技術の利用による影響の軽重を読み誤っている。本判決では、警察による顔認証技術の濫用についての現実的な危険性を否定しているが、本件において問題とされた顔認証データベースの利用履歴などが十分に記録されていないことも明らかとなっている。外部からの不正アクセスの可能性も否定されているが、同システムの利用履歴が十分に記録されていない以上、この問題を検証するのは事実上困難である。更に、本件におけるような明確な根拠規定に基づかない警察の顔認証技術の利用が肯定されるという先例ができてしまえば、不特定多数人に対する行動の萎縮効果など、望ましくない結果を招来させかねない。

以上のような観点からも、本件におけるような最終的に刑事捜査・訴追目的で行われるセンシティブな個人情報の収集・処理・管理・事後的利用は、これを総合的に統制できるよう具体的な刑事訴訟法の規定を持って根拠付けられなければならないだろう。

この事件ののち、EUは公共空間での顔認証技術を用いた捜査を原則禁

止した。これを受けてEU加盟国は法整備などの対応を迫られることになるため、ドイツにおける対応が注目される[27]。

３．わが国における顔認証技術を用いた捜査手法統制のあり方に関する若干の考察

⑴　実務における従来の理解

わが国の実務において、写真撮影、映像記録を行う捜査手法に関する刑事訴訟法上の規定は存在せず、判例法理に従い、何人も、その承諾なしに、「みだりに」その容貌等を撮影されない自由を有していることを前提とし、現行犯ないし準現行犯状況の存在、証拠保全の必要性および緊急性の存在、撮影が一般的に許容される限度を超えない相当な方法をもって行われることを要件として、個別の写真撮影の許容性が判断される。近年では、監視カメラ等の設置数が劇的に増加しており、継続的な映像撮影に関する問題が顕在化しているが、わが国の刑事訴訟法及び警察法、個人情報保護関連法規の解釈によれば、民間からの映像提供及び監視カメラの設置、映像の取得、取得映像の処理・保存、事後的利用について強制処分性が認められるには至っていないと考えるのが一般的な理解であろう[28]。以上の点について、東京高裁Ｎシステム判決[29]で示された基準が参考となる。本判決は、Ｎシステムが記録するのは個人の容ぼうではなくナンバープレートに限られるという技術的な前提をとりつつ、個人の情報を収集し管理することは、犯罪予防、捜査目的から正当なものであるとする。更に、ナンバープレートの性質及び情報収集の場所が公道上であることから、取得される個人情報は公権力に対して秘匿されるべき情報ではないとされる。そして、収集、管理の方法は、走行中に自動的にカメラで撮影し、データをコンピュータで処理することによって行われるため、有形力の行使に当たらず、国民に

⑵⑺　EUの顔認証技術利用原則禁止について、朝日新聞デジタル版2021年４月22日配信。https://www.asahi.com/articles/ASP4Q3QHNP4QULFA002.html

⑵⑻　星・前掲註⑽・54頁。

⑵⑼　東京高判平21年１月29日〔LEX【文献番号】２５４５０９８６〕

特別の負担を負わせるものではなく、取得されたデータは、警察の目的達成に必要な短期間保存されることはあるが消去される前提があること、目的外に使用されることはないというのであるから、公権力がみだりに国民の情報を収集、管理するということはできないとする。ここから窺われるのは、まず我が国の実務における個人情報保護の方法として、取得される場所の公共性、情報の性質などの要素が考慮され、ドイツとは異なり保護の必要性に濃淡がつけられることを前提とすることである。そして、保護されるべき個人情報であったとしても、公益の確保と個人情報保護の要請が衝突した場合、前者が優先される傾向にあるといえる。警察といえども「みだりに」個人を撮影・記録することは許されないが、警察の行動を統制する個別法によらずとも[30]、公共性の高い場所でありかつ強制力を伴わなければ、その目的達成の範囲で行われる限り「みだりに」個人情報を取得したのではないとするのが我が国における従来の判例法理であるように思われる。更に、警察による取得情報の保存、データベース形式による事後的運用について、法的統制によらずとも目的外利用、濫用の虞がないと判断している点も注意を要する。

⑵ 刑事手続における個人情報保護に関する理解の変化：契機としてのGPS捜査判決[31]？

最高裁昭和51年決定は[32]、「強制処分とは、有形力の行使を伴う手段を意味するものではなく、個人の意思を制圧し、身体、住居、財産等に制約を加えて強制的に捜査目的を実現する行為など、特別の根拠規定がなければ許容することが相当でない手段を意味する」とする。「個人の意思を制圧」することの意義をめぐっては争いがあったが、GPS捜査判決において、

⑶⓪ この点につき、東京高裁Nシステム判決は、「我が国においては、警察は、警察法２条１項の規定により、強制力を伴わない限り犯罪捜査に必要な諸活動を行うことが許されていると解される」とする。

⑶① 最大判平成29年3月15日刑集71巻3号13頁。

⑶② 最決昭和51年3月16日刑集30巻2号187頁。

GPS 捜査が「合理的に推認される個人の意思に反して」私的領域に侵入するものであるとしたうえで、これが「個人の意思を制圧」するものであると判断されたことから、「個人の意思を制圧する」とは、「個人の意思に反する」ことを意味するものであることが示された。この理解に従えば、強制処分法定主義は、個人に意思に反してその「権利・利益」を侵害する捜査機関の行動を強制処分として捉えることを意味することになる。「権利・利益」の内容が問題となるが、GPS 捜査が「個人の行動を継続的、網羅的に把握することを必然的に伴うから、個人のプライバシーを侵害しうるものであり、また、そのような侵害を可能とする機器を個人の所持品に密かに装着することによって行う点において、公道上の所在を肉眼で把握したりカメラで撮影するような手法とは異なり、公権力による私的領域への侵入を伴うものというべきである」としたことをどう捉えるべきか。「個人の行動を継続的、網羅的に把握することを必然的に伴う」という実質的側面に着目する場合、従来は公道上において認められなかったプライバシー侵害の可能性を認め、GPS 捜査が「個人の意思を制圧して憲法の保障する重要な法的利益を侵害する」としその強制処分性を認めたこと見ることもできる。そうだとすれば、強制処分性判断にとって重要となる「権利・利益」の解釈に際して、プライバシー権の根拠となる憲法 13 条を媒介として、情報プライバシーに関する要素を取り入れることが可能となるかもしれないし、GPS 判決の射程を最も広く捉えた場合ドイツにおける情報自己決定権的な要素を取り入れることも可能となる。この場合、最高裁において「GPS 捜査が「『検証』では捉えきれない性質を有する」ことが示されたことに鑑み、警察の新たな捜査手法、とりわけ情報そのものはもちろんその取り扱いに関する権利・利益に対する侵害を伴う捜査手法統制を行う際にも、立法的措置が行われる必要があると考えることもできる[33]。

---

(33) もっとも、このような理解は、GPS 捜査判決の射程を最も広く捉えたものである。GPS 発信機の装着を重視した判決であるとすれば、GPS 捜査の違法性は私的領域に対する意思に反する侵入を意味するものにとどまり、判決の射程は個人の情報プライバシーにまでは及ばないということになる。以上に関して、小山・前掲註(5)・14－15 頁。

⑶　監視カメラ設置及び顔認証技術を用いた捜査手法統制に必要な規律要素

①情報プライバシーに対する侵害を伴う捜査手法に対する立法的統制の必要性

官民を問わず監視カメラの設置による映像取得と、警察による取得映像の AI による顔認証技術が行われる場合、これが個人情報に対して何らかの侵害を与えることに疑いはない。しかしながら、従来、警察によって犯罪予防、捜査目的で個人の容ぼうを映像に記録することは、警察法 2 条 1 項により正当化され「みだりに」行われているのではないとされてきたように思われる。しかしながら、先に検討した GPS 判決によれば、強制力を伴わない公道上の情報プライバシーに対する侵害についても強制処分性が認められる可能性があり、個別法による立法的統制が行われることが望ましいとされた。情報プライバシーの理解の仕方について、我が国における自己情報コントロール権的なものか、さらに進んでドイツにおける自己情報決定権的なものかで個別事案における結論が分かれることも想定されるが[34]、いずれにしても我が国の刑事手続きにおける個人情報保護のあり方を一歩前進させるものであると期待したい。

②顔認証技術を用いた捜査手法の具体的な統制方法

ⅰ．総論

現在の技術的水準からすれば、監視カメラと顔認証技術による個人特定

---

[34]　自己情報コントロール権は、個人情報の中でも人格的自律に関わるものに法的保護の必要性を認める。一方、情報自己決定権は情報自体の価値判断に基づかず、情報の取り扱い方を重要視する。DNA 型鑑定をめぐる問題について、いずれの考えに基づいた場合でも法的保護の必要性を肯定しうるが、位置情報や公道上における容ぼうの撮影等、従来単純な個人情報として理解されるものについて、保護の必要性に関する結論がわかれることも想定される。AI をはじめとする高度な情報技術を用いた捜査手法を効果的に統制するためには、情報自己決定権的な発想が望ましいように思われる。

を繰り返し行うことにより、容易に個人の位置情報を含めた個人情報を取得することができる。更に、一旦個人識別符号である顔特徴量データが取得されデータベース化されれば、継続的に個人の行動を追跡し行動パターンを把握、そこから性格、嗜好などを推定することすら困難なことではなくなっている。監視カメラの設置及び取得映像に対する顔認証技術を用いることで行われる個人特定はもちろん、これを他の先端的技術と組み合わせることにより、対象者に対するプライバシー侵害はより深刻なものとなる。以上のことからも、目に見える強制力を伴わない手法を用いるものであったとしても、警察等国家的機関によってこのような技術が用いられる場合、当該手法によって個人に与えうる侵害の程度を想定し、かつこれを用いる場合でも可能な限り侵害の程度を低く抑えることができるように個別法による統制が必要となってくる。

どのような規制方法が用いられるべきかが問われるが、情報の取得段階、取得情報の処理・解析段階、処理・解析された情報のデータベースへの登録段階、データベースに登録された情報の事後的利用段階に分類した議論が行われなければならない。そして、各段階において取得、処理・解析、保存、事後的利用の範囲と適用に関する明確かつ正確な規定を設けており、かつ濫用のリスクから対象者のデータを効果的に保護することを可能にする措置が講じられることが必要となる[35]。

---

(35) この点について、例えば、IoT 推進コンソーシアム、総務省、経済産業省による「カメラ画像利活用ガイドブック」がある。民間利用の範囲であれば、ここで示されるガイドラインに従った利用を行うことで、一定程度適正な運用を期待できる。また、技術発展のスピードを考えた場合、議会法による統制ではなくガイドラインを用いることで柔軟な運用を行い、技術の更なる発展を阻害せず、経済的メリットを享受できるという利点もあるように思われる。

しかしながら、対象者にとって最も高リスクとなる類型の一つである警察利用については、行政警察、司法警察双方の活動領域において、以下で検討する内容を踏まえた個別法による統制が行われる必要がある。

ⅱ．情報取得段階

まず、監視カメラ設置（情報収集）主体が民間、警察等国家機関であるのかが明確に区別されなければならない。民間設置カメラの許容条件について、設置主体（事業者名等）、設置目的（防犯か商用か）、設置期間、設置場所、取得映像の再利用可能性の明示（AI 等による解析の有無）、取得映像の保管方法、保管期間、問い合わせ先の明示、対象者による異議申し立て等についての告知を行なった上で、対象となる個人の同意が推定的にでも担保されるような配慮を行うべきである。監視カメラ設置数から考えれば、警察利用の際に民間設置カメラからの映像提供を受ける回数が相当数にのぼることが予想されるが、現状ほとんどの場合、任意処分として捜査事項照会書の提示で映像の提供を受けていると考えられる。この点につき、現行法による統制を考えた場合でも、任意処分によるのではなく、携帯電話位置情報等と同じく、原則として検証令状による司法的チェックが入ることが最低限必要となる。情報取得目的の明確化と目的外利用を原則禁止すべきであることが個人情報保護の本来あるべき姿のであることを考えると、将来的に個別法が設けられる際には、情報取得の段階で顔認証技術の利用目的であることが明示されなければならない。将来のデータベース登録を行う場合には、別の根拠規定に基づく再度の裁判所による司法審査が必要となる。

警察によって、監視カメラが設置される場合、それが人の目によるものに限定され、映像の記録、保存が行われないのであれば、プライバシーに対する影響はさほど大きくないと判断できるのかもしれない。しかしながら、現状カメラの設置が行われる場合、映像の記録が行われないことは最早想定できず、映像が顔認証技術を用いて解析・処理されることを前提とする方が現実的である。監視カメラの設置につき、取得映像の処理、解析、更には保存、事後的利用まで見据えた、警察の監視、追跡に関する一連のプロセスの統制を可能とする立法が行われることが必要となる。先に述べたように、犯罪予防目的、捜査目的では統制方法が異なるのが我が国の現行法の特色ではあるが、犯罪予防のために取得された映像が期せずして将

来の捜査に用いられることは多々あることであろう。そのため、犯罪予防目的での監視カメラ設置及び運用についての行政法的性格を有する個別法が設けられる場合には、捜査目的で行われる設置に関する刑事訴訟法の個別規定との連続性が考慮された立法が行われなければならない。様々な方法が考えられるが、捜査目的での再利用には、別個の司法審査が必要であることを旨としつつ、捜査利用の際に取得映像のスクリーニング措置が行われることは必要となろう。犯罪予防目的で監視カメラを設置し映像を取得する場合でも、設置場所や期間について、基本的には民間設置の場合と同様に、対象者の同意が担保される枠組みづくりが必要となる。また、一定の期間ごとに設置及び運用の妥当性をモニタリングできる制度設計が重要となる。また、捜査目的の場合秘匿してカメラ設置を行うことが必要となる場面が想定されるが、対象犯罪の限定、撮影対象者が無関係のものに広がりすぎないよう限定的な運用が必要となる。

ⅲ．情報処理、解析段階

民間機関の場合、対象者の同意無く、重要な個人識別符号である顔特徴料データを含む映像を保存すること、これを顔認証ソフトウェアを通じて処理・解析、データベースすることは禁止されるべきである。一方で、警察が犯罪予防活動として、顔認証ソフトウェアを用いて危険人物等の洗い出しを行うような場合、犯罪予防目的と対象となる個人の侵害される基本権とが比例関係にあることが求められる。これを満たすためには、まず対象者、場所の限定等が行われなければならない。犯罪予防目的という未だに具体的な法益侵害等が生じていない状態で行われる不特定多数人を対象とする警察の監視行動を正当化するためには、対象者が過去に重大犯罪をおこなっている場合、テロ犯罪等に代表される重大な犯罪発生の蓋然性が認められる場所などに設置､運用場所が限定される必要がある（大規模駅、空港等)。それでも、可能な限り広範囲の映像を入手して膨大な数に上ることが予想される危険人物リストとの照合を行うという監視カメラと顔認証技術を用いた活動の性質に鑑みると、実際の規制には困難を伴うことが

予想される。この問題は、犯罪捜査目的での利用の際により顕著となろう。まず、顔認証技術の利用は誤認証を起こしやすい問題が指摘されており[36]、アルゴリズムの誤作動により捜査対象とされた個人には、深刻な侵害を与えてしまう結果となる。これは、犯罪の軽重を基準とした対象犯罪の明確化が行われる等の措置が講じられた場合でも同様であり、顔認証技術を過度に信頼することなく、人間の手（目）による最終的判断が行われなければならない[37]。更に、従来の捜査であれば対象者の限定が行われるが、顔認証技術を用いた捜査手法はその性質上、無関係な不特定多数人に対して看過し得ないプライバシー侵害を与えうる。これを避けるために、無関係の者を除外する作業が行われなければならないが、人的なモニタリング、スクリーニングは現実的ではなく、ソフトウェア処理により対象者以外の個人識別符号の即時廃棄等の措置が講じられる必要性がある。

ⅳ．保存、事後的利用：データベース運用段階

民間機関による対象者の同意を得ない顔特徴量データの保存・データベース化は許容されてはならない。警察による場合でも、個人データの保存、事後的利用は対象者により深刻かつ継続的な侵害を与える可能性が高く、現在の捜査に用いるのと比してより厳格な統制が行われる必要がある。具体的には、対象犯罪の限定、データの保存期間、消去条件、特に消去義務が明確に規定された個別法が設けられる必要がある[38]。対象犯罪は、いわゆる重大犯罪に限定されることになるだろうし、データの保存期間についてもEU、ドイツ法などを参考にした場合、一定期間経過後に当該デー

⑶⑹　例えば、ドイツにおいてマスクを正確に装着した場合、誤認証を起こしやすいことが報告されている。Vgl. *Heckmann* Fn(22), S.1.

⑶⑺　例えば、GDPR 22条よれば、重要な事項の最終判断はアルゴリズムによるプロファイリング結果にのみ基づいて行われてはならないとする。

⑶⑻　この点について、DNA型データベースに対する統制方法が参考となる。拙稿「無罪判決確定者による警察DNA型データベースに登録された個人情報の抹消請求について」北九州市立大学法政論集47巻3/4号（2020年）95頁以下参照。

タを継続して保存しても良いか否かを判断する必要がある。そして、捜査途上で得られたデータを無制限、無条件に保存することは許されず、捜査対象に被疑事実の蓋然性が認められない場合、後々の裁判で無罪が確定した場合などは、即座に当該データのデータベースからの消去が求められることになろう。

おわりに

従来、刑事手続において単純な個人情報を対象とする捜査は幅広くかつ寛容に認められてきた。しかしながら、今日のようにAIの加速度的な発展を見た社会において、個人情報に認められる価値を事前に見積もって法的保護に値すべきか否かを判断する方法では、時として対象者に当初予期し得なかった過度な侵害を与えることになる。対象となる個人情報の価値判断を通じて刑事手続において保護されるべき権利・利益であるかを判断するのではなく、いかなる方法を用いて情報が取り扱われているのかという視点で法的な統制の必要性及び具体的方法を考えなければならない。

Reprinted from

KITAKYUSHU SHIRITSU DAIGAKU HOU-SEI RONSHU

Journal of Law and Political Science. Vol. XLIX No. 1 / 2

October 2021

Regulierungsmaßnahme zur polizeilichen Gesichtserkennung

MIZUNO Yoichi