北九州市立大学法政論集第47巻第1・2合併号（2019年12月）抜刷

論　　説

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――

水　野　陽　一

北九州市立大学法政論集第47巻第1・2合併号（2019年12月）

論　　説

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――

水　野　陽　一*

はじめに

人工知能（AI:artifical intelligence）の社会における実装は、既に現実のものとなっている。AIは、社会を大きく変革させる可能性を持っているものではあるが、我々は同時にAIのもたらす危険性を十分に認識しなければならない。AIは、良くも悪くも我々人間に対して、大きな影響を持ちうる存在になっているのである。いわゆるビッグデータの解析とAIは、これを経済活動に活用する企業等はもちろん国家機関にも、一般市民の個人情報の収集、解析・処理し、これを保存し、様々な場面でこれを活用することを容易にする。とりわけAIによる個人に対するプロファイリングが問題となる。プロファイリングとは、収集された情報、特に個人情

* 本学法学部准教授

報を AI によって解析し、特定の個人に関する性質を分析、予見するものである。プロファイリングの内容は多岐にわたり、個人の労働能力、経済状況、健康状態、趣味嗜好、関心、信用性、行動、滞在場所等の現況、将来における状況を一定の確率で特定できる。AI による個人の性質の特定は、もちろん絶対のものとはなり得ないが、ビッグデータに基づいたプロファイリングによって、従来人間の能力では発見できなかった事象間の相関関係を確認、発見することができる場合もあることが指摘されている。

既述の通り、AI による高精度のプロファイリングを行うためには、大量のデータを効率よく収集し、これを保存、解析する必要があり、これは刑事手続においても同様である。通常の刑事事件においても迅速な対応が求められるが、とりわけいわゆる「テロとの戦い」の文脈では、刑事捜査・訴追機関がいかに素早くかつ効率よく犯罪予防及び、捜査・訴追に関する情報を収集するかが重要となる。しかしながら、その一方で世界的に個人情報保護の重要性が認識されており、テロ対策と個人情報保護とをいかにバランス良く両立させるかが問われる。

近年の世界レヴェルにおける個人情報保護法制の中で、とりわけ重要となるのは EU データ保護一般規則（General Data Protection Regulation：以下、GDPR とする）(1) であろう。本規則は、EU 域内における個人情報保護法制の調和及び共通した個人情報保護基準の定立を図るために EU 委員会によって策定され、2016 年 4 月に制定、2018 年 5 月 25 日に施行された。これにより EU 加盟国は、GDPR に則った個人情報保護法制を整備することが求められている。更に、GDPR は、その名が示すとおり一般的な個人情報の移転、処理に関わる基準を定めたものであり、刑事司法領域においては、GDPR に加えて EU 刑事司法データ保護指令 (2) の存在が重要

(1) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

(2) Directive (EU) 2016/680 of the European Parliament and of the Council of 27

となる。

先述の通り GDPR は、EU が策定した個人情報保護に関する基準を定めたものではあるが、同規則の対象は、EU 加盟国内及び加盟国間における個人情報の移転、処理のみならず、EU 域内から域外へ個人情報が移転される場合に EU 域外の事業者等をも対象としている点に注意しなければならない。EU 域内の個人情報を取り扱う場合には、わが国も GDPR の適用対象となる。

Ⅰ　EU 刑事司法領域における個人情報保護
――ドイツにおける議論を参考に

1　EU 法レヴェルにおける個人情報保護法制

(1)　総論

ヨーロッパ基本権憲章 7 条は、私生活及びコミュニケーションの尊重に関する権利について、8 条は個人情報保護に関する権利について規定することから、EU 域内において私人の個人情報保護の要請が基本権に根ざしたものとして位置づけていることがわかる(3)。上記、基本権レヴェルでの要請をより詳細に具体化したものが GDPR ということになろう。

GDPR は、EU 域内における個人情報保護に関して、最低限遵守されるべきで基準を示すものであるから、EU 加盟国はこれを満たした制度的保障、及び権利保障のために国内法整備を行うことが求められることになる（GDPR 6 条 2 項）(4)。ドイツは GDPR 対応のため、2017 年 6 月、ドイツ

April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

(3)　更に、ヨーロッパ連合の機能に関する条約16 条においても、再度個人情報保護について言及されている。

(4)　GDPRの日本語訳について、個人情報保護委員会作成の仮訳を参照した。

連邦データ保護法（Datenschutz-Grundverordnung）を全面的に改正している(5)。

更に、GDPR は、個人情報の EU 域外及び他の国際機関への移転が行われる場合、EU 委員会が移転先における個人情報保護基準が十分であるかを審査し、これが十分な水準に達していることを求める（GDPR 45 条）。いわゆる十分性認定が行われていない場合でも、個人情報の移転が認められる場合もあるが（GDPR 46 条、49 条）、厳格な手続的要件を課されることになるため、我が国を含め EU 域内の個人情報移転に関係する可能性のある各国はその対応に追われている実情がある。

GDPR 2 条 2 項 d は、個人情報が「公共の安全への脅威からの保護及びその脅威の防止を含め、所管官庁によって犯罪行為の防止、捜査、検知若しくは訴追又は刑罰の執行のために」取り扱われる場合には、GDPR の適用対象外となるとしている。本条の規定によれば、警察、検察等の刑事捜査・訴追機関が個人情報を取り扱う場合、基本的には GDPR の適用対象外となるが、取り扱う情報が民間機関から提供されたものである場合、当該情報の取得行為、取得情報それ自体は当然 GDPR の適用対象となる（GDPR 6 条 2 項）。

(2) GDPR が定める個人情報取り扱いに関する規制

GDPR 6 条は、個人情報取り扱いの適法性について言及している。例えば、監視カメラ等による映像記録及び当該情報の取り扱いについて重要となるのは、GDPR 6 条 1 項 f であり、ここでは管理者及び第三者が正当な

---

https://www.ppc.go.jp/files/pdf/GDPR-provisions-ja.pdf から取得。（最終アクセス日2019 年10 月 9 日）

(5) GDPR は、EU 規則（Regulation, Verordnung）であるため、その適用に際して EU 加盟国における国内法制化は必要とされず、EU 加盟国自体はもちろん、その国内企業、自然人等に対して直接適用される。
Vgl.*Oppermann / Classen / Nettesheim*, Europarecht, 4.Aufl. 2010, §10 Rn.82ff.
しかしながら、GDPR は多くの場面で具体的運用に関して EU 加盟国における国内法整備を求めている。

利益の確保を目的とした場合にのみ個人情報の取り扱いが正当化される旨規定されている。正当な利益の存在がいかなる場合に認められるかが問われるが、単なる威嚇効果を狙ってカメラ設置をする等、抽象的危険に対する危惧ではこれを正当化することは認められず、少なくとも具体的危険の防止を目的としたものであることが求められる。例えば、以前に何らかの事件が発生した場所であること、またセルフサービス店、宝石店では定型的危険の存在が認められやすい。更に、犯罪防止及び民事上の損害賠償請求事由に当たる事情の防止のためのカメラ設置にも、正当な利益の存在が認められることになるだろう。以上に関して、カメラ設置の必要性についてもこれが十分に考慮されなければならない。例えば、カメラ設置によって十分にその目的が達成されるのか、当該目的達成のために代替手段を用いることができないのかが問われることになる。

上記に加えて、カメラ設置に関する透明性の確保が必要となる。例えば、当該カメラ管理者の氏名・連絡先、データ保護監督者の連絡先、カメラ設置の正当化根拠、カメラから取得される個人情報の保存先、データ移転先の情報の公開が求められる（GDPR 13 条 1 項）。これに加えて、個人情報の保存期間の公表、当該情報の消去に関する権利告知、異議申立の権利等の告知が行われなければならない（GDPR 13 条 2 項）。

また、原則として取得情報の目的外利用は認められていない（GDPR 5 条1 項 b）。取得情報の例外的な目的外利用の許容条件について、各加盟国は GDPR 6 条 4 項の要請を考慮に入れた立法を行うことが求められる。

以上の GDPR からの要請に対応するため、ドイツ連邦データ保護法 4 条は、公共空間でのカメラ設置について具体的規定を設けている。ドイツにおいて、公共空間における監視カメラの設置は、以下の目的を達するため必要な範囲においてのみ認められる。例えば、公的機関の任務達成のため、住居権（Hausrecht）を保持するため(6)、その他特定の目的達成のた

(6) 住居権とは、一定の空間への立入りを許可しまたは禁止する権利を意味する。以上について、松宮孝明「ポスティングと住居侵入罪」立命館法学 297 号（2004 年）

めの正当な利益保持のために必要な場合に、これが認められる(7)。また、上記 GDPR からの要請により、監視カメラから取得された情報の目的外利用は原則禁止となるが、ドイツ連邦データ保護法 4 条 3 項は、国家の安全及び治安維持、犯罪の訴追に関わる利用についてのみ、例外的に監視カメラより取得された個人情報の目的外利用が認められる場合があると定めており、警察、検察等の刑事捜査・訴追機関等への情報引き渡しについて、本条の規定を根拠に認められることになり、これは GDPR 6 条の規定が公共の利益の為のデータ取り扱いを認めることと一致する。

(3) GDPR が定めるセンシティブ情報取り扱いに関する規制

GDPR 9 条 1 項は、原則として個人の生体データ等、センシティブ情報の取り扱いを禁止しているが(8)、これは、刑事手続において必要な範囲での情報取り扱いまでをも妨げるものではない（GDPR 9 条 2 項 f）。刑事手続において、特に監視カメラ等から得られた情報を処理して個人を特定する場合、事件現場の残留物から得られた遺伝情報等を用いて個人を特定する場合などが想定されるが、捜査・訴追目的等を達成するために必要かつ十分な範囲で（比例原則）当該センシティブ情報の取り扱いが認められることになる（GDPR 9 条 2 項 g）。これを受けて、ドイツ連邦データ保護法 22 条は、公的機関及び民間機関において、社会的安全及び社会的保護に関する権利行使及び義務の履行に必要な場合等に、センシティブ情報の取り扱いを許容する。更に、公的機関が重要な公的利益にとって絶対的に必要な場合、公共の安全にとって重大な危険防止にとって必要な場合、公共の福祉に対する重大な不利益、懸念を防止するために必要な場合に当該

---

16 頁註15参照。

(7) ドイツ連邦データ保護法 4 条 1 項の文言から、スポーツ競技場、ショッピングセンター、公共交通機関の発着場等の安全保持等がその代表例となるだろう。

(8) 個人の生体データとは、極めて多義的であるが、GDPR の定義に則れば、監視カメラ映像の分析によって得られる顔特徴量データ、遺伝情報などは本条の規制対象となる。

情報の取り扱いが認められ、危機管理、紛争の阻止、人道的措置の領域における義務の履行のために必要な場合も同様であるとされる。ドイツ刑事司法領域において、何らかのセンシティブ情報の取り扱いが必要となる際には、ドイツ連邦データ保護法 22 条及び、刑事法規範において個別の規定が設けられている場合にこれが許容されることになる。

(4) 個人情報の消去義務

GDPR 17 条 1 項は、いわゆる「忘れられる権利」について定めており、当該権利実現のため、17 条 1 項 e が EU 加盟国に対して立法化等適切な処置を求める。更に、GDPR 17 条 1 項 a は、データの目的外利用を禁じており、この場合当該データを遅滞なく消去しなければならない。EU 域内における国内法制化の例を挙げると、例えばドイツ連邦データ保護法 4 条 5 項は、取扱データが取得目的に照らして必要がなくなった場合に、遅滞なくデータを消去しなければならないとする。

(5) プロファイリングに対して異議を呈する権利

GDPR は、個人情報の取得それ自体はもちろんのこと、取得された情報の適切な処理を求めている。とりわけ、個人に対する AI 等によるプロファイリングの実施について問題となる。GDPR 4 条 4 項は、「プロファイリング」とは、個人（自然人）と関連する一定の個人的側面を評価するための、特に、当該個人の業務遂行能力、経済状態、健康、個人的嗜好、興味関心、信頼性、行動、位置及び移動に関する側面を分析又は予測するための、個人情報の利用によって構成される、あらゆる形式の、個人情報の自動的な取扱いを意味すると定める。GDPR 22 条は、個人に対してプロファイリングに対して異議を唱える権利を認めている。当該権利が行使された場合には、例外的にプロファイリングの実施が認められる場合を除いて（GDPR 21 条）、直ちにデータ管理者によるプロファイリングの中止が行われなければならない。これに関連して GDPR 22 条は、プロファイリングに代表される AI による自動化された判断にのみ基づいて、個人が取り扱

われることを禁止している。更に、GDPR 13条がプロファイリング等の判断過程の公正性、透明性を求めていることから、個人情報の取り扱いに関する責任の所在を明確にすることを求めている。

2　EU 刑事司法領域における個人情報保護

(1)　総論

EU 域内において行われる個人情報の取り扱いは、原則として GDPR の規制を受けることになるが、刑事司法領域においては EU 刑事司法データ保護指令が重要となる。同指令は、その前文 1 で個人情報の保護が基本権であることを宣言する。これは、同指令が刑事捜査・訴追目的の達成と個人情報保護の重要性をともに認識し、両者のバランスを図りつつ、EU 域内の刑事司法における個人情報の取り扱いに際して最低限遵守されなければならない基準を示すものであることを意味する。EU 加盟国には、刑事捜査・訴追における個人情報の取り扱いについて、EU 刑事司法データ保護指令に則った立法及び法解釈、運用を行う義務が課せられるが、本指令よりも厳格なデータ保護基準を設けることは妨げられない（EU 刑事司法データ保護指令 1 条 3 項)。本指令の内容には、曖昧な部分も多く存在しており、EU 加盟国内における具体的内容の実施方法について、決して小さくない立法裁量が認められていると考えられる(9)。

(2)　EU 刑事司法データ保護指令の具体的内容

本指令は、EU 域内における警察及び司法当局間で犯罪予防、捜査、訴追等に関わる情報共有及び当該情報に関係する個人の基本権保護を目的とする（EU 刑事司法データ保護指令 1 条 1 項)。民間機関及びその他の目的

(9)　*Weichert,* Bewertung der EU-Richtlinie für den Datenschutz bei Polizei und Justiz, S.4 2016.
https://www.netzwerk-datenschutzexpertise.de/sites/default/files/bewertung_2016_02_eudsri_polizei.pdf から取得。
（最終アクセス日2019年10月 9 日）

で行われるデータの取り扱いは、GDPR が適用されなければならないが（EU 刑事司法データ保護指令 9 条 2 項）、両者は互いに密接に関係し、相互補完的な関係にあるため、その定義は一律ではないように思われる。

EU 刑事司法データ保護指令 4 条 1 項が、データ処理の一般的許容要件について言及する。ここでは、当該データの取り扱いが比例原則に則ったものであること、データの取り扱いに必要性が認められなければならないとされる。更に、目的外利用について、各 EU 加盟国において必要性及び比例性を考慮した規定が設けられる（EU 刑事司法データ保護指令 4 条 2 項）。EU 刑事司法データ保護指令は、個人情報の取り扱いに関して具体的場面を想定した具体的要件を定めるものではないが、EU 加盟国の立法及び法解釈、運用の指針を示す。例えば、センシティブ情報について、厳格な必要性の審査を要求し、かつ当該情報取り扱いの運用には高い安全性が求められるとしている（EU 刑事司法データ保護指令 8、9 条）。EU 刑事司法データ保護指令 3 条 4 項は、GDPR におけるそれと同様にプロファイリングについて定義する。また、刑事手続において、プロファイリングの結果にのみ基づいて個人に不利な決定を行うことは原則として禁止されている（EU 刑事司法データ保護指令 11 条 1 項）。更に、民族、宗教的及び政治的信条、遺伝子情報に基づくプロファイリングが行われてはならない（EU 刑事司法データ保護指令 11 条 3 項）。EU 加盟国は、以上の要請を満たしたプロファイリングに関する規定を設けることが求められる（EU 刑事司法データ保護指令 24 条 1 項 e）。しかしながら、各 EU 加盟国における実務がその運用を満たすことができなかった際の具体的措置、例えば証拠法上の取り扱い等について、本指令は何らの規定も置かない。

この他にも、EU 加盟国は取り扱いデータの保存期間及び保存の必要性についての審査機関についての規定を設けることが求められる（EU 刑事司法データ保護指令 5 条）。更に個人情報の取り扱いについて、被疑者、有罪判決を受けた者、被害者、証人等について分類し、その取り扱い方法について個別の規定が設けられなければならないとされる。また、誤った個人情報が移転された場合、不当に当該情報が移転された場合には、受信

者は直ちにこれを通告し、削除の手続が行われなければならない。当該手続についても EU 加盟国は適切な規定を設けなければならないものとされた。

以上のように、GDPR と並んで、刑事司法の領域では EU 刑事司法データ保護指令が重要となるが、その具体化については EU 加盟国の立法に委ねられる部分が多い。以下では、ドイツにおける議論を参照し、EU 域内の刑事司法における個人情報の取り扱いについて考察する。

3 ドイツ刑事司法における具体化

(1) 基本権としての個人情報保護：ドイツにおける情報自己決定権の議論

ドイツにおいて、情報自己決定権とは、「各人が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」であり「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権限」であるとされている。しかしながら、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、「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」と言い換えることもできよう。ドイツの情報自己決定に関する議論においては、通常、情報取り扱いに関する権限は、当該情報が帰属ずる個人に完全に委ねられるとする前提に立ち、これを制限するためには情報自己決定権に優越する公的な利益の存在が必要となるとされる(10)。ここでは、情報の重要性の程度という価値判断は行われない。仮に情報自己決定権に対する制限が認められる場合におい

(10) ドイツにおける情報自己決定権に関する議論について、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』（尚学社、2013 年）281 頁以下を参照した。

ても、法律による明確な条件設定が必要となり、これが対象者となる個人に示されることが必要となる。

以上のことは、刑事司法領域においても同様に妥当し、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る必要がある。

(2)　ドイツ刑事司法における個人情報保護

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し、これは個人情報を用いた捜査手法統制に関する一般的規定であると理解することができよう。本条がいう、ドイツ連邦、州法には、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等も含まれると考えられ、同法は当然にEU法に適合的である必要があることから、ドイツ刑事司法上の個人情報の取扱は、部分的にではあるがGDPRにも適合的であることが求められることになるだろう。更に、EU刑事司法データ保護指令の要請に適った立法及び法解釈、運用が行われなければならない。

(3) 写真撮影、監視カメラ等を用いた監視型捜査における個人情報保護

具体的な捜査手法に対する統制について、例えばドイツ刑事訴訟法100条hは、公共空間における写真撮影及び映像の記録及び、その他の方法による捜査について定めており、これらは対象の監視及び撮影された写真の提示を通じた事案の解明を目的として行われる[(11)]。上記捜査手法が許容されるための要件として、嫌疑の存在、捜査目的を達するために他の手法を用いることが困難であることが求められる。また、事件捜査に関係のない第三者が映像に映り込むような場合には、これに可能な限り配慮しなけれ

(11) *Graf*, Beck Online Kommentar zur StPO 30.Ed. §100h Rn.1ff., 2018.

ばならないとされている。取得された情報は、当初の使用目的に鑑みて不要となった時点で遅滞なく消去されなければならない。

また、近年、警察による監視カメラから取得された顔特徴量データの処理、解析に関する刑事訴訟法上の個別の根拠規定が存在しないことが問題視されている。例えば、ハンブルク警察において、同捜査はドイツ刑事訴訟法161条、163条の規定とドイツ連邦データ保護法48条の規定に基づき行われているが(12)、これは検察官及び警察官の一般権限に基づき顔特徴量データの処理、解析を用いた捜査が行われていることを意味する。顔特徴量データの処理、解析の性質に鑑みると、これを用いた捜査が与える個人の基本権侵害の程度は低いものではなく、比例原則に則った捜査機関に対する統制を可能とする個別の刑事訴訟法上の根拠規定が必要となるように思われる。この点について、顔特徴量データの取得後、自動で同データの処理、解析が行われる場合に多くの問題が存在する。従来、捜査対象者となる者の嫌疑性の有無、程度によって、許容される捜査手法の種別が判断されてきた。しかしながら、不特定多数人を対象とする監視カメラによる映像撮影と、そこから得られた情報の処理、解析が行われる場合、そもそも事前に捜査対象者の特定が行われないことも多い。会場警備等の際、不特定多数人の中から、特定の危険人物を洗い出すことを目的とする使用方法がポピュラーであるとも考えられるが、具体的な嫌疑性がないのにもかかわらず抽象的な犯罪発生の危険を理由として、公益の追求を目的として無関係な者をも含めた不特定多数人に対する基本権侵害を肯定できるかについては議論が分かれよう。更に、情報の処理、解析に用いられるソフト

(12) ハンブルクで開催されたG20サミットにおいて、監視カメラを通じて取得された顔特徴量データの処理、解析が会場警備等に用いられた。これに対して、ハンブルク自由民主党から刑事訴訟法上の根拠規定の欠缺が指摘された。ハンブルクにおける状況に関して、以下のweb サイトを参照した。
https://www.lto.de/recht/nachrichten/n/gesichtserkennung-rechtsgrundlage-stpo-aenderung-aufklaerung-straftaten-ein griff-persoenlichkeitsrechte/
（最終アクセス日2019年 2月19日）。

ウェアの誤差率に起因する問題も軽視できないとする指摘もある(13)。誤差率の問題は、非捜査対称者に関わるデータを自動的に即時消去するという対策を講ずる場合にも軽視できないし、何より誤った解析結果に基づく誤った捜査が行われる危険性が考慮されなければならない。

監視カメラによる情報取得と顔特徴量データの処理、解析を用いた捜査の運用について、ドイツ連邦データ保護コミッショナー、ドイツ社会民主党からも問題点が指摘されており(14)、今後の動向が注目される。

(4) 遺伝子解析を用いた捜査における個人情報保護

まず前提として、刑事手続における個人の人格的プロフィールに関するセンシティブ情報の取扱は、ドイツ基本法 1 条 1 項に反するとして禁止されている。刑事手続における DNA 型鑑定は、対象が DNA コード化領域を対象とする場合にのみ認められることになる。

ドイツにおける DNA 型鑑定に関する立法例を参照すると、被疑者の同意が得られない場合の DNA 型鑑定実施は、捜査の遅延が危ぶまれる場合を除いて裁判官の命令に拠らなければならない旨規定されている（ドイツ刑事訴訟法 81 条 e、f）。

また、ドイツにおける DNA データベースに関する立法例を参照すると、DNA データベース運用のためには鑑定資料採取及び DNA 型鑑定の実施よりも一層高い条件を備えた法定要件を満たす必要があるとされている(15)。

---

(13) 例えば、昨年度ベルリン中央駅で行われたパイロットプロジェクトにおける顔認証一致率は80%であったとされる。
http://www.spiegel.de/netzwelt/netzpolitik/berlin-gesichtserkennung-am-suedkreuz-ueberwachung-soll-ausgeweitetwerden-a-1232878.html（最終アクセス日2019 年2 月19 日）。

(14) https://www.lto.de/recht/nachrichten/n/gesichtserkennung-rechtsgrundlage-stpo-aenderung-aufklaerung-straftaten-eingriff-persoenlichkeitsrechte/（最終アクセス日2019 年2 月19 日）。

(15) ドイツにおける DNA データベース関連規定の立法状況について、拙稿「刑事手続における強制採血とDNA 型鑑定に関する一考察」広島法学36 巻 2 号（2012 年）118 頁以下参照。

ドイツにおいて、将来行なわれることが予想される犯罪捜査での利用を目的とした DNA 型鑑定は、鑑定資料の採取も含め刑事訴訟法 81 条 g の規定を根拠に実施されており、これは先に見たドイツ刑事訴訟法 81 条 e、f の規定が現在問題となっている犯罪捜査を対象としたものとはその性格を異にする。対象犯罪について重大犯罪、性的自己決定に対する罪及び累犯傾向が認められる犯罪類型に限定されており、裁判所において再犯の危険性の程度という要素が重視され、将来行われる犯罪捜査のための DNA 型鑑定実施の可否について判断されていることがわかる（ドイツ刑事訴訟法 81条 g 第 3 項）。また、ドイツ連邦憲法裁判所の判断によれば、本条に基づく DNA 型鑑定結果の将来における利用は刑事訴追を目的としたものに限定されることになっており(16)、DNA 型鑑定結果の保存、運用を行うドイツ連邦刑事局（Bundeskriminalamt）においても(17)、その利用目的は犯罪捜査及び犯罪予防目的及び国際司法共助に限定されることになる（ドイツ刑事訴訟法 81 条 g 第 5 項 2 号）。

更に、DNA 型鑑定結果の廃棄について、嫌疑不十分による不起訴及び公判において被告人に対して無罪判決が下された場合には、当該データは即刻廃棄されなければならないとされる（ドイツ連邦刑事庁 8 条 3 項）。DNA 型鑑定記録の保存期間についても問題となるが、ドイツ連邦刑事局法 32 条 3 項によれば、対象者が少年の場合は 5 年、成人の場合は 10 年毎に、保存されたデータについて、これを削除するのか、今後も継続して保存するかを審査するとしている(18)。

---

(16) BVerfGE 103, 21.

(17) DNA 型データベースの運用に関わる、データの利用、処理、消去は、連邦警察法に基づいてこれが行なわれることになるが、基となる情報取得は、刑事訴訟法による法的統制のもと行われている。

(18) 以上に関して、ドイツ現行法下では DNA データの保存期間が必ずしも明確になっていないことから、対象者の情報自己決定権に対する過度な介入を招くとの批判もされる。玉蟲・前掲註 9 ）405 頁。

Ⅱ　我が国の刑事司法領域における個人情報保護

1　我が国の具体的問題に関する検討

(1)　総論

現在、わが国の個人情報保護委員会は、EU からのデータ移転を円滑に行う為、「個人情報の保護に関する法律に係る EU 域内から十分性認定により移転を受けた個人データの取扱いに関する補完的ルール」を定めるなどして、2019年1月23日（現地時間）、GDPR による十分性認定を受けた。

しかしながら、わが国において個人情報保護は未だに基本権として位置づけられていない(19)。個人情報保護が基本権とされていない以上、刑事司法領域において、個人情報に対する何らかの侵害を伴う刑事捜査・訴追機関の行動がとられた場合でも、個人情報に対する侵害それ自体が裁判所による司法審査の対象になり難いという事態を招く(20)。

確かに、十分性認定に際して、対象国に EU からの要請と完全に一致する個人情報保護制度の構築を求めるものではなく、憲法、刑法を含んだ法制度をはじめとして、他の関連立法等、データ保護の監督機関等を含め総合的に判断し、実質的な等価性があればこれが認められるものと解されるが（GDPR 45 条 2 項）、個人情報保護に対する根本的な理解に相違があることは、少なくとも十分性認定の「再審査」（GDPR 45 条 3 項）が行われた際に何らかの問題を生じさせる可能性があるのではないだろうか。わが国の政府が EU との交渉で示した国内における個人情報保護関連法制についての説明と、実際に行われている具体的運用に少なからぬ乖離が認められる部分も有り、今後予定される十分性認定の再審査までに根本的な改善が求められるように思われる。

---

(19) 内藤静雄「日本とEUの個人情報保護法制の比較」ジュリスト 1521 号（2018 年）15、16 頁。

(20) もちろん、個人情報の取得のために、住居内等への立ち入りが行われる、対象者の身体的自由を侵害する等の事情があれば、情報取得「手段」の強制処分性が認められることになる。

以下では、わが国の刑事司法における個人情報保護に関する問題として、主に写真撮影、監視カメラ等を用いた監視型捜査に関する問題、遺伝子解析を用いた捜査に関する問題を取り上げる。我が国における立法状況及び、法解釈、具体的運用が EU 法的観点から見ていかなる問題を孕んでいるのかを検討し、GDPR からの要請を満たしていないと考えられる部分については法改正等の提言を行う。

（2）写真撮影及び記録映像を用いた捜査手法に関する問題点の検討

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ない。判例は、いわゆる京都府学連事件判決において[21]、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、みだりにその容貌等を撮影されない自由を有しており、警察官といえども正当な理由なしに写真撮影をすることは憲法 13 条に違反するとした。しかしながら、その一方で、個人の私生活上の自由は、公共の福祉のために必要な場合には、国家権力による相当の制限を受けることを容認している。以上を前提として、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、個別の写真撮影が許される場合があるとした[22]。

更に、上記個別の写真撮影の問題に加えて、近年では監視カメラ等による継続的な映像撮影に関する問題が議論されている。京都府学連事件において、「犯罪が行われたと思料するとき」に、捜査活動の一環として被疑者に対する写真撮影が行われたものであるが、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ものが多いように思われる（警察法 2 条、警察官職務執行法 1 条 1 項）[23]。こ

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

(22) 以上に関して、星周一郎『防犯カメラと刑事手続』（弘文堂、2012 年）168-169頁を参照した。

(23) 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・

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。

更に、上記に加えてカメラの設置主体による相違も見られる。例えば、警察等によるカメラ設置が行われる場合には、これは行政警察活動の範疇で行われたものであると理解されるが、監視カメラの大半が民間機関によって設置されたものであることを考えると、民間設置の防犯カメラ映像等の捜査への利用が如何なる場合に許容されるかが議論されなければならない(24)。情報提供に際して民間側には、個人情報保護法に照らした配慮が求められる。この点について、防犯目的での監視カメラ設置について大阪地裁が示した、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、という基準が参考となる(25)。上記基準は、EU法からの要請にも親和性が認められるように思われるが、これに加えてカメラ設置の透明性、データ削除の要件についても検討されるべきであろう。

更に、防犯カメラ設置目的を考えれば、犯罪捜査目的達成のために、警察等捜査機関に対してカメラ映像を提供することは認められることになりそうである。しかしながら、個人情報データベース等を構成する個人データ（個人情報保護法2条6項）を第三者に提供する場合には、利用目的による制限を定めた16条の特則である第三者提供の制限に関する規定である23条により、第三者提供は原則として本人の事前同意を得て行うことが定められている(26)。ただ、法令に基づく場合には、例外的に事前同意がなくても情報提供を行うことができるとされており、捜査目的を達成するため行われる情報提供もこれに含まれることになるだろう（刑事訴訟法197条

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。

(24) 同前53頁。

(25) 大阪地判平成6年4月27日判時1515号116頁。本裁判例について、同前50頁を参照した。

(26) 同前53頁。

等)。それ故、捜査側は、刑事訴訟法197条等を根拠として、任意捜査の一環として当該情報の提出を求めることができることになる。提供側拒否の場合、強制捜査の対象となる場合も想定されるが、わが国の実情に鑑みると基本的には映像を差し押さえること自体に強制処分性が認められるとは考えにくく、提供者の同意がないことのみが問題となる(27)。

以上の問題に加えて、取得された写真及び映像から抽出されたデータを利用した生体認証の許容性も問題となる。個人情報保護指針（個人情報保護法47条、53条）に則った運用が行われ、一定程度対象を限定し、関係しない情報を遅滞なく削除すれば従来のプライヴァシー侵害と質、量ともに本質的に相違しないプライヴァシーへの影響しかないとする意見もあるが(28)、疑問である。顔特徴量データ等の処理、解析を行う場合、対象者へのプライヴァシー侵害の程度は、単に写真、映像を撮影する場合よりも高いものとなる。また、不要なプライヴァシー侵害を避けるために、対象の限定、関係しない情報を削除する為に、何らかのソフトウェアを用いることが想定されるが、先に見たドイツにおける指摘からもわかるように、誤差率に起因する問題を看過することはできない。

以上のように、わが国の刑事司法における個人情報保護に関する感度は決して高いものとはいえないが、これを物語る事実が明らかとなった。カルチュア・コンビニエンス・クラブ（ 以下、CCC とする ）が捜査機関からの捜査関係事項照会書に応じて、裁判所の令状なしに「T カード」利用者の氏名や購入履歴を捜査機関に提供していることを問題視する報道が2019年に入って広がった。CCCは、遅くとも2012年から警察からの捜査関係事項照会書に応じて、T カード利用者の氏名、生年月日、物品等の購入履歴、レンタル履歴の個人情報を警察に「任意」で提出していた。これらの個人情報から、AI によるプロファイリングにより個人の性質、趣味嗜好等を推定することもできる。以上のような裁判所の司法判断を経ずに

(27) 同前 54 頁。
(28) 同前 52 頁。

行われる捜査機関の個人情報の収集は、EU からの十分性認定を受けるための条件に反する可能性がある。

十分性認定のドラフトを見ると、わが国において警察の組織法である警察法 2 条の存在から警察が自制的かつ制限的に捜査活動を行っており(29)、捜査関係事項照会書による個人情報の提供が企業に強制されることはなく、必要な場合において令状取得が適切に行われてきたという、やや実態とは異なった認識を EUが有していることが分かる(30)。また、EUがわが国の令状審査において、被疑者・被告人の防御権が尊重され、犯罪の重大性のみならず、押収物の価値に重きを置いた司法判断を行っていると認識していることも重要である(31)。EU 法を考慮に入れた場合、捜査機関による個人情報の取得に際して、対象者の同意の有無のみを論ずれば良いということにはならず、対象となる個人情報それ自体の価値に注目した司法判断が行われる必要がある。特に、個人のセンシティブ情報の取得について、対象者の同意がある場合でも、これを許容するための条件を定めた個別の根拠規定の存在が求められることになろう。

更に、取得情報を処理、解析してこれを捜査に用いる場合、そこから生ずる人権侵害の度合いは更に高いものとなる。わが国の現行法は、捜査機関による情報取得自体についても EU 法からの要請を満たしていない可能性が有り、情報処理について法の欠缺が存在することは明らかである。捜査機関の行う個人情報取得と取得情報の処理について、それぞれの性質に着目した個別の統制方法が検討されるべきである(32)。EU 法からの要請に

(29) 警察法は、刑事訴訟法とは異なり、捜査機関を統制する役割を担うものではない。以上について、笹倉宏紀「行政調査手続と捜査」井上正仁・坂巻匡編『刑事訴訟法の争点』ジュリスト増刊100 頁、100−103頁参照(2013 年)。

(30) COMMISSION IMPLEMENTING DECISION of 23.1.2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information, paras 125-126.

(31) *Id*, at 121-124.

(32) 我が国の警察実務における情報の取り扱いについて、もっぱら情報取得時のイン

よれば、個人情報を刑事捜査・訴追にこれを用いる場合には、一定程度の嫌疑の存在、代替手段の利用可能性の検討、被疑者以外の第三者に対する配慮が行われなければならないことから、わが国の現行法でこれに対処できない部分については立法的措置も含めた根本的な対策が求められる可能性がある。

(3) DNA 型鑑定等をめぐる問題点

わが国の刑事手続において、DNA 型鑑定結果の証拠能力は承認されている(33)。

警察実務において、DNA 型鑑定の実施に際して、鑑定資料の提出に被疑者の同意が得られない場合には、身体検査令状と鑑定処分許可状の併用によって強制採血が行われ、鑑定資料としての血液が採取されることになる。鑑定自体についても、同様に鑑定処分許可状を根拠にこれが実施されていると考えられる。以上のように、被疑者の同意が得られない場合には、DNA 型鑑定に関する一応の司法審査が行われているようにも見えるが、ここで留意すべきは DNA 鑑定自体に強制処分性が認められているというよりは、むしろ鑑定資料の採取に伴う身体への侵襲を強制処分として捉えているにすぎないということである。以上のことは、鑑定資料の提出に被疑者の同意が得られる場合において、何らの令状によらず口腔内組織片が採取され、DNA 型鑑定についても何らの司法審査を経ないままこれが実施されることになる警察実務における現状の運用方法を見ても明らかであ

パクトが着目されることで、情報取得の法的正当性に関する議論の重要性のみが強調されてきたきらいがある。情報取得の正当性の審査が軽視されてはならないが、その重要性が強調される過ぎることよって、取得情報の保存・処理・解析に関する問題の議論が未だ十分になされていないことも事実である。以上のような状況が、警察実務において取得された情報に対して法的統制が及ばない、「取得時中心主義」と呼ばれる事態を生じさせているという指摘がされる。以上に関して、山本龍彦『プライバシーの権利を考える』（信山社、2018 年）89 頁以下参照。

(33) 最決平成 12 年 7 月 17 日刑集 54 巻 6 号 550 頁。

ろう。また、以上のような運用を経て収集された DNA 型鑑定結果は警察によって保存され、DNA データベースという形態で管理、運用されている。DNA データベースの運用についても、国家公安委員会規則である DNA 型記録取扱規則は定められているものの、刑事訴訟法上の規定は存在せず、捜査手続の途上で得られた DNA 型鑑定結果の事後的利用について何らの法的規制も存在していない現状がある。これは、EU 法が、個人情報の中でもセンシティブデータの取扱に特段の注意を払い、不当な基本権侵害とならないように EU 加盟国において国内法整備が進められている状況と大きく異なる。以上に関して、DNA 型鑑定について、東京高裁平成 28 年 8 月 23 日(34) において、これまで任意処分の範囲で行われるとされてきた DNAを含む唾液を警察官によって採取される行為が強制処分にあたると判断され、注目に値する。わが国においても、刑事手続における DNA 型鑑定について、具体的根拠規定が設けられることが求められる。

更に近年では、過去に行われた犯罪に対する従来型捜査に加えて、将来行われるかもしれない犯罪の予防に DNA鑑定を用いようとする動きがある。例えば、ヒトゲノム情報から、対象人物の犯罪可能性・再犯可能性を解析しようとするものがあるが、その実施は、わが国の警察実務における現在の DNA型鑑定の対象が非コード化領域のみを対象としていることで同鑑定が強制処分の対象とならないとする警察当局の説明と矛盾することになる(35)。

この様な将来における危険判断をも含んだ方法を用いることは、現在の裁判所による司法審査のあり方を根底から覆す可能性がある。また、上記と併せて、わが国において DNA型鑑定に関する具体的根拠規定が全く存在していない実情に鑑みれば、我が国の現行法下で当該捜査手法を用いる

(34) 東京高判平成 28 年 8 月 23 日高裁刑集 69 巻 1 号 16 頁。本裁判例についての評釈として、久岡康成「刑事犯例研究23」立命館法学第 378 号（2018 年）359 頁以下参照。

(35) 警察実務の説明について、松下徹「警察における捜査手法の高度化―DNA 型鑑定及びDNA型データベースを中心に」刑事法ジャーナル29 号（2011 年）20 頁以下参照。

ことは困難といわざるをえない(36)。

(4) 小括：個人情報の取得とプロファイリングに関する問題

以上見たように、我が国の刑事手続における個人情報の取り扱いについて、様々な問題があることが明らかとなった。AI の社会における効果的な実装に際して、大量の個人情報の取得が必要となるのではあるが、我が国において個人情報の取得それ自体についても多くの解決しなければならない問題がある。具体的には、個人情報保護が基本権とされていないことに起因して、様々な場面で立法の欠缺が見られる。この問題は特に刑事司法の領域において深刻な弊害をもたらす。強制処分法定主義が妥当する我が国において、未だに電子化された個人情報の取得に関する具体的な刑事訴訟法の規定が存在していないことはその顕著な例であるといえ、刑事捜査・訴追機関が裁判所の事前審査なしに広範囲にわたって個人情報を取得できる実態がある。このような事態に対して、一部企業は自前のガイドラインを作成して、令状が提示されないことには警察の情報提供依頼には応じないなど、個人情報保護に配慮した動きを見せているが(37)、民間機関の自助努力にのみ個人情報保護水準の維持、発展を委ねることには許されない。個人情報取得に対する法的統制を十分に整備した上で、当該取得情報の処理、そこから得られた結果の保存、運用についても各レヴェルにおける具体的な基準が立法によって示されなければならない。とりわけ、顔認

(36) しかしながら、「将来起こるかもしれない危険性」判断に際して、いわゆるビッグデータを収集、加工し人工知能による分析結果を判断資料として用いることで、より偏りのない公正な判断が行われることを期待できるかもしれない。AI とビッグデータの活用による犯罪予防に関するドイツ法務省の下記のホームページを参照。https://www.bmjv.de/DE/Ministerium/ForschungUndWissenschaft/Datenethikkommission/DEK_Empfehlungen.pdf?__blob=publicationFile&v=2（最終アクセス日2018 年 10 月 22 日）

(37) CCCは、今後、令状によらない警察への情報提供を原則行わないことを発表した。以上について、以下のホームページ参照。https://www.ccc.co.jp/news/2019/20190823_005537.html（最終アクセス日2019 年 9 月 3 日）。

証技術を用いた犯人性の推定等、AI による自立的判断のエラーが発生しやすい領域においては、特段の注意が必要なるように思われる。また、DNA 解析に基づく判断についても、対象物である DNA の有するセンシティブな性質を考慮に入れた適切な立法的措置が求められる。

おわりに

EU とわが国との間には、個人情報保護に対する理解の大きな相違がある。すなわち、EU においては、個人情報保護が基本権に関する問題であることが認識されているが、わが国においてはそのような共通理解を得るまでにいたっていないということである。

わが国においても、GDPR の十分性認定を受けるための個人情報保護法制についての追加的措置が行われるなど、個人情報保護についての対策が行われる。しかしながら、先に述べた個人情報保護に関わる根本的な理解の相違は、本来であれば最も大きな個人情報への侵害が想定される刑事司法の分野において、十分な立法的措置が行われないまま、重要な個人情報への侵害を伴う捜査手法行使が容認されているという問題を生じさせている。AI による自動化された判断の可否について、大量の情報取得、取得情報の処理、運用、判断結果の保存等、様々な段階における検討が必要となるが、我が国の刑事司法において AI 判断の前提となる情報取得についてすら十分な法的統制の枠組みが存在していないことが明らかである。

GDPR の規制対象は、民間機関等、刑事捜査・訴追機関ではない組織の行う個人情報の取扱いであるから、民間機関が取得、処理した情報を警察等に引き渡したとしても、直接の規制対象にはならないかもしれない。しかしながら、情報の移転先である警察等の公的機関において十分な個人情報保護を行うための制度的保障が十分ではないと判断されれば、将来予定される GDPR からの十分性認定の再審査に少なからぬ影響があるように思われる。

Reprinted from

KITAKYUSHU SHIRITSU DAIGAKU HOU-SEI RONSHU

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

December 2019

Künstliche Intelligenz und juristische Herausforderungen aus der Perspektive des Strafprozessrechts

MIZUNO Yoichi