

日本政府の 2018 年 9 月 14 日付け
「法執行及び国家安全保障目的の日本の公的機関による個人情報の収集及び使
用」に対するカウンターレポート

2026 年 1 月 26 日

欧州委員会 データ保護課長 Mr. Olivier MICOL

欧州委員会 国際関係データ流通課長 Ms. Louisa KLINGVALL

欧州データ保護監察機関 (EDPS) 事務局長 Mr. Leonardo CERVERA NAVAS

欧州データ保護会議 (EDPB) 事務局長 Ms. Isabelle VEREECKEN

写し) 法務大臣 平口 洋 殿
個人情報保護委員会委員長 手塚 悟 殿

公益社団法人自由人権協会 (JCLU)
監視とプライバシープロジェクトチーム

はじめに

本レポートは、日本政府が発出した、[2018 年 9 月 14 日付「法執行及び国家安全保障目的の日本の公的機関による個人情報の収集及び使用」と題する報告書](#)（以下「政府報告書」という。）の問題点などを指摘する、いわゆるカウンターレポートである。

政府報告書は、欧州の[「一般データ保護規則」\(General Data Protection Regulation, “GDPR”\)](#)に定められた、いわゆる「十分性認定」を受けるために、日本の関係する複数の省庁を作成名義人として、欧州委員会委員宛に送付された書簡に添付されたもので、その表題のとおり、警察をはじめとする法執行機関や、安全保障機関における個人情報の取り扱いについて、日本の法制度や実務を取りまとめて報告するものである。

GDPR は、欧州における個人情報保護に関する包括規制である。原則として EU 域内における個人データを域外に移転することを禁止しつつ、例外的に移転を認める場合の一つとして「十分性認定」（“adequacy decision”）という制度を設けている (GDPR・前文第 103 項、第 45 条)。域外の国や地域について、欧州における個人情報保護と同程度に十分な保護がなされていることを欧州委員会が認定すると、当該国や地域に対する個人データの移転が包括的に許容されることとなる。

2019 年 1 月 23 日、日本の個人情報保護委員会と欧州委員会は、相互に十分性認定を行った。その際、政府報告書は、欧州委員会が日本の個人データの保護水準を認定するにあたり、重要な基礎資料とされた。

このことは、欧州委員会の Web サイトに掲載されている、日本に対する十分性認定を行った[委員会実施決定 \(COMMISSION IMPLEMENTING DECISION \(EU\)2019/419\)](#)（以下「本決定」という。）の記載からも明らかである。本決定は、附属書 II (ANNEX II) として政府報告書の英訳版を掲載した上、前文第 3 パラグラフで、「欧州委員会はまた、日本の事業者に移転された個人データが公的機関によって公益目的、特に刑法執行および国家安

全保障目的（「政府アクセス」）のために収集され、その後使用されることに関して、日本法において利用可能な制限および保護措置（監視および個人の救済メカニズムを含む）を評価した。この点に関して、日本国政府は欧州委員会に対し、最高レベルの大蔵および機関により署名された公式見解、保証および確約を提供しており、これらは本決定の附属書IIに含まれている。」（第113 パラグラフ）と強調している。

なお、政府報告書は、日本政府の「日 EU 間・日英間のデータ越境移転について」と題する Web ページにおいても、「欧州委員会の求めに応じ、EU から日本の民間事業者へ移転された個人データについて、日本の行政機関が収集・使用する場合における、当該個人データの取扱いに係る日本の法制度を説明する文書を発出しました。」との説明とともに掲載されている。

本決定は、本文において、「日本の公的機関が、本決定附属書 II に記載された説明、保証及び約束（本決定に基づく移転された個人データについて、日本の公的機関が刑事法執行または国家安全保障目的で収集・アクセスを行う場合の条件や制限を含む）を遵守していない場合」には、十分性認定の効力停止、修正等がありえる旨明記しており（第3条、下線は引用者）、刑事法執行や安全保障目的における個人情報の取り扱いの重要性が強調されている。

2019 年の十分性認定後に欧州委員会が実施した [2023 年の第 1 回定期レビュー](#)においても、法執行機関や安全保障機関の個人情報保護の取り扱いには個別のコメントがなされた。すなわち、「3 結論（“CONCLUSION”）」において、「最初の見直しの一環として得られた全体的な所見に基づき、欧州委員会は、日本が、当該決定の附属書 II に含まれる公式な表明、保証、及びコミットメントとともに、補完的ルールによって補完される個人情報保護法（APPI）の適用を受ける日本の個人情報取扱事業者に対し、欧州連合（EU）からの個人データについて、引き続き十分な保護水準を確保していると結論付けた。」¹ と言及している。

また、同レビューに関する基礎調査をまとめた [コミュニケーション・スタッフ・ワーキングドキュメント](#)においても、「日本政府は、日本の公的機関による刑事法の執行および国家安全保障を目的とした個人データへのアクセスと利用に関する制限および保護措置について、いかなる処理も必要かつ相応なものに限定され、独立した監督および実効的な救済メカニズムの対象となることを明確にした上で、欧州委員会に対し、公式な表明、保証、およびコミットメントを提供した。これらの救済メカニズムには、十分性認定に基づき個人データが移転される EU の個人のために日本政府が創設し、個人情報保護委員会（PPC）が所管・監督する特定の紛争解決手続が含まれる。」² と記載されており、十分性認定を

¹ 対応する原文は、“Based on the overall findings made as part of this first review, the Commission concludes that Japan continues to ensure an adequate level of protection for personal data from the European Union to personal information handling business operators in Japan subject to the APPI as complemented by the Supplementary Rules, together with the official representations, assurances and commitments contained in Annex II of the decision.”

² 対応する原文は、“The Japanese government furthermore provided official representations, assurances and commitments to the Commission regarding limitations and safeguards as regards access to, and use of, personal data by Japanese public authorities for criminal law enforcement and national security purposes, clarifying that any such processing is limited to what is necessary and proportionate and subject to independent oversight and effective redress mechanisms. These redress mechanisms include a specific dispute resolution

維持するにあたって、法執行機関や安全保障機関における個人情報の取り扱い状況が重視されていることがわかる。

しかし、本レポートの作成者らの所感として、政府報告書は、主に日本の刑事手続における個人情報の取り扱いについて、実態と異なる記載ぶりになっており、少なくとも誇張等がみられるほか³、多くの点で、本来記載されるべき記載の欠如や、実態とは大幅にニュアンスが異なる記載等が認められる⁴。本レポートの作成者らは、[公益社団法人自由人権協会（「自由人権協会」）](#)に所属する、刑事弁護実務、憲法訴訟、個人情報保護法案件などに携わる弁護士である⁵。自由人権協会は、日本国憲法が施行された 1947 年に設立された基本的人権の擁護を唯一の目的とする公益社団法人である。本レポートは、欧州委員会による十分性認定について利害関係を有しない団体によって作成されたものであり、欧州委員会による十分性認定を否定することも肯定することも意図して作成されたものではない。政府報告書の記載に対し、実務家にとって暗黙知とされている事実を指摘することで、今後行われる欧州委員会における十分性認定の更新審査がより正確かつ適切なものとなること、及び本レポートで指摘する政府報告書と日本における個人情報保護の実態との乖離を埋めるべく日本政府が適切な措置を講ずることを願い、本レポートを公表するものである。さらに、もし、十分性認定に基づいて EU 市民の個人データが日本に移転され、そのデータに対して検査機関等によるアクセスの濫用等が生じれば、EU 市民の基本権が侵害されることとなる。本レポートは、日本において、EU 市民を含めたすべての人々に対して高い水準の個人データ保護の基本権保護が確保され、日本法と EU 法の「本質的同等性」が維持されることを狙いとしている。

本レポートでは、政府報告書の項目の順序に則して、各項目の冒頭で報告書の記載内容を整理した上で、報告書に記載があるものについてはその記載の正確性を検証し、また実務における実態を紹介し、報告書に記載がないものの重要な論点等については、個別に項目を設けて記載する。

なお、本レポート作成にあたり、政府報告書発出時以降に法改正などが行われている場合には、基本的に本レポート作成時の最新のものを基礎として指摘する。特に行政機関の保有する個人情報の保護に関する法律（行個法）は、個人情報保護法に一本化されることにより 2022 年 4 月に廃止されたため、政府報告書において行個法の適用を前提としている記述について、本レポートでは個人情報保護法が適用されるものとして記載する。

procedure, administered and supervised by the PPC, that the Japanese government has created for EU individuals whose personal data is transferred based on the adequacy decision.”

³ 後掲指宿論文 61、62 頁は複数の誤りを指摘している。後掲 Drechsler・横田論文 350 頁には、同指宿論文に言及するとともに、「虚偽ないし少なくとも誇張が含まれている」と評している。

⁴ 後掲小向論文 67 頁脚注 8 は、検査関係事項照会について、政府報告書の英語版(正文)と日本語(参考訳)との翻訳を指摘している。すなわち、「検査関係事項照会の法的位置づけについてわが国では、法律の根拠があるので『検査機関に対し報告義務を負う』ものであると説明されることがある。なお、法務省が欧州委員会委員に当たる書簡では、英語の正本で『Under the Code of Criminal Procedure, the inquired persons are requested to report to investigative authorities.』と書かれている部分が、個人情報保護委員会が作成した参考訳では、『刑事訴訟法の下では、照会先は検査機関に対し報告義務を負うが、』と訳されている。少し意味合いが違うように感じるが、これは、『法的義務はあるが強制するものではない』という説明が、英語ではうまく表現できなかっただけであろう」と指摘している。小向論文の指摘する理由づけの当否はともあれ、「requested」と「義務を負う」では意味が異なる。

⁵ なお、事実のリサーチ及び英訳の過程で、一般社団法人 LEDGE の所属弁護士らからレビューとコメントの協力を受けた。

第1 「I 政府アクセスに関する法的な一般原則」について

政府報告書のこの項目では、「公権力の行使として、政府アクセスは法律を完全に尊重しながら実施されなければならない」ことを前提として、Aとして「憲法の枠組み及び、法原則の留保」が、Bとして「個人情報保護に係る具体的規定」が、それぞれ記載されている。そして、行個法が「民間部門及び公的部門における個人情報についての権利を保障している」ことを示すことで、「日本において、個人情報は、民間部門及び公的部門において、重層的な仕組みで保護されている」ことが記載されている。

1 「A. 憲法の枠組み及び、法原則の留保」について

(1) 政府報告書のこの項目では、冒頭で「日本国憲法第13条及び判例にて、憲法上の権利としてのプライバシー権を認めている」と明記している。

しかしながら、日本政府は、多くの訴訟において、「憲法上の権利として」プライバシー権が認められていることを否定している。例えば、政府が進めるマイナンバー制度（社会保障、税、災害対策を目的として日本の全住民に付与された国民識別番号）の違憲性を争ったいわゆるマイナンバー違憲訴訟（大阪高等裁判所令和3年(ネ)第588号事件）において、政府は、「最高裁判例は、憲法13条により保障された人権としての『プライバシー権』が認められるか否か、その内容はどのようなものであるかなどについては判示しておらず、・・・『プライバシー権』を認めることについては、慎重な立場をとっている。」（同事件における被控訴人国の答弁書）などと主張している。

実際、判例や裁判例において、いわゆる「プライバシー権」を明確に定義づけて認めたものは存在せず、日本の法実務上、「日本国憲法第13条及び判例にて、憲法上の権利としてのプライバシー権を認めている」が公権解釈として確定しているとは言い難い。

(2) また、日本政府は、外国籍者の憲法上の保護について限定的な枠組みを採用している。例えば、いわゆるマクリーン事件最高裁判決（最大判昭和53年10月4日民集32巻7号1223頁）は、外国人に対しても権利の性質上必要な範囲で日本国憲法に規定する人権保障が及ぶとしつつ、かかる保障は外国人在留制度のわく内で与えられているにすぎないとし、在留許可の延長等の判断は法務大臣の広範な裁量に服するから、日本国内における政治的表現行為を理由に在留延長を不許可とすることも許されると判断している。

(3) さらに政府報告書のこの項目では、「日本の法的枠組みにおいて、（犯罪捜査でなく）国家安全保障を理由として強制的な手段による情報収集は認められていない」こと、「強制的な収集である場合には、法律の留保の原則によって、個別に法律に基づかねばならない」こと、「強制的な手段による個人情報の収集は、常に令状に基づく必要があること」、「非強制的、任意の収集である場合には、自由にアクセスできる情報源からの取得や、任意の開示請求（すなわち情報を持つ自然人／法的組織に対し強制的でない請求）に基づき提供を受けること」、また「公的機関が調査を行う権限がある範囲において認められうる」ことなどが記載されている。全体のトーンとして、国家による個人情報の収集が制限的・謙抑的に行われている印象を受ける。

しかしながら、本レポートにおいて後述するとおり、日本では、国家機関による「非強制的、任意の収集」に藉口した個人情報の収集が広く行われている。その実態はおよそ制限的・謙抑的なものではない。

(4) なお、日本政府は、アメリカ政府より Xkeyscore の提供を受けていると報じられている⁶。Xkeyscore は、国會議員が提出した質問趣意書でも指摘されたとおり⁷、アメリカ諜報機関である国家安全保障局（“NSA”）の構築したデータベース・検索・プロファイリングツールであり、NSA が用いる大規模監視ツールにより取得された膨大な個人情報が保存されている。アメリカ政府は、日本政府の協力の見返りに Xkeyscore を提供したと報じられているところ、この協力とは、アメリカ国内における日本国籍ではない者を日本政府が監視してその情報をアメリカ政府に提供する一方で、日本国内におけるアメリカ国籍でない者をアメリカ政府が監視し、その情報を Xkeyscore に保存することを意味しているものと思われる。そうすると、日本国内における EU 市民は、日本政府の協力の下、アメリカ政府による大規模監視の対象とされている可能性がある。

2 「B. 個人情報保護に係る具体的規定」について

(1) この項目では、「憲法に基づき、かつ憲法の規定を具体化する、個人情報保護法及び行政機関の保有する個人情報の保護に関する法律（行個法）は、民間部門及び公的部門における個人情報についての権利を保障している」と記載されている。

しかしながら、個人情報保護法の立法過程において立法担当者が策定した国会想定問答集では、「法目的に、『プライバシー権』あるいは『自己情報コントロール権』を明記すべきではないか」という想定の問い合わせに対し、「『プライバシー権』や『自己情報コントロール権』という概念については、憲法上明文の規定はなく、その内容、範囲及び法的性格について様々な見解があり、十分な明確性を有するものとは言い難い。」、「したがって、本法案の目的規定においては、『プライバシー権』、『自己情報コントロール権』という文言を用いてはいない」と記載されていた。また、「『プライバシー権』をどのようなものと理解しているのか」という想定の問い合わせに対する答えの中では、「最高裁判例においては、近年、若干の判例の中で『プライバシー』という語が用られているが（マ）、その定義や具体的な内容には触れられていない」と述べていた⁸。このように、政府は、プライバシーの権利が憲法上の権利として確立したものであるという考え方にもしろ懐疑的な見解をとり、個人情報保護法が憲法上の権利を具体化したものであるとする上記政府説明とは相容れない考え方をとってきた。判例においても、開示・訂正・利用停止請求権は、憲法上の権利を具体化したものではなく、あくまでも法律上ないし条例上設けられた権利という位置づけが前提になっている⁹。

このように日本の個人情報保護法は、事業者と行政機関に対する義務規定を列挙し、違反に対する指導等の根拠となる行政法規と位置づけられている。この点で、個人データの保護を保障した EU 基本権憲章 8 条を具体化した立法である GDPR とは根本的な発想が異なっている。

欧州において、個人データへのアクセス権、訂正権、消去権などの諸権利は、EU 基本権憲章 8 条等に明記されたファンダメンタル・ライツ（基本権）の核心（エッセンス）

⁶ <https://theintercept.com/document/2017/04/24/japan-provided-with-xkeyscore/>

⁷

https://www.shugiin.go.jp/internet/itdb_shitsumon.nsf/html/shitsumon/a193263.htm

⁸ JCLU 監視とプライバシープロジェクトチームの所属メンバーが内閣府から情報公開請求により入手した個人情報保護法の法律案想定問答集（国会審議において議員から質問が出た場合に備えて法案を策定した政府が準備する答弁案を記載した内部文書）の問 23 及びその更問

⁹ 最判平成 18 年 3 月 10 日裁時 1407 号 3 頁参照。

をなすものである。これらは単なる行政手続上の仕組みではなく、個人の尊厳に直結する権利として保障されている。これに対し日本では、これらはあくまで個人情報保護法などの法令上付与された請求権にとどまり、基本的な権利という性質は認められていない。この「権利としての格差」は、制度のあらゆる局面に影響を及ぼしている。とりわけ法執行機関や国家安全保障の文脈では、法律上のアクセス権、訂正権、消去権などが極めて制限されていることもあり、決定的な違いを生じさせているように思われる。

（2）またこの項目では、「都道府県警察による個人情報の取扱いについては、個人情報の保護、権利、義務について行個法と同等の内容を規定する都道府県の条例（注：現在は個人情報保護法）により規律されている」との記載がある。

しかしながら、そもそも捜査機関による個人情報の取り扱いについては、取得時のみわずかな規律があるものの、取得後の保存、分析、プロファイリング、行政機関相互の情報提供などに関して法の規律は存在していない。また、EUにおいてファンダメンタル・ライツとされる、データ主体のアクセス権、訂正権、消去権などは、捜査実務における個人データに関する限り、ほとんど全面的に否定されているのが実情である。

また、取得時における規律としても、旧行個法（現個人情報保護法）において、内部の手続を踏めば発することができる捜査関係事項照会（刑事訴訟法 197 条 2 項）によりデータ主体の同意なく自由に個人情報を取得することが可能とされ、また利用目的による制限（個人情報保護法 69 条）等も適用されない。捜査関係事項照会による個人情報の取得に関する情報開示などもなされていない。個人情報保護法による規律は実質的に及ばないに等しい。

なお、かつて、少なくない地方自治体では要配慮個人情報の取得・提供やデータ結合の制限等に関して法よりも厳格な規律を設けていたが、個人情報保護法改正（平成 29 年 5 月 30 日施行平成 28 年法律第 51 号）により、地方自治体が条例で独自の規定を設けることは許されないとするのが個人情報保護委員会の解釈であり、個人情報保護のレベルが低下したとされている。

第2 「II 法執行目的の政府アクセス」（3 頁以下）について

政府報告書のこの項目では、A として政府アクセスの「法的根拠及び制限」が、B として政府アクセスの「監督」が、C として「個人の救済」が記載されている。

1 「A)法的根拠及び制限」（3 頁以下）について

この項目では、1)として「強制的な手段による個人情報の収集」が、2)として「任意協力の要請を通じた個人情報の収集（任意捜査）」が、記載されている。

（1）「1)強制的な手段による個人情報の収集」（3 頁以下）について

この項目では、a)として「法的根拠」が、b)として「制限」が、それぞれ記載されている。

ア 「a) 法的根拠」（3 頁以下）について

（ア）この項目では、冒頭で憲法の規律が記載されている。憲法 35 条が「正当な理由」に基づき、とくに、捜索される場所や差し押さえられる物が示されている令状による限り、これが侵されることはないことを規定しているから、「結果として、犯罪捜

査の文脈における行政機関による電子情報の強制的な収集は、令状によってのみ行われる」との記載がある。

強制的な収集が令状によってのみ行われることは事実である。ただ、その手続を回避して、実務上、「非強制的、任意の収集」に藉口した個人情報の収集が広く行われており、刑事裁判における証拠の大半は任意検査に基づき取得されるものである。照会する側は令状審査を経ずに検査機関内部の手続で任意の照会が可能であり、他方、照会を受ける側の「検査には協力すべき」という社会通念の存在も相まって、「非強制的、任意の収集」の濫用が強く懸念されるのが実態である。

また、令状審査については、対審構造が設けられていないこと、とりわけ電子情報について場所や物の特定が不明瞭かつ包括的なものも許されていることなどから、厳格な審査が行われているとは言い難い。

（イ）政府報告書のこの項目では、「刑事訴訟法第 197 条 1 項によれば、強制の処分は、この法律に特別の定のある場合でなければ、これをすることができない。そして刑事訴訟法第 218 条第 1 項は、犯罪の検査をするにあたり必要があるときにのみ裁判官が発する令状により、差押え等をすると規定している」との記載がある。

しかしながら、検索差押許可状や検証許可状、記録命令等の令状について、2023 年度統計（裁判所の「令和 5 年司法統計年報 2 刑事編」15 頁）によれば、全裁判所において 247,490 の発付件数のうち、却下されたのはわずか 138 件で、却下率は 0.05% とほぼ 100% に近い割合で令状が発付されており、裁判官による審査が機能しているか疑わしい。

令状発令にあたっては被疑事実との関連性が必要とされるが、多くの場合抽象的な関連性のみに基づき、膨大なデータが取得されている。国家主権の観点から国外に所在するデータの取得には一定の限定があるものの、それ以外にデータの形式や内容に関する限定等は存在しない。検査対象者が保有する第三者の個人データを取得することも許されている。

また、手続保障に関する限り、例えば令状の執行にあたり、令状の提示しかなされず、令状の写しが対象者に交付されないことや、差押の対象物件の記載が「ハードディスク 1 個」などと抽象的であることなどから、実質的に不服申立てをする機会が制限されている。なお、いわゆる GPS 検査において、検査官が自ら取り付けた GPS 端末を押収する際に、目録には「衣類等一式」と記載し、その後作成した写真撮影報告書にも「白色塊」とのみ記載して、GPS 端末を利用した検査を隠蔽していたことも明らかとなっている（[東京地判平成 29 年 5 月 30 日判時 2387 号 133 頁](#)）。

2025 年に新たに制定された電磁的記録提供命令では、顧客の個人データを保有する事業者等に対して、令状に基づき検査機関へのデータの提供を命じることが可能となるが、データ主体に対する通知の制度は設けられていない。また、令状発付に合わせて秘密保持命令が付されると、事業者がデータ主体に通知することも禁止される。そのためデータ主体は、検査機関にデータを移転させられても争う機会を与えられない。

データ主体に通知されないという手続上の不備は、あらゆる令状で同様である。例えば、被処分者がハードディスクの差押えを受け、その内部に第三者のデータが多数含まれていたとしても、検査機関も被処分者もデータ主体に通知することはない。また、犯行現場に残された、犯罪と無関係な者の写真、指紋、及び／又は DNA サンプルが採取された場合において、データ主体本人は自らの個人データが取得され、解析され、保存され、プロファイリングにかけられたとしても、知る手段が存在しない。知ることができるのは、

刑事事件として自らが起訴され（犯罪と無関係な者が起訴されることはまずない）、証拠開示を受けた場合などに限られる。現行の法制度ではデータ主体を保護する制度が設けられていない。

このように、データ主体に対する通知という観点では、EDPB が 2018 年 12 月 5 日付で採択した意見（“[Opinion 28/2018 regarding the European Commission Draft Implementing Decision on the adequate protection of personal data in Japan](#)”）（以下「EDPB 意見」という。）のパラグラフ 140 において、EU の法制度では、捜査を妨げるおそれがなくなった時点でデータ主体等の影響を受ける者にデータ取り扱いを通知しなければならないと指摘されていることと、保護のレベルが大きく異なる。

なお、政府報告書では、「通信傍受に関する法律」についても言及している。確かに日本においては、電話等の通話内容にとどまらずそのメタデータもいわゆる通信の秘密に該当するとして、憲法上とりわけ厳格な保護が認められており（21 条 2 項）、それを受け、捜査機関が通信情報を取得するためには、通信傍受に関する法律に基づく特別な令状が必要となる。しかし、法務省の作成資料¹⁰によれば、2002 年から 2022 年の 21 年間にについて令状請求件数と令状発付件数は完全に一致しており、令状発付率は 100% とされている。

(ウ) さらに、項目全体として、個人情報の「収集」に関する法的根拠のみが論じられていることからわかるとおり、日本の法実務において、捜査機関による個人情報の取り扱いについて法的規律が及ぶ対象は、原則として取得の場面のみとされている。取得後の個人情報の取り扱いについて、捜査機関はほぼ法的規律を受けない。[GDPR](#) や [EU 捜査機関データ保護指令（“LED”）](#)においては、個人データの取り扱い（“processing”）は、「自動的な手段によるか否かを問わず、収集、記録、編集、構成、記録保存、修正若しくは変更、検索、参照、使用、送信による開示、配布、又は、それら以外に利用可能なものとすること、整列若しくは結合、制限、消去若しくは破壊のような、個人データ若しくは一群の個人データに実施される業務遂行又は一群の業務遂行を意味する」（GDPR4 条(2)、LED3 条(2)）とされており、捜査実務においても取得にとどまらない広範な取り扱いに規律が及んでいる。これに対し日本では、民間事業者等を規律する個人情報保護法における「取扱い」の概念はある程度広範である一方、その規律は捜査活動には及ばず、それ以外に捜査機関の個人データの取り扱いを規律する法律は刑事訴訟法を除いて存在しない。そして刑事訴訟法では、少なくとも捜査活動に関連する個人データの取り扱いに関する限り、取得さえ適法であれば、その後の「記録」以降のほぼあらゆる取り扱いについて、令状も個別具体的な法的根拠も本人同意もなく行うことが可能とされている。

例えば、DNA サンプルから DNA 情報を抽出し、保存し、別目的で利用することすら、行政内部の規則である「DNA 型記録取扱規則」以外の法的根拠もないまま行われている。その規則の内容としても、取り扱い記録の作成義務も設けられておらず、実際に、少なくとも後から検証できるような形での記録は作成されていないと思われる。DNA サンプルや DNA 型情報の削除要件も後述のとおり明確にされておらず、取り扱いに対する第三者の監督や検証も定められていない。また、刑事訴訟実務上、DNA 型鑑定の実施には令状も本人同意も不要とされている。

¹⁰ 「法施行～令和4年の通信傍受実施状況」（改正刑訴法に関する刑事手続の在り方協議会第6回会議（令和5年4月26日）https://www.moj.go.jp/shingi1/shingi06100001_00089.html 配布資料 21 <https://www.moj.go.jp/content/001395643.pdf>

プロファイリングも同様である。日本の法実務において、プロファイリングは強制手段とされていない。そのため、捜査機関は、いったん個人データを取得さえすれば、まったく法的規律を受けることなくプロファイリングを行うことができる。この点も、GDPR や LED がプロファイリングに関する定義規定を設け (GDPR4 条(4)、LED3 条(4)) 、一定の規律を設けていることと対照的である。日本の捜査機関は、令状も法的根拠も本人同意も得ないまま、自由に収集した個人情報をプロファイリングしている。

これらの当然の帰結として、日本の捜査機関において、個人情報の取り扱いの各過程の記録は、有罪立証に必要な範囲にほぼ限られている。例えば、被告人がマンションのゴミ集積場に投棄したゴミ袋を、本人に無断で捜査官が回収し、中に含まれていたタバコの吸い殻から DNA サンプルを抽出し、DNA 型情報を解析した捜査の違法性が争われた事件において（東京高判令和 3 年（2021 年）3 月 23 日判タ 1499 号 103 頁）、捜査機関は被告人以外の数名に対し同様の捜査活動をしたと認めながら、被告人以外については、ゴミを回収する過程やその後の DNA サンプルの抽出作業、DNA 型データの解析、解析後の DNA サンプルの保管等に関するほぼすべての過程が全く捜査記録として作成されておらず、捜査官の記憶を除き事後検証ができなかったとされている。このような場合、収集された個人データにつき、そのデータ主体が誰で、いつ、どのようにデータとして収集されたものか、収集後に、誰が、いつ、どのような処理を行ったか、現在は誰がどのように保管しているかなどを、事後に追跡することはほぼ不可能となる。このように、GDPR が個人データの処理につき、全て記録し、かつ責任者による説明責任を義務付けていること（30 条）、また、LED が、法執行機関に対して取り扱い記録の文書化と監督機関による監督を義務付けていること（24 条）と、保護の水準が全く異なる。

記録がないため、取り扱いがなされたことを本人を含む外部者が把握することすら困難である。何らかの経緯で取り扱いがなされたことを知り、裁判等で争ったとしても、取り扱いの経緯等について客観的な記録がないため、担当者の証言以外に証拠がなく、充実した審理は期待できない。加えて、捜査機関の個人情報の取り扱いを規律する具体的な法律がないため、外延が不明確な憲法上のプライバシー権などによる規律を求める他なく、裁判所が違法判断を下すことは限られている。

このほかに、遺伝子データ（“genetic data”）、生体データ（“biometric data”）及び健康に関するデータ（“data concerning health”）の取り扱いについて、GDPR 上では（推知情報であるかを特に区別せず）原則として禁止され、LED では厳格な比例原則に服するとされているが、日本では、個人情報保護法において、民間企業等における「要配慮個人情報」としての一定の保護があるにとどまり（なお、「要配慮個人情報」については、個人情報保護委員会が定めたガイドラインにより、推知情報は該当しないこととされており、また、健康診断等の検査結果も医師等が診断した場合だけに限定されるなど、GDPR 上の対応する権利とは内容に違いがある）、捜査機関における特別の取り扱い要請は存在しない。捜査機関は、何らの令状も個別具体的な法的根拠も本人同意もないままに、自由に遺伝子データ等を収集し、保存し、プロファイリングしている。典型的なものは上述したとおり DNA 情報であり、捜査機関は法律の根拠なく、令状審査も受けずに、DNA サンプルを自由に採取し、解析し、データとして保存し、あらゆる捜査に転用している。本人からの開示・削除・修正要請に関する規律もほとんど存在しないに等しい¹¹。取

¹¹ イ(イ)で後述するとおり、「犯罪捜査等に支障を及ぼすおそれがあると当該行政機関の長が認めることにつき相当の理由がある」場合は不開示とすることが認められており、開示が認められる場面はきわめて限られるし、訂正は、データが開示された結果、誤りがあることをデータ主体が認識することが前提になっているから、開示がされなければ利用できないのが基本となる。

り扱い記録も、少なくとも外部から検証できる形では作成されておらず、その監督もされていない。

イ 「b)制限」について

この項目では、(1)として「憲法及び授権された法律による制限」が、(2)として「行個法による制限」が、記載されている。

(ア) 「(1) 憲法及び授権された法律による制限」(4頁以下)について

この項目では、条文による規律として上述した内容が繰り返されているとともに、裁判官による令状発布の考慮要素として、犯罪捜査のために必要があること、罪を犯したことを疑うに足りる状況があること、差押え等の場合の対象の特定などが挙げられている。また、これらの令状審査において、請求者である捜査機関は具体的な証拠書類を提供しなければならず、裁判官が犯罪の嫌疑が十分でないと判断すれば令状が却下されることなどが記載されている。

こうした記載に誤りはない。しかし、捜査差押許可状等について年間却下率が0.05%と極めて低いことは既述のとおりである。これに対し、捜査機関は、裁判官が令状発布を認定するような適切な場合にだけ捜査機関が令状申請をしている結果である、などと主張するかもしれない。しかし、例えば、最終的に検察官自らが犯罪成立の余地がないと判断して起訴取消となつたいわゆる大川原加工機事件においても、裁判官は無批判に捜索・差押え令状を発令していた¹²。このことからわかるとおり、令状審査はほとんど形式化している。

また、個人情報の取得時以外に令状審査がなされないこと、取得後の取り扱いについて記録の作成や監督機関の監督がないこと（新個人情報保護法74条参照）、取り扱いがなされたことを本人を含む外部者が把握することが困難であるため争うことが容易ではないこと、争いとなつても担当者の証言以外に証拠がなく充実した審理がなされないこと、法的規律がないために裁判所が違法判断をすることがほとんどないことなども、既述のとおりである。

(イ) 「(2) 行個法による制限」(6頁以下)について

この項目では、行政機関の個人情報の取り扱いに対する規律として、法律に基づく一般的な記載がなされている。具体的には、保有の必要性（個人情報保護法61条（旧行個法3条））、正確かつ最新情報とする努力義務（個人情報保護法65条（旧行個法5条））、漏洩防止等の必要な措置（個人情報保護法66条1項（旧行個法6条1項））、職員における第三者提供と不正目的利用の禁止（個人情報保護法67条（旧行個法7条））、目的外利用及び第三者提供の禁止（個人情報保護法69条（旧行個法8条））、必要な場合の利用制限等（個人情報保護法70条（旧行個法9条））、苦情対応の努力義務（個人情報保護法

¹² このことは、捜査活動の違法性を問う国家賠償請求事件の裁判資料等から明らかになっている（東京高判令和7年5月28日）。裁判資料等は以下のサイトに格納されている。

[https://www.call4.jp/search.php?type=material&run=true&items_id_PAL\[\]&match+comp&items_id=I0000084](https://www.call4.jp/search.php?type=material&run=true&items_id_PAL[]&match+comp&items_id=I0000084)。なお、大河原加工機事件を報じた英語記事としてBBCのウェブサイトがある（BBC News, "Japan: Police apologise at grave of wrongfully accused businessman," <https://www.bbc.com/news/articles/c0e9jl2182no>（最終閲覧日：2026年1月25日））。

128条（旧行個法48条）である。

これらの記載に誤りはない。しかし、法執行機関に対しこれらの規律はほとんど機能しない。というのも、「法令の定める所掌事務を遂行するため」や「法令に基づく場合」を除く取り扱いを禁止する規律は多くの場面で設けられているものの、裁判所は、法執行機関の個人情報の取り扱いに関し、明らかな私的利用の場合を除き、ほぼ全面的に「個人の生命、身体及び財産の保護」や「犯罪の予防、鎮圧及び捜査」といった、警察法2条1項が定める抽象的な目的に基づく活動であるとして、「法令に基づく場合」などの規律を満たすと認めるためである。例えば、日本に居住するすべてのムスリムまたはOIC諸国出身者の広範かつセンシティブな個人情報を無断で取得し、保有し、プロファイリングに用いた捜査活動の違法性が争われた裁判において、裁判所は、当該「情報収集活動及び収集した情報の保管が、警察法2条1項の定める警察の責務に照らして必要な活動である」とか、「事柄の性質上、国際テロ対策という以上にその目的を明らかにすることは困難」であるから目的を明示する必要はないなどとして、捜査に必要であるという目的があれば法執行機関が外務省や地方自治体などの外部の行政機関と個人情報を共有することを認め、個人情報保護法違反に関する原告らの主張を一律に退けた（東京地判平成26年（2014年）1月15日・判タ1420号268頁）。なお、裁判所はこの判決で、個人情報保護法の一部の規定について、個人の権利を保護するものではないから、その違反は賠償請求の根拠となり得ないとも述べている。

ちなみに、警察法2条1項は、「警察は、個人の生命、身体及び財産の保護に任じ、犯罪の予防、鎮圧及び捜査、被疑者の逮捕、交通の取締その他公共の安全と秩序の維持に当ることをもってその責務とする」という一般的抽象的規定であり、個人データ処理の法的根拠となる具体的かつ明確な法令が不存在な場合に、このような組織法を根拠とした正当化が裁判でも認められている点に留意する必要がある。

その他、保有する個人情報のファイルについて、通常の行政機関は保有に先だって個人情報保護委員会に届け出る義務（個人情報保護法74条1項）及び、法定の事項を記載した帳簿を作成して公表する義務を負うが（同法75条1項）、捜査目的で収集・保有する個人情報については、そのような届出や帳簿の作成・公表義務が免除されているため（同法74条2項2号、75条2項1号）、個人情報保護委員会が犯罪捜査に関する個人情報ファイルについて実効的な監督をすることは実質的に不可能になっている。

同様に、個人が捜査機関の保有する個人情報を開示請求したとしても、「犯罪の予防、鎮圧又は捜査、公訴の維持、刑の執行その他の公共の安全と秩序の維持に支障を及ぼすおそれがあると当該行政機関の長又は地方公共団体の機関が認めることにつき相当の理由がある」場合は不開示とすることが認められており（個人情報保護法78条1項5号（旧行個法14条5号））、実務上、開示請求はほぼ全面的に否定されている。

さらに、捜査機関を含む行政機関等には、民間事業者に課される「個人データの第三者提供」に関する確認及び記録作成義務は課されていない。

また、捜査機関を含む行政機関等については、要配慮個人情報に関して、本人の同意なき取得や第三者提供が認められている（個人情報保護法69条2項2-4号（旧行個法8条2項2-4号））。

このように、行政機関における個人情報保護の程度は、民間事業者よりも緩やかである上、捜査機関に対する規律は幅広く実質的に免除されている。

その上、取り扱いの記録義務やその開示も認められておらず、実質的な救済の可能性は閉ざされている。救済の前提となるデータ主体である本人が自らの個人データ処理がされた事実を知る手段がないため、捜査機関に対する個人情報保護法の規律は、ほとんど

実効性が期待できない。

(2) 「2) 任意協力の要請を通じた個人情報の収集（任意検査）」（7 頁以下）について

政府報告書のこの項目では、a)として「法的根拠」が、b)として「制限」が、記載されている。

ア 「a) 法的根拠」について

(ア) この項目では「個人情報は、自由にアクセスできる情報源あるいは個人情報を保有する事業者からの提供を含む、自発的な情報提供により収集される」との原則が記載されている。

まず指摘されるべきこととして、日本の刑法実務では、「任意」の概念が非常に広く、令状を要する『強制検査』に該当しない検査は、すべて法的に『任意（検査）』と位置づけられる。この法的な分類は、対象者の協力が自発的になされたものであること、あるいは真の自由意思に基づいていることを保証するものではない。

また、任意に情報を取得する対象として、被疑者・被告人など本人も含まれている。そのため、被疑者が身体拘束を受け、被疑者側からは義務ではないかと誤信するような状況下で提供された証拠についても、任意のもと収集された証拠として用いられる。これは LED が、前文 35 において検査機関と検査対象者との非対称性を強調した上で、データ主体には「真正かつ自由な選択肢がないため」（“the data subject has no genuine and free choice”）同意を法的根拠とすることは原則として許されないとし、明文規定としてもセンシティブデータの取り扱いが許される根拠から本人の同意を明確に除いていることと対照的である（LED10 条¹³）。

例えば、ある事案では、被告人が保釈を請求したのに対し、検察官が、押収されたパソコンやスマートフォンなどのデバイスのパスコードを被告人が任意に開示していないことを理由に保釈に反対し、裁判所も保釈請求を却下した。被告人が保釈を得るためにパスコードを開示するしかないと判断し、数か月の身体拘束の後にやむなくパスコードを開示し、実際にその直後に保釈された事案について、裁判所は、この開示は任意になされたもので、その開示の適法性に影響は生じないと判断している（東京高判 2025 年 9 月 16 日判例集未登載（令和 5 年（う）第 676 号事件））。自白に関連しても、最高裁は任意の概念をきわめて広く捉えており、例えば任意同行後に、検査機関が警察署付近の宿泊施設に 5 日間にわたり被疑者を宿泊させ、取調べを続けるという検査手法の違法性が争われた事案において、任意の検査として適法であると判断している（最決昭和 59 年 2 月 29 日刑

¹³ LED10 条の条文は次のとおり。”Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be allowed only where strictly necessary, subject to appropriate safeguards for the rights and freedoms of the data subject, and only:

(a) where authorised by Union or Member State law;
(b) to protect the vital interests of the data subject or of another natural person; or (c) where such data have manifestly been made public by the data subject.

集 38 卷 3 号 479 頁（高輪グリーン・マンション事件））¹⁴。

逮捕されることを恐れてやむを得ず応じる場合も同様である。実務上多くの場合で、任意の取り調べとして警察署に呼び出された被疑者が、写真撮影・指紋採取・DNA サンプルの採取等を求められ、逮捕されることを恐れやむを得ず応じる場合でも、「個人の意思を制圧」する場合にあたらないとされている（2023 年 2 月 17 日名古屋地裁判決等参照）。取得後にどのようなデータ処理をしようとデータ主体に通知もなされないことは既述のとおりである。警察が保有する DNA や指紋のデータベースにはこのように「任意」として採取されたものが多数含まれている。

一度提出した情報を削除することは極めて困難である。任意による証拠提供であっても撤回することは認められていない。刑事裁判において任意に提供された証拠の証拠能力を争う場合も、任意性がないことを事実上被疑者・被告人側で明らかにしなければならない。

（イ） 政府報告書のこの項目では、任意に基づく情報収集として、実務上多く用いられる「検査関係事項照会」（刑訴法 197 条 2 項）という制度が紹介されている。

検査機関が検査に必要な情報につき、書面で民間事業者に対し任意の提供を求めるもので、通信企業・民間企業や医療機関、教育機関、宗教機関、公的機関等に対し、幅広く行われている。

検査関係事項照会を受け取った事業者が、これに応じて個人情報を提供した場合、本人の同意も令状もなくとも、個人情報保護法における第三者提供の適法要件の一つである「法令に基づく場合」（27 条 1 項 1 号）に当たるとして、原則として法的責任を負わない。

政府報告書では、「プライバシー権や、かかる照会による負担への個人の意識の高まりを背景に、事業者において、かかる照会への回答がより慎重になされる傾向が顕著となっている」と記載されている。

しかしながら、検査関係事項照会制度は、令状を取得することなく、広範かつ膨大な個人情報を取得する迂回制度として機能しているというのが実情である。

そもそも検査関係事項照会においては、個人情報を必要とする理由が一切記載されない。後述（本レポート 14 頁及び末尾別紙）のとおり、書面には「検査に必要なため」以上の具体的な情報が記載されていないため、受領した民間事業者は、提供の必要性を検討することができず、提供を拒絶するかどうかを個別具体的に判断できない。そのため、多くの事業者では、求められた個人情報の種類や形式に着目して機械的に対応している。そして、仮に提供を拒み、後に令状に基づき強制検査を受けると業務に多大な支障が生じる一方で、提供したとしても、個人情報保護法上、法令に基づく個人データの第三者提供の場合に該当するとされ、提供は合法と考えられることから、事業者がデータ主体から損害賠償を受けるリスクは極めて低いとされている。また、日本においては、令状または検査関係事項照会に基づき個人情報を提供したデータについて開示する、いわゆる透明性レポート制度を導入する企業の数が極めて限られており¹⁵、幅広く検査関係事項照会に応じて

¹⁴ 他の例として、最高裁 1989 年 7 月 4 日第三小法廷決定（刑集 43 卷 7 号 581 頁、判時 1323 号 153 頁、判タ 708 号 71 頁）では、自白の任意性判断において任意同行後の被告人に対する合計 22 時間にわたる取調べが任意検査として許容されるかが問題となつたが、適法であるとされている。

¹⁵ 2025 年 5 月時点での透明性レポートを確認できた国内企業としては次のものがある。

LINE ヤフー株式会社 <https://www.lycorp.co.jp/ja/privacy->

個人情報を捜査機関に提供したとしてもそのことが公になることがない。そのため、開示に応じた場合のリスクがほとんどないことも相まって、実際の必要性を度外視し、幅広く開示に応じる民間事業者が多いのが実情である。

その典型的な事例として、いわゆる CCC 事件がある。これは、欧州委員会による、日本に対する十分性認定の定期レビューにおけるコミッショナ・スタッフ・ワーキングドキュメント (4.2.1) においても指摘されているもので、カルチュア・コンビニエンス・クラブ株式会社 (CCC) という共通ポイントサービスなどを主な事業内容とする会社が、ポイントカードの利用履歴を含む膨大かつ広範な個人データを、捜査関係事項照会に基づき捜査機関に任意に提供していたことが明らかとなった事件である。この任意提供の事実は、2019 年に報道機関の独自調査によって明らかになるまで、捜査機関においても CCC においても開示されることはなかった。報道を受け、当初、CCC は適法性を強調していたが、後に少なくとも GDPR の十分性に反する事例であるとの指摘が相次ぎ、外部の有識者による第三者委員会を組成して検証を行い、透明性レポートを公表するなどの対応策が公表された。

しかし、刑事弁護実務などで捜査機関から開示された証拠を見る限り、CCC 以外の多くの企業においても同様の取り扱いがなされていると思われる。開示制度や監督制度がないために、捜査関係事項照会に基づく民間企業からの個人情報の任意提供がどの程度の規模、頻度、内容で行われているか、外部において正確に把握することはできない。本決定の案に対して EDPB 意見のパラグラフ 150～152 では、捜査関係事項照会の数や種類、回答に関する情報がないこと等を指摘し、それゆえ、EDPB としての評価ができない旨指摘したうえで、欧州委員会に対して、それら情報をモニターするよう求めている。日本政府として、捜査関係事項照会に基づく個人データ取得の正当性を主張するのであれば、外部から検証可能なように、関連する情報を公表すべきである。なお、現時点でも捜査関係事項照会による広範な情報収集を規制する具体的な法律の規定はない。

上記コミッショナ・スタッフ・ワーキングドキュメント 4.2.1 は、捜査関係事項照会書に関する警察庁の通達に言及している。そこでは、既定の書式によって照会が行われるとされていること等について肯定的評価がなされている。しかし、捜査関係事項照会書の既定の書式¹⁶はきわめて簡易なもので、記入欄のつくりなどによって具体的な捜査や必要性を担保しやすい構造にはなっているとは言えない。添付照会書の書式のとおり、「捜査のため必要があるので、下記事項につき至急回答願いたく」とのみ記載されているのが実情である。同通達では、「照会件数及び照会事項は必要最小限度にとどめること」と記載されている（2 照会要領（3）留意事項イ）。しかし、実際の運用が適正に行われているかは警察内部の統制に委ねられており、外部からは不明である。

（ウ）その他、任意捜査に関する指摘事項を以下列記する。

近年、捜査機関は、イスラエルの企業 (Cellebrite 社) が開発したソフトウェア

securityprivacytransparency/

CCC 社 <https://privacy.cccmkhd.co.jp/news/2076/>

株式会社メルカリ <https://about.mercari.com/safety/transparency/>

Paypay 株式会社 <https://paypay.ne.jp/privacy/disclosure/>

さくらインターネット株式会社 [https://www.sakura.ad.jp/corporate/wp-](https://www.sakura.ad.jp/corporate/wp-content/themes/sakura-corporate/assets/pdf/TransparencyReport2023H1.pdf)

サイボウズ株式会社 <https://cybozu.co.jp/privacy/disclosure-policy/transparency/>

¹⁶ 本レポート末尾に別紙として書式を掲載した。

を利用し、押収したコンピュータ、ラップトップ、タブレット、携帯電話、ハードディスク等のデータ保存媒体について、パスコードを経由することなく、情報を収集する検査手法を確立している¹⁷。当該ソフトウェアの利用やデバイスからの情報抽出について、個別の法律の規定は存在せず、警察法 2 条の包括規定で対応している。令状審査も必要とされていない。抽出された情報をどのように用いるかにつき、なんらの規律も存在しない。なお、技術上は、パスコードロックの解除後に、デバイスからインターネットを経由して各種クラウドサービスにアクセスし、情報を抽出することも可能である。国外のクラウドサービスに関しては検査主権等の問題から一定の限界があるものの、判例は、記録媒体がサイバー犯罪条約の締約国にあり、かつ「記録を開示する正当な権限を有する者の合法的かつ任意の同意がある場合」には、「国際検査共助によることなく」、強制処分としての「リモートアクセス及び同記録の複写」を行うことができると判断している（最決 2021 年 2 月 1 日刑集第 75 卷 2 号 123 頁）。この判断はあくまで強制処分におけるものだが、同最決はこの事件について、「関係者の任意の承諾に基づくものとは認められないから、任意検査として適法であるとはいえないとも述べており、同意に基づくものであれば任意検査として自由に行えることを前提としている。記録媒体がサイバー犯罪条約の締約国内にあって、記録を開示する権限を有する者から任意の同意があれば、主権の問題はクリアできることと判断していることに照らすと、すでに任意検査にも転用されていると考えられる。いずれにせよ検査手法が全く公開されないため、外部から監督する手段がない。

同意については、既述のとおり検査実務も裁判実務も、GDPR や LED とは相当異なる判断枠組みを用いている。前掲 2025 年東京高判では、東京高等裁判所は、「電磁的記録媒体にパスワードがかけられるなどしてロックされている場合に、使用者の同意を得てパスワードの提供を受けることは執行への任意の協力」として適法であるとした上で、開示によって、検査機関がデバイス内の情報にアクセスすることとなることは当然理解している以上、「保釈を得る目的を有していたこと」や、「結果的に被告人が考えていた以上の犯行が発覚したこと」などは同意の効力に影響を及ぼさないと述べている。典型的な人質司法（罪を認めない被疑者・被告人を長期間にわたり身体拘束することで、事実上その身体を人質として自白や有罪判決を得ようとする日本の刑事司法の実務運用の批判的表現）。の状況において、保釈と引き換えになされた“同意”に基づく検査すら、任意検査と位置付けられている。

検査機関は、公道のゴミ集積所やマンションの共用部分におけるゴミの取得をすべて任意検査として行っている。裁判所もそのような検査を適法としている。例えば前掲令和 3 年東京高判では、検査機関がゴミとして捨てられたたばこの吸殻から本人の承諾なく DNA サンプルを採取し、鑑定して DNA 型の同一性を確認した事例について、裁判所は、吸殻の証拠能力を肯定したうえで、検査機関は、被告人の DNA 型を把握し、犯人の可能性がある者の DNA 型との同一性を確認したにすぎない（被告人の DNA サンプルから遺伝情報や生来情報を検出してそれを検査に利用したわけではない）から適法であると判断した。このように、検査機関は具体的な犯罪の嫌疑がほとんどなくとも、例えば同種前科

¹⁷ 日本経済新聞の記事などで明らかにされている

(<https://www.nikkei.com/article/DGXMXZ040837750S9A200C1CC1000/>最終閲覧日 2026 年 1 月 25 日)。なお、警察庁が公開する随意契約企業及び製品一覧には、同社の製品等が掲載されている (https://www.npa.go.jp/news/procurement/npa/chotatsu_kouhyo/02_buppin_zuikexl 最終閲覧日: 2025 年 1 月 25 日)。

があるというだけで、自由にゴミを取得し、DNA サンプルを採取し、解析に用いてデータベースとすることができます。

なお、2025 年 9 月、佐賀県警察科学捜査研究所において、長年にわたり DNA 型鑑定を実際には実施していないにもかかわらず過去の別事件の鑑定資料を用いて実施したように装うといった捏造などの不正が行われていたことが発覚した。この件に関連して警察庁による特別監察が行われているものの、日本弁護士連合会（「日弁連」）等が要望している中立的第三者による検証は実施されていない¹⁸。これまでにも捜査機関による証拠の改ざんがあったことを踏まえ、鑑定資料を含む犯罪捜査の記録を管理及び保管することを義務づける法律の制定を求める意見が日弁連から出されるなどしているが、外部の第三者機関の設置や新たな監督制度の創設に関する議論はなされていない。前述のとおり、犯罪の捜査に関連した個人情報ファイルの保有については、個人情報保護委員会への通知を免除されており、帳簿の作成や公表も免除されているから、DNA のデータベースについて、外部からデータ登録や統計処理等に關しその正確性は検証する方法は存在しない。

判例は、都道府県警察が警察法 2 条に基づき、「公共の安全と秩序の維持」のために情報収集活動をすることを認めており、都道府県警察は、具体的な犯罪の嫌疑がなくとも、民間企業から個人情報を含む情報を提出させている。その情報収集の対象範囲は極めて広く、暴力的な活動に従事する団体に限らない。裁判例として、名古屋高裁 2021 年 9 月 13 日判決（大垣事件）が挙げられる。この事件では、岐阜県警が、風力発電所の設置を計画した電力会社と協力して、計画に反対する住民の情報を電力会社に提供し、また電力会社から提供を受けていた。このような情報の提供・収集も、基本的には「任意」のものとして行われている。この事件では、例外的かつ偶発的に該当する警察活動が明るみに出たために、裁判が可能となった。しかし、一般に「公共の安全と秩序の維持」に関する活動は、全く情報公開されず、「開示することにより、犯罪の予防、鎮圧又は捜査、公訴の維持、刑の執行その他の公共の安全と秩序の維持に支障を及ぼすおそれがあると当該行政機関の長又は地方公共団体の機関が認めることにつき相当の理由がある情報」は不開示とされるため（個人情報保護法 78 条 1 項 5 号）、本人によるアクセス権も認められない。また、公安警察活動に対して情報公開制度はほとんど機能しておらず、議会や公安委員会による監督制度もほとんど機能していないため、全国で類似の活動が行われていることは想像に難くないが、その点の検証は不可能である。

イ 「b) 制限」（8 頁以下）について

（ア）「(1) 憲法及び授権された法律による制限」（8 頁以下）について

政府報告書のこの項目では、憲法 13 条の趣旨を踏まえた最高裁判例として、学生のデモ活動を警察が写真撮影することの適法性が問われた京都府学連事件（最大判 1969 年 12 月 24 日刑集 23 卷 12 号 1625 頁）と、パチンコ店前に設置した監視カメラを利用した捜査活動の適法性が争われた事件（最判 2008 年 4 月 15 日刑事判例集 62 卷 5 号 1398 頁）を引用している。その上で、これらの判例で指摘された要素が任意捜査一般に求められる要

¹⁸ 日弁連「佐賀県警察科学捜査研究所の職員による DNA 型鑑定に係る不正行為に関する会長声明」（2025 年 9 月 29 日）

素であると整理し、その限界について「犯罪の嫌疑」、「検査の必要性」、「方法の相当性」の「3 基準を踏まえ、一般的に、社会通念に従って相当といえるか否かという観点で判断」されるとしている。また、3 つの要素のうち「検査の必要性の要件は、刑事訴訟法 197 条から直接導かれる」だけでなく、「警察庁から都道府県警察宛てに発出された通達においても確認されて」おり、当該通達が「検査の目的のために必要な場合にのみ検査関係事項照会を行う旨を含む多くの手続上の制限を定めている」こと、刑事訴訟法 197 条第 1 項が「過去に起きた犯罪に関する具体的な嫌疑がある場合にのみ適用され」、「違法行為がいまだ行われていない個人情報の収集と利用に関係するものではない」ことなどが記載されている。

まず指摘すべきこととして、任意検査における「犯罪の嫌疑」は極めて広い運用が認められている。例えば、東京地判 2022 年 3 月 10 日は、組織法である警察法において、「警察は、個人の生命、身体及び財産の保護に任じ、犯罪の予防、鎮圧及び検査、被疑者の逮捕、交通の取締その他公共の安全と秩序の維持に当ることをもってその責務とする」

（2 条 1 項）と定めていることを根拠として、停車中の運転席に座っていた市民が、警察車両を見て、「すぐに真下に視線をそらしたように見えた」という警察官の主観的な判断をもとに声をかけて質問することは、「対象者の任意の協力を求める形で行われ、対象者の自由を不当に制約することにならない方法、態様で行われる場合には適法性が認められる場合がある」とし、「犯罪の予防その他公共の安全と秩序の維持」に当たる活動として許されるとしている。もちろん、任意検査である以上、その人物に対する強制力の行使は許されないが、任意検査が抑制的に行われているかのような政府報告書の記載には疑問を呈さざるを得ない。

また、検査関係事項照会には、既述のとおり、検査機関の内部統制以外に規律はない。民間事業者等は「検査の必要のため」以上の情報は得られず、その必要性を検証することはできない。刑事裁判において開示されるものは当該事件と関係する検査関係事項照会書とその結果のみで、起訴されなかった事案に用いられた照会書は一切外部に開示されない。そのため、検査関係事項照会制度が、例えば政治目的や経済目的など犯罪検査と無関係に用いられたとしても、制度上これを規律し是正する手段はない。

照会によって得た情報を別の事件に用いることも全く禁止されていない。そのため、「過去に起きた犯罪に関する具体的な嫌疑がある場合にのみ適用され」とあるものの、全く別の微罪を理由として情報を取得し、その情報を「公共の安全と秩序の維持」目的として用いることも許されている。実際、検査関係事項照会で得た情報を他の情報と併せてデータベースに登録して検査機関内でプロファイリングしていた例も発覚している。例えば、前述したムスリムを監視する検査手法では、民間企業や大学、金融機関から検査関係事項照会により得られた情報を、ムスリムを管理するデータベースに登録していたことが流出資料から裏付けられている。その他、多数の民間事業者等に散在する個人情報を、検査関係事項照会の名目で取得し、そのすべての情報をデータベースに統合して、行動様式や信仰内容などをプロファイリングすることが実際に行われていた。ムスリム検査の違法性を争った裁判でもこのような検査手法が適法とされたため、検査機関のこのような活動を制御する方法は、現時点では存在しない。

EDPB 意見パラグラフ 77 では、「個人の権利（特にアクセス権、訂正権及び異議申立権）に対する制限が、民主主義社会において必要かつ比例的であり、基本的権利の本質を尊重するものであるか否かについて、欧州委員会からの保証を求める」とある。ここで

任意検査の限界として述べていることは、アクセス権等の問題ではないものの、日本における個人の権利に対する制限が、「必要かつ比例的」とは言えないことを示している。

監視カメラ等について、政府報告書では、裁判例を引用し適正に用いられているかのように記載されているが、いくつか指摘されるべき事項がある。まず、監視カメラ等を利用して個人データを処理することを具体的に認める法律は存在せず、検査機関自身における監視カメラ等の利用に関する具体的な法律も存在しない。また、検査機関が民間事業者等から監視カメラ等の映像・画像・音声を取得することについても、具体的な法律は存在しない。検査機関は検査関係事項照会等により、個人データの処理について規定した法律という具体的な根拠規定なしに、個人データを取得し、保存し、データベース化することができる。監視カメラの性能等についてもいかなる規律もない。顔認証機能付きかどうか、自動追跡機能があるか、IP アドレスが付されているかどうか、リアルタイムで情報を取得するものであるかどうかなど、どのような性能であろうと自由に利用することができる。これは検査機関自身が設置するものであれ、民間事業者等が設置したカメラの情報を取得する場合であれ、同様である。実際、検査機関は商店街や自治会等に対しても監視カメラの設置を促進する取り組みを行っているが、これについても具体的な法律の根拠はなく、どれほどの監視カメラを活用しているか、データ取得の際の具体的な手続（取得に際して検査関係事項照会を用いているなど）、取得したデータはどのように管理しているかなど、その他具体的な運用実態は全く不明である¹⁹。すべて任意検査の限界という抽象的な規律に基づき実施されている。前述のとおり、検査機関が保有する個人情報ファイルについての通知制度がないため、本人は自らの個人データの存在の有無について知ることができず、また、情報公開もないため、裁判等で争うことでも困難である。

（イ）「(2) 特定の事業者に係る制限」（9 頁以下）について

政府報告書のこの項目では、通信事業者や電気通信事業者など、特定の事業者について追加的な制限がかかることが記載されている。これらの事業者は、原則として第三者に個人情報を提供できず、特に任意検査に基づく照会には応じられないと記載されている。さらに、法令で開示が禁止されている場合（例：刑法 134 条の秘密保持義務）には、事業者は任意協力要請を拒否しなければならないとも記載されている。

この項目の記載に特段指摘すべき事項はない。

（ウ）「(3) 行個法に基づく制限」（10 頁以下）について

政府報告書のこの項目では、行個法において、行政機関における個人情報の収集及び取扱いについては、前記 II. A. 1. b) (2) ((2)行個法による制限)の項において説明するような制限が設けられていると記載されている。なお、同様の制限が、都道府県条例により設けられており、都道府県警察にも適用される。

同項目（前記 II. A. 1. b)(2)）で指摘した内容がここでもあてはまる。

¹⁹ 日本弁護士連合会「監視カメラに対する法的規制に関する意見書」(2012年(平成24年)1月19日付)
https://www.nichibenren.or.jp/library/pdf/document/opinion/2012/120119_3.pdf

2 「B) 監督」（10 頁以下）について

（1）「1) 裁判所による監督」（10 頁）について

政府報告書は、「強制な手段により行われた個人情報の収集に関して、これらは令状に基づかなければならず、裁判官による事前審査に服することになる」と述べており、本決定では、「それらの場合における収集は、厳格な『正当な理由』の基準に基づき、裁判官によって事前に審査される。」と結論づけている（本決定前文 132 項）。しかし、本レポート 6 頁「ア『a) 法的根拠』（3 頁以下）について」で述べたとおり、「非強制的、任意の収集」に藉口した個人情報の収集が広く行われており、また、令状審査を受けた場合であっても、厳格な審査が行われているとはい難い²⁰。政府報告書は、「当該捜査が違法であった場合、裁判官はその事案の後の刑事裁判において係る証拠を排除することができる。個人は、捜査が違法であると主張する自身の刑事裁判において、その排除を要請することができる」として、捜査の違法性があれば証拠排除が可能であるかのように述べている。

しかし、判例上、証拠能力がないとして証拠排除されるためには、単に捜査の違法性があるというだけでは足りず、令状主義の精神を没却するような重大な違法があり、これを証拠として許容することが将来における違法な捜査の抑止の見地からして相当でないと認められる場合に限られている（最判 1978 年 9 月 7 日刑集 32 卷 6 号 1672 頁）。しかも、令状主義を没却するかどうかにおいて、裁判所は警察官らの主觀を重視しており、実質的には警察官らが意図的に令状主義を没却しようとした場合を除いて証拠排除されることはない（最判 2022 年 4 月 28 日刑集 76 卷 4 号 380 頁など）。また、既述のとおり、裁判所が任意捜査の限界と判断することも極めて稀である。現実の証拠排除のハードルは極めて高く、政府報告書はこのことに全く触れていない。

（2）「2) 行個法に基づく監督」（10 頁以下）について

政府報告書には、各行政機関の長が自らの機関における行個法の施行を監督する権限を持っているが、同時に総務大臣にも監督的な役割が与えられ、総務大臣は、行個法の施行状況や苦情処理、総合案内所への照会を通じて必要があると判断した場合、行政機関の長に対して資料や説明を求めることができるほか、個人情報の取扱いに関して意見を述べることができるとの記載がある。また、法違反や不適切な運用が疑われる際には、行個法に基づく措置を講じて改善を促すことが可能であり、これにより、各行政機関における個人情報の取扱いが適法かつ統一的に運用されることを確保するのに役立つとの記載がある。なお、これらの記載のうち、「総務大臣」とあるところは、2022 年 4 月施行の個人情

²⁰ 指宿後掲論文 61 頁は、この点に関する政府報告書について、「はかなくも GPS 大法廷判決が、令状による事前審査方式ではいかなる位置情報がどの程度取得されたかを統制できないと、明白に指摘していました。それを知りながらこんな回答をしている」と批判する。指宿論文が指摘する「GPS 大法廷判決」（2017 年 3 月 15 日最高裁大法廷判決・刑集 71 卷 3 号 13 頁）は、「GPS 捜査は、GPS 端末を取り付けた対象車両の所在の検索を通じて対象車両の使用者の行動を継続的、網羅的に把握することを必然的に伴うものであつて、GPS 端末を取り付けるべき車両及び罪名を特定しただけでは被疑事実と関係のない使用者の行動の過剰な把握を抑制することができず、裁判官による令状請求の審査を要することとされている趣旨を満たすことができないおそれがある」などと指摘し、GPS 捜査について、刑訴法が規定する令状を発付することへの疑義を表明している。最高裁は、そのうえで、「[GPS 捜査]の特質に着目して、憲法、刑訴法の諸原則に適合する立法的な措置が講じられることが望ましい」との判断も示しているが、いまだ立法的措置はとられていない。

報保護法改正により、「個人情報保護委員会」に改められた。

この項目における記載自体に誤りはない。ただ、実際には、警察組織や公安調査庁、防衛省などに対する規律はまったく機能していない。その意味でこの記載は事実と異なる。なぜならば、原則として行政機関が個人情報ファイルを保有しようとするときは、当該行政機関の長は、あらかじめ、個人情報保護委員会に対し、通知しなければならないとされているものの（個人情報保護法 74 条 1 項）、同法は「国の安全、外交上の秘密その他の国の重大な利益に関する事項を記録する個人情報ファイル」、「犯罪の捜査、租税に関する法律の規定に基づく犯則事件の調査又は公訴の提起若しくは維持のために作成し、又は取得する個人情報ファイル」について、通知義務を免除しているため、個人情報保護委員会の監督対象から除外されており（74 条 2 項 1 号及び 2 号）、また、行政機関の長が行個法の施行を監督する権限を行使して個別の対応をした事例はきわめて限られているからである。すなわち、1999 年から 2000 年にかけて発生した一連の警察不祥事（神奈川県警における警察署集団警ら隊（当時）内部での集団暴行事案、覚せい剤使用事案の隠蔽など）を受けた警察改革により、2012 年 12 月の警察法の改正がなされ、公安委員会の警察に対する監察の指示権が規定され、一時は、実際にこの指示がなされた事例があったが（たとえば平成 18 年版警察白書 249 頁注に具体例のきわめて簡単な記載がある）、その後は下火になり、昨今の警察白書では、監察の指示権があるという抽象的権限が記載されるだけになっている。

例えば、既述のとおり、警察庁において、ムスリムを対象とした大規模な情報収集活動を行い、その大量の検査資料がインターネットに流出した事件があった。この流出資料が、警察庁が作成して保管していたものであることは裁判所において認定されている。明らかな個人情報管理に関する重大な事故であったが、これに対しても、当時の総務大臣はなんら対応していない。また、前述したとおり、岐阜県警が風力発電計画に反対する市民を監視し、電力会社と個人情報を共有していた事実が裁判所で認定されているが、これについても岐阜県が岐阜県警に対し何らかの対応をとったことはない。その他自衛隊情報保全隊による情報収集活動や、警察組織による市民のデモ活動の録画、CCC 事件など、多数の個人情報の取り扱いに関する違法・不当な活動が指摘されてきたが、個人情報保護法（旧行個法）に基づき、監督機関が何らかの対応をとったことは一度もない²¹。

（3）「3）警察における公安委員会による監督」（11 頁以下）について

政府報告書では、日本の警察行政について、警察庁が国家公安委員会、都道府県警察が都道府県公安委員会の管理をそれぞれ受け、民主的運営と政治的中立性を確保していること、国家公安委員会は警察庁長官の任命や大綱方針の策定などを担い、都道府県公安委員会は住民代表で構成される独立した合議制機関として都道府県警察を管理することが記載されている。また、都道府県公安委員会の委員は知事が議会の同意を得て任命し、任期や罷免要件が法律で定められており、政治活動の制限によって独立性と中立性が守られていると記載されている。さらに、都道府県公安委員会は、警察活動の報告を定例的に受け、大綱方針を示して指導を行うほか、必要に応じて具体的な事案に指示を出したり、その

²¹ 後掲指宿論文 62 頁は、「総務省の方が一度でも警察の個人情報収集について総務省が指導した実績があるとご存知であれば教えていただきたいんですが、寡聞にして知りません。これも十分性認定としては十分ではないでしょう。」と指摘する。

履行状況を点検したりする権限を持つとの記載もある。

この記載自体に誤りはない。法制度上は、中立的な監督制度が設けられているよう見える。しかし、実質的には機能していない。これまで述べてきたように、警察組織においては個人情報の取り扱いに関して様々な問題が認識されているが、裁判所の判断を待たずに、公安委員会が監督権限を行使して都道府県警察に対して警察が保有する個人データについて調査したり、抹消を命じた例は見当たらない。大垣事件では、個人情報の抹消を命じた名古屋高等裁判所の判決に基づき、2024年に岐阜県警察が同県公安委員会委員長の立ち会いの下で情報の抹消をした例が報じられたが、このような例は極めて稀な事例と言われている。また、東京都公安委員会が、警察が設置する街頭カメラに関して、「犯罪の捜査その他警察の職務遂行のため活用」した場合にその旨を公安委員会に報告するものと定めた例はあるが²²、公安委員会がデータを確認したり、抹消を求めたりする定めは無く、公安委員会に自分の画像が保存されているかについて個人が公安委員会や警察に確認を求めたり抹消を求めたりできる旨を定めた規定はない。2025年に、佐賀県警科学捜査研究所の職員が、DNA型鑑定において、実際は鑑定していないのに鑑定したように装うなどの不正行為をしていた問題が発覚した際も、佐賀県公安委員会は独自の調査を行うことは無く、佐賀県警からの報告を受けるだけであった。佐賀県公安委員会が公表した再発防止の提言も、警察庁から佐賀県警に対する重点的な業務指導を求める内容であって、公安委員会として独自に調査・確認する権限を有することの記述は無く、そのような権限行使することについての提言も無かった。

このことは制度上の問題に由来する。まず、公安委員会に独自の予算はほとんどない。そのため独立した専門家を構成員とすることはほとんど期待できない。警察法においても、公安委員会の庶務は監督対象である警察庁及び都道府県警察が担うとされており（警察法13条及び44条）、公安委員会独自の事務局は存在しない。実際には警察が公安委員会の仕事を代行しているに等しい状況にある。

日本弁護士連合会が実施した調査²³によれば、都道府県の公安委員会委員の多くは、「会社役員」や「銀行・信金等金融関係」といった財界・企業関係者が選ばれている。ほかに「大学・教育関係」「医師・医療関係」がつづき、平均年齢は67歳である。議会の同意を得て知事が任命するが、それ以前に警察が同意できる人物が条件といわれており、警察の組織的な違法・不当な活動を監督する能力と意欲を有する委員は限られている。EDPB意見書パラグラフ173は、監督機関の完全性、中立性及び独立性について触れているが、都道府県の公安委員会が、これらの点に関するEUの要求水準を満たしているかは疑問である²⁴。

²² [平成14年\(2002年\)2月21日付東京都公安委員会規程第1号「街頭防犯カメラシステムに関する規程」5条及び6条](#)

²³ 第45回(2002年)人権擁護大会シンポジウム第1分科会基調報告書「だいじょうぶ?日本の警察—いま市民が求める改革とは」80頁

²⁴ 指宿後掲論文62頁は、「警察は『独立した審査を受けている』というふうに言っています。けれども、その審査をする『都道府県公安委員会』、Prefectural Public Safety Commissionsが監督して個人の権利や自由をきちんと守っているとの認定については、そんな実態はありません」、「各都道府県の公安委員会の議事録を見ても、警察が収集した個人情報についての報告は行われていません。議事録にそういう記載がないんです。ないにもかかわらずどうして独立した審査を受けていると言えるのか」と「公安委員会による監督」に疑義を呈している。

（4）「4）国会による監督」（12 頁以下）について

政府報告書では、「国会には国政調査権があり、国会は、公的機関の活動に関連して調査を行い、この目的のために書類の作成と目撃者の証言を求めることができる（憲法 62 条）。この文脈において、国会における所管委員会等の場において、警察の情報収集活動の是非について検証することができる」との記載がある。さらに国会法により、「内閣及び公的機関に調査を行う上で必要となる報告や記録の作成を求め」たり、国会議員が質問主意書を提出して内閣に回答を求める 것도でき（国会法 74 条・75 条・104 条）、過去には、行政機関による個人情報の取り扱いを対象とした質問主意書も存在しているとの記載もある。

しかし、国会に「個々の強制捜査で収集された個人情報の管理を独立して監督する権限はない」²⁵。さらに、実態として、捜査機関や安全保障機関の個人情報の取り扱いに関する、政府はほとんど実質的な答弁をしない傾向にある。例えば、行政機関による個人情報の取り扱いを対象とする質問主意書として、脚注に挙げられるのがデータベース上確認できるか²⁶、そのすべてにおいて、すでに公開されている統計データの開示を除き実質的な答弁はなされていない。捜査機関の情報の取り扱いに対する国政調査権の実効性は極めて限定的である²⁷。

3 「C)個人の救済」（13 頁以下）について

（1）「1)令状に基づく強制的な情報収集に対する司法救済（刑事訴訟法第 430 条）」（13 頁以下）について

政府報告書には、刑事訴訟法 430 条 2 項により、令状に基づく差押え（個人情報を含む）に不服がある場合、管轄裁判所に対して処分の取消や変更を求める準抗告を提起することができるとの記載がある。この手続は事件の終結を待たずに行うことができ、裁判所が差押えの必要性がないと判断した場合や手続が違法と認められる場合には、処分の取消や変更を命じることが可能であるとの記載もある。

この記載自体に誤りはないが、実効性は極めて低い。なぜならば、当事者の適正な

²⁵ 後掲指宿論文 61 頁

²⁶ ・「情報公開請求者の『応接記録』に関する質問主意書」（平成 14 年 7 月 31 日）
・「政府が保有する個人情報の管理体制に関する質問主意書」（平成 16 年 5 月 26 日）
・「個人データ流出に関する質問主意書」（平成 16 年 7 月 30 日）
・「難民認定申請者の個人情報に対する守秘義務に関する質問主意書」（平成 17 年 6 月 22 日）
・「デジタル庁が十月二十六日に基本契約を行った AWS に関する質問主意書」（平成 21 年 3 月 27 日質問第 92 号）
・「自衛隊による住民基本台帳閲覧及び個人情報の収集に関する質問主意書」（平成 26 年 9 月 29 日）
・「辺野古基地建設事業の警備業務に関する質問主意書」（平成 28 年 5 月 30 日）
・「情報公開・個人情報保護委員会の諮問等に関する質問主意書」（平成 30 年 4 月 18 日）
・「政府各府省のウェブサイトにおけるクッキー使用に関する第三回質問主意書」（平成 30 年 7 月 20 日）
・「自衛隊による住民基本台帳閲覧及び個人情報の収集に関する質問主意書」（平成 26 年 9 月 29 日）
・「デジタル庁が十月二十六日に基本契約を行った AWS に関する質問主意書」（令和 3 年 11 月 10 日）

²⁷ なお、国政調査権よりも検察における捜査が優越しているのではないかと問いただす質問主意書に対し、政府が明確な回答を避けたものとして平成 30 年 3 月 20 日付けの答弁（[「国政調査権と検察による捜査権の優越関係に関する質問主意書」](#)に対するもの）がある。

手続が保障されていないためである。当事者は救済を求めるにあたり、自らの個人データを含む一切の検査資料に起訴前の検査段階ではアクセスできない。令状には、検査関係事項照会書と同様、「検査に必要なため」以上の具体的な理由は記載されないから、検査機関がなぜその処分をしたのか、具体的な理由を知ることができない。起訴されて以降も検査の必要性は継続するとされており、起訴後には一部の証拠が開示されるという点を除き、裁判が終結するまで状況はほとんど変わらない。その結果、検査機関が反対すればほとんどの場合に処分は取り消されない。司法による救済の実効性は限定的である。

また、個人情報の取り扱いに関する救済という意味では、司法の手続はほとんど意味がない。例えば携帯電話やデバイス等を差し押さえられ、かつその内部の情報を解析された場合、刑事手続において争うことができる内容は物の返還や処分の取消しにとどまり、検査機関が取得した情報の削除やデータベース登録の取消し、プロファイリングによって得られた解析結果の削除などは認められていない。さらに、たとえば、DNA型記録について言えば、「DNA型記録取扱規則」は、第7条で、犯罪鑑識官が保管する被疑者DNA型記録を抹消しなければならない場合について規定しているものの、そのような場合とは、「被疑者DNA型記録に係る者が死亡したとき」を除けば、「被疑者DNA型記録を保管する必要がなくなったとき」という抽象的な規定を置いているだけである。また、電磁的記録提供命令が取り消された場合に電磁的記録が消去されないことに関連して、政府の国会答弁で、担当国務大臣は、「現行の刑事訴訟法、この下でも、検査機関が証拠を押収した場合に、その押収処分が事後的に取り消された場合でも、この当該証拠の複製等を廃棄、消去することとはされておりません」と答弁している²⁸。法令上、消去を求める権利が規定されておらず、司法において個人情報の取得後の取り扱いを争う方法が認められていないのである。なお、この解析結果等が証拠として提出されたとしても、前述のとおり違法収集証拠として証拠排除することには高いハードルがある。

（2）「2) 民事訴訟法、国家賠償法に基づく司法救済」（13頁以下）について

政府報告書では、憲法13条に基づくプライバシー権が侵害されたと考える場合、個人は犯罪検査で収集された個人情報の削除を求めて民事訴訟を起こすことができ、また、個人情報の収集や監視によりプライバシー権が侵害され、損害を受けた場合には、国家賠償法や民法に基づき損害賠償請求訴訟を提起できるとの記載もある。損害には財産的損害だけでなく精神的損害も含まれ、賠償額は裁判官が個別の事情を考慮して判断するとされる。国家賠償法は、公務員が職務を行う際に故意または過失により違法に他人に損害を与えた場合、国や公共団体に対して賠償を求める権利を認めており、訴えは民事訴訟法に従い、不法行為の場所を管轄する裁判所で提起できるとの記載もある。

まず、金銭的救済は諸外国と比べて遙かに低い。例えば、個人情報の取り扱いに関して裁判所が認める金額は、相手が検査機関であれ民間事業者であれ数千円から数万円程度がほとんどである（大阪高判2001年12月25日・宇治市住民基本台帳データ漏洩事件・慰謝料1万円、最判2017年10月23日など・ベネッセ個人情報流出事件・慰謝料1000～3300円）。前掲大垣事件においては、100万円の損害賠償が認められているが、組織的違法行為の損害としては低廉であり、抑止効果としても損害の補填としても不十分である。

²⁸ 第217回国会 参議院 法務委員会 第6号 令和7年4月24日(鈴木馨祐国務大臣答弁)

また、国家賠償請求において違法性を主張する場合、職務行為基準説がハードルになり得る。この法理（職務行為基準説）の下では、違法性は、単に（行政権限の行使要件といった）客観的な法規範への違反を確認するだけでは決定されない。むしろ、行為時の公務員の主観的な状況を考慮に入れたうえで、行為者がその注意義務を尽くしたか否かによって判断される。同説によれば、行政処分としての個人情報の収集や監視が法令の定める制限や監督に違反して行われたことが、直ちに国家賠償法上の違法性につながらないことになる（違法相対説）ため、違法性の認定の余地は抗告訴訟におけるそれよりも狭くなる。例えば、個人情報の取扱いに関連して、行個法45条1項の解釈適用を誤り、刑事施設被収容者の診療情報につき非開示決定を行った東京矯正管区長の取り扱いについて、最高裁は、開示しなかったことを違法と認めたが、国家賠償法上の救済を否定した（最判2023年10月26日集民270号215頁）。

その他、国家賠償法上の救済は金銭賠償に限られており、捜査機関による組織的な違法取り扱いであっても、削除請求等を行うとした場合には通常の民事訴訟で行わなければならぬこととなる。しかし捜査機関等の取り扱いを監督する特別の救済制度が設けられていないため、捜査機関側は証拠開示等の義務も負わず、救済を求める者による立証活動は極めて困難である。

なお、国家賠償法には相互保証規定が設けられており、外国籍者による損害賠償請求が制限される場合がある。また、損害賠償が認められるとしても、その金額について外国人の本国の物価水準にとどめられる場合もある。

（3）「3）警察による違法/不適切な捜査に対する個人の救済：都道府県公安委員会への苦情（警察法第79条）」（14頁以下）について

政府報告書では、警察法に基づき、個人は都道府県公安委員会に対して、警察官の職務執行における違法や不適切な行為について文書で苦情を申し立てができるとの記載がある。この権利には個人情報の収集・利用に関する職務も含まれ、都道府県公安委員会は法律や条例に従って苦情を処理し、その結果を申出者に文書で通知するとの記載もある。また、必要に応じて事実関係の調査や措置、報告を都道府県警察に指示する権限を持ち、調査や措置の履行は警察庁の通達にも示され、通知内容は、警察の報告や委員会の指示に基づき作成されるとの記載もある。

記載自体に誤りはないが、前述のとおり公安委員会の監督はほとんど機能しておらず、国家公安委員会や都道府県公安委員会が、裁判所の判決を待たずに警察における個人情報の取扱いに関して警察に勧告等したことは一度もない。苦情を申し立てたとしても、その苦情に基づき具体的な措置が取られるることはほとんどなく、申立書に対する調査結果に関する通知内容においても具体的な内容が記載されることはほとんどない。例えば、日本の警察組織はいわゆるレイシャル・プロファイリングに基づき人種や肌の色等に着目して外国人と思われる対象者を狙い撃ちにして職務質問をする慣行があるとされているが、このことへの苦情を申し立てても、そのような差別的な対応は行っていないとのみ回答され、具体的な対応はほとんど行われていない。

日弁連が実施している人権救済手続において、警察等の公的機関による人権侵害が認定され、「勧告」や「警告」が発せられる事例が多数存在する。しかし、これらの措置には法的拘束力がないため、警察等の公的機関が日弁連の措置に従うことを拒否するケースが常態化している（日弁連2012年1月30日付け『渋谷警察署ホームレス指紋採取等人

権救済申立事件』における警告や、日弁連 2017 年 4 月 20 日付け『警察における DNA 採取に関する人権救済申立事件』における勧告など）。警察等はこれらの勧告・警告に対し、適正な職務執行であった旨回答するに留まり、勧告・警告を適切に受け止めた様子は窺えない。日弁連という法律の専門家集団による是正要請ですら無視されるという事実は、日本において、裁判所の確定判決以外に、捜査機関の違法行為を是正させる実効的なメカニズムが存在しないことを如実に示している。

（4）「4) 行個法・刑事訴訟法に基づく個人の救済」（15 頁以下）について

ア 「a) 行個法」（15 頁以下）について

政府報告書では、行政機関は、行個法に基づき個人情報に関する苦情の適切かつ迅速な処理に努める義務を負い、総務大臣は、都道府県ごとに情報公開・個人情報保護総合案内所を設置し、開示請求や訂正請求、利用停止請求などの手続を案内しており、個人は、保有個人情報が適法でない場合や違法に利用されている場合、利用停止や消去を請求できるとの記載がある。また、犯罪捜査のために収集された個人情報（令状や捜査関係事項照会に基づくもの）は、刑事訴訟法や刑事確定訴訟記録法の特別な規則に従うため、通常の行個法の開示・訂正・利用停止権の対象外とされるが、この除外は、捜査の機密保持や適切な刑事裁判の確保、関係者のプライバシー保護のために正当化され、行個法第 2 章の個人情報取り扱いの基本原則が適用されるとの記載もある。

記載に誤りはないものの、捜査活動について監督が機能していないこと、そのため救済もほとんど機能していないことは前述のとおりである。決定的な問題は、日本の法制度において、本人への直接開示が制限される場合における代替措置が欠如していることである。EU の LED14 条や 17 条では、捜査の密行性などを理由にデータ主体への直接のアクセス権等が制限される場合であっても、独立した監督機関がデータ主体に代わってデータの適法性を確認する「間接アクセス（Indirect Access）」の制度が保障されている。これにより、本人は捜査内容を知らされなくとも、監督機関を通じて「データが法に従って取り扱われているか」といった確認や、必要な是正を受ける権利が担保される。しかし、日本にはこのような間接アクセス制度に相当する制度が全く存在しない。個人情報保護委員会は、捜査機関が保有する個別の捜査情報ファイルについて、本人に代わって内容を確認し、適法性を検証する権限を行使する実務上の枠組みを持たない。したがって、日本の法制度上、捜査機関が「捜査に支障がある」として開示を拒否した場合、その判断が妥当か否かを中立的に検証する術は、本人にも監督機関にも残されていないのである。

イ 「b) 刑事訴訟法」（16 頁以下）について

政府報告書では、起訴された場合、被告人・弁護人は証拠を閲覧できると記載されている。

しかし、検察官が証拠請求していない証拠については直ちに閲覧することはできない。公判前整理手続または期日間整理手続に付された場合は、証拠開示制度が法定されているが、公判前整理手続に付される事件自体が限定されている。公判前整理手続を経ない場合、検察の任意開示に頼るほかない。ちなみに、日本では米国その他の法域などと異なる

り、検察官に被告人に有利な証拠（*exculpatory evidence*）の開示義務はない。

また、証拠開示制度では、弁護人が表題のみを頼りに開示を求め、これに対し検察官が法律上の要件を満たす場合に限り開示するという非効率な手続がとられている。検察官の判断に不服があれば証拠ごとに弁護人が異議を申し立て、裁判所が裁定するという迂遠な制度となっている。開示は検察庁または警察署にある紙の記録を弁護人が謄写するのが原則という制度となっており、謄写費用はすべて被告人が負担する。事件によって数百万以上の謄写費用が必要となる。

（5）「5) 公的機関による違法/不適切な捜査に対する個人救済：個人情報保護委員会への苦情」（17頁以下）について

政府報告書では、個人は、EU から移転された自身のデータが日本の公的機関により違法に取り扱われた疑いがある場合、個人情報保護委員会に苦情を申し立てることができること、委員会は関係機関に調査を依頼し、必要な情報提供を受けて適法性を評価し、違法があれば是正（削除を含む）を行わせ、その完了も確認すること、評価後、委員会は結果や是正措置を本人に通知し、法執行関係の苦情では刑事記録の閲覧等の権利についても案内すること、不服がある個人には、利用可能な救済手段や手続の説明、行政・司法機関への申立てに関する支援も提供することの記載がある。

確かに個人情報保護委員会の英語ウェブサイト上で、「[Complaint Mediation Line for Japanese administrative authorities' handling of personal data transferred from the EU and the UK based on an adequacy decision, etc.](#)」（十分性認定等に基づき EU・英国から移転された個人データの日本の行政機関による取り扱いに関する苦情調停窓口）という専用窓口が設置され、電話番号が案内されている。

EDPB 意見書では、個人情報保護委員会が単なる連絡窓口になるだけであれば、EU の水準と同程度に実効性ある救済とはいはず不十分であるとの指摘がなされていた（EDPB 意見書パラグラフ 203）。実際、この苦情処理に関連して、個人情報保護委員会が、行政機関に対していかなる法律上の権限を有するのかは明確ではない。上述のとおり、警察における個人情報の取り扱いについて、個人情報保護委員会が監督権限を行使して調査したり資料提出の要求をしたことはなく、勧告をしたこともないこと、警察が構築している指紋・顔写真や DNA 型の各データベースについて、個人情報保護委員会が法制定の提案をしたことないこと、さらに裁判所も、警察による個人情報の取り扱いについてきわめて緩やかな判断を行っていることなどに照らすと、本レポートで指摘しているような問題について、個人情報保護委員会への苦情申し立てにより適切な救済がなされることを期待するのは難しいであろう。

第3 「III. 国家安全保障目的の政府アクセス」（19頁以下）について

1 「A. 個人情報の収集のための法的根拠と制限について」（19頁以下）について

（1）「1) 関係省庁における情報収集の法的根拠」（19頁以下）について

政府報告書では、「国家安全保障目的のための行政機関が行う個人情報の収集は、当該行政機関の所掌事務の範囲内にあることが必要である」こと、強制処分による情報収

集は犯罪捜査のみを目的とする令状の発付により行われるのであり、「国家安全保障のみを理由として強制手段による情報収集を可能とする法律は存在しない」ことが記載されている。

国家安全保障のみを理由として強制手段による情報収集を可能とする法律は確かに存在しない。しかし、組織法に過ぎない警察法に基づき、具体的な犯罪の嫌疑が無くとも、「公共の安全と秩序の維持」（警察法 2 条）のために情報収集活動することが認められており、これはむしろ規律がまったくない状態で情報収集ができるという意味に近い。このような状況は、欧州人権条約によって定められた基準により規制がなされなければならないとする EU のアプローチ（EDPB 意見書パラグラフ 220 参照）とは程遠いものである。

規律が働いていないことを示す実例として、例えば、前掲ムスリムの監視捜査では、国際テロ防止という安全保障目的であれば、裁判所が極めて緩やかに個人情報の取得を許容することが明らかとなっている。

なお、日本において国家安全保障目的で個人情報を取得・管理し得る公的機関として、都道府県警察、警察庁、公安調査庁、自衛隊情報保全隊がある。

ア 「(1) 内閣官房」（19 頁以下）について

政府報告書では、内閣官房は、内閣法 12 条 2 項の定める所掌事務の範囲で「オープンソースや他の公的機関等からの情報について、収集・集約・分析・評価を行う」のであり、「事業者から直接的に個人情報を収集する権限を有していない」との記載がある。

これは、捜査関係事項照会制度のような法律上の制度が内閣官房にはないということを意味するにとどまる。前掲ムスリムの監視捜査事件においても、日本の裁判所は、安全保障目的であれば、特段の手続きを経ずに省庁間で情報を共有することを適法としているから、内閣官房は、警察組織と協力して情報を取得させ、それを提供させることで、実質的に事業者から個人情報を収集することが容易に可能となっている。

内閣官房には内閣情報調査室があり、内閣情報調査室を含む情報コミュニティ各省庁（主に警察庁、公安調査庁、防衛庁、外務省）が相互に緊密な連携を保つつつ、情報収集に当たっている（内閣情報調査室ウェブサイト²⁹）。都道府県警察の警備課が「公共の安全と秩序の維持」のために収集した情報が、警察庁を通じて内閣情報調査室に共有されている。

イ 「(2) 警察庁・都道府県警察」（19 頁以下）について

政府報告書では、警察庁が、特に警備警察事務を司る警備局、また警備警察事務のうち外国人や外国を本拠地とする日本人に関するものを扱う外事情報局の活動との関係で、警察法の定める所掌事務の範囲で直接情報収集を行うことがあると説明されている。都道府県警察については、警察法 2 条の所掌事務の範囲で情報収集を行うと記載するにとどまる。

日本の警察執務は、各都道府県公安委員会の管理の下で各都道府県警が行うことと

²⁹ https://www.cas.go.jp/jp/gaiyou/jimu/jyouhoutyousa/intelligence_taisei.html

されているが³⁰、階級の高い（警視正以上）の幹部警察官は国家公務員とされ、都道府県警察の主要部門のトップは警察庁の官僚が配置され、警察庁長官は「警察庁の所掌事務について、都道府県警察を指揮監督する」（警察法 16 条）とされている。加えて、公安関係予算は国庫から支出されることになっており、事実上、警察庁が都道府県警察をコントロールしている。

例えば、自動車ナンバー自動読み取りシステム（通称 N システム）が全国の幹線道路や高速道路に設置され、通行した全車両のナンバーデータを無人カメラで記録し、読み取られた情報は通信回線を通じて都道府県警察本部に設置された中央装置に送られる。データは、当該都道府県を管轄する管区警察局に設置されたサーバにも送信されて保存されており、記録されたデータは警察庁をはじめとする警察組織のどこからでも検索可能になっている。ちなみに、この N システムの根拠や規制について定めた法令は存在しない。

国家安全保障を目的とする情報収集の手段につき法定はされてはいないが、都道府県警と緊密に連携することで実質的には国家的に活動を行うことができている。

ウ 「(3) 公安調査庁」（20 頁以下）について

政府報告書では、公安調査庁が「我が国の公共の安全に対し明確に国内又は国外からの脅威をもたらしていると正確に特定された団体のみ」を対象に、破壊活動防止法（破防法）及び無差別大量殺人行為を行った団体の規制に関する法律（団体規制法）が規定する権限に基づき、もっぱら任意での情報収集を行うこと、また情報の収集や利用は「法律で定められている関連する保護措置及び制限の対象となり、特に、憲法によって保障された通信の秘密があり、行個法に基づく個人情報の取扱いに関する規則に依拠する」ことが記載されている。

しかし、団体規制法における情報収集は、実質的には任意とは言えない。事前予告なく朝方に 10 名以上の公安調査庁の調査官が対象団体の施設を訪れ、立入検査（団体規制法 7 条）を行う。立ち入りにあたっては事前にメディアに通告し、複数のメディアのカメラが立入の様子を撮影して放送する。立入検査拒否には罰則があり（同法 39 条）、施設の管理者が検査時にその施設を不在にしていると、立入検査拒否として逮捕される恐れがあると通告される。立入検査は 10 時間以上に及ぶことが通常であり、休憩を求めたり中止を求めれば検査拒否に当たる可能性があると通告される。立会人が所持する携帯電話も検査の対象となり、電話の通話履歴の画面を表示させ、それを写真撮影する検査も行われている。これも拒絶すると検査拒否として逮捕される可能性がある旨通告される。団体に所属する構成員の氏名や住所も提供を求められ、拒絶すれば逮捕の危険がある。このように、あらゆる情報提供は逮捕の警告下で行われるため、拒絶の余地はほとんどなく実質的には強制として行われている。なお、裁判所はこのような態様での立入検査も適法としている（東京地判 2017 年 5 月 30 日など）。

形式上、公安調査庁も個人情報保護法に基づく個人情報の取扱いに関する規則に依拠しているが、同法は「国の安全、外交上の秘密その他の国の重大な利益に関する事項を記録する個人情報ファイル」、「犯罪の捜査、租税に関する法律の規定に基づく犯則事件の調査又は公訴の提起若しくは維持のために作成し、又は取得する個人情報ファイル」に

³⁰ なお、形式上都道府県警察を規律している各条例は、EDPB 意見書パラグラフ 224 において英訳がないために検証できないことが指摘されていた。現時点においても英訳されたものは管見の限り見当たらない。

について、個人情報保護委員会の監督対象から除外しており（個人情報保護法 74 条 2 項 1 号・2 号）、また、これらの個人情報は開示請求しても全面的に不開示とされており、実質的に法的規制がないに等しいことは前述のとおりである。

工 「(4) 防衛省」（21 頁）について

政府報告書では、防衛省設置法 3 条及び 4 条に定めのある所掌事務の遂行に必要な情報を、任意協力または自由にアクセス可能な情報源を通じてのみ収集し、「一般市民の情報は収集しない」と記載されている。

これは事実ではない。自衛隊情報保全隊が、市民による自衛隊のイラク派遣反対運動などを監視し、運動に参加していた市民らの個人情報を収集していたことが明らかになっている（仙台高判 2016 年 2 月 2 日判時 2293 号 18 頁）。

また、防衛省は、自衛官及び自衛官候補生募集のために、全国の地方自治体に対し、各自治体が管理する住民の氏名・住所・生年月日及び性別といった個人情報の提供を求めている。このような住民情報の提供を問題視した一部の自治体や新聞等のマスメディアの指摘に対し、政府は住民情報の提供に法的な問題はないとする閣議決定を行い、それを受けた防衛省及び総務省は、自治体に対し、住民情報の提供が適法であり、提供に問題はないとする通知を出し、個人情報の提供を促している³¹。

(2) 「(1)³²制限と保護措置」（21 頁以下）について

ア 「a) 法的制限」（21 頁以下）について

(ア) 「(1) 行個法に基づく一般的な制限」（21 頁）について

政府報告書では、「あらゆる活動分野での行政機関による個人情報の収集及び取扱いに適用される一般法」たる行個法に基づく個人情報の収集・取扱い上の規制が、国家安全保障分野にも適用される旨記載されている。

しかし、個人情報保護法の規制がほとんど機能していないことはこれまで述べたとおりである。

(イ) 「(2) 警察に適用される特定の制限（警察庁及び都道府県警察）」（21 頁）について

政府報告書では、警察による情報収集は、警察法 2 条の制限のもと、「公共の安全と秩序の維持」の範囲で、「不偏不党かつ公平中正な方法で」、また「憲法の保障する個人の権利及び自由の干渉にわたる等その権限を濫用すること」なく実施される旨記載されている。既述のとおり警察法は組織法であり、同法 2 条は抽象的な規定で、個人データ処理の法的根拠となる具体的かつ明確な法令とは言えない。

³¹ 「自衛官又は自衛官候補生の募集事務に関する資料の提出について（通知）」（令和3年2月5日付け防衛省人事教育局人材育成課長、総務省自治行政局住民制度課長通知）

³² 原文ママ。おそらく 2) の誤りであると思われる。

この点の具体例をみてみると、例えば「公共の安全と秩序の維持」のために収集される個人情報が、極左暴力集団等に限らず、風力発電計画について学習会などを開いていた市民まで対象にしていたことが近時の裁判例（前掲の大垣事件）で明らかになっている。このような情報収集は、新聞が報じた内部告発によって明らかになった。不偏不党かつ公平中立な方法で情報収集が遂行されているかを市民がチェックする手段はなく、個人情報保護委員会の権限も実効性がなく、実際に個人情報保護委員会が警察庁又は都道府県警察の個人情報収集について立入検査を行ったことは無く、何らかの勧告等を行ったこともない³³。

（ウ）「(3) 公安調査庁に適用される特定の制限」（21頁以下）について

政府報告書では、「破防法第3条及び団体規制法第3条には、両法に基づき実施される調査を必要最小限に留め、国民の基本的人権を不当に制限したりすることのないように戒める旨の規定が設けられている」、「また破防法第45条及び団体規制法第42条に基づき、公安調査官が職権を濫用した場合、公的部門の他の分野における『一般的な』職権濫用の罪より重い罰則が設けられている」と記載されている。

記載に誤りはない。しかし職権濫用等により摘発された事例は皆無であり、事実上機能していない。政府は、事例が皆無なのは職権が濫用された事実がないためであると言ふかもしれないが、外部からの検証の仕組みはない。

（エ）「(4) 防衛省に適用される特定の制限」（22頁）について

政府報告書では、防衛省が行う情報の収集整理について、限定がある旨の記載がある。この記載が誤りであることは既述のとおりである。

イ 「b) 他の制限」（22頁）について

政府報告書では、判例上、「事業者へ任意協力を要請するには、犯罪捜査のために必要でなければならず、捜査の目的を達成するために相当なものでなければなら」ず、また「安全保障分野において調査機関により行われる調査」について、上記主要原則は、「類似的に適用され、各事案なりの事情を適切に考慮した上で、遵守されなければならない」と記載されている。さらに「上記の制限の組合せにより、情報の収集及び加工が、所管行政機関の特定の職務の遂行に必要な範囲で、特定の脅威に基づいて行われることが確保され」、「国家安全保障上の理由による大量かつ無差別な個人情報の収集やアクセスが排除される」と記載されている。

しかし、安全保障分野について政府の調査権限やその限界を定めた法律はなく、

³³ 警察につき、本レポート第2/「II 法執行目的の政府アクセス」について/3「C)個人の救済」について/(5)「5) 公的機関による違法/不適切な捜査に対する個人救済:個人情報保護委員会への苦情」について 参照。また、警察及び防衛省、公安調査庁につき、第3/「III. 国家安全保障目的の政府アクセスについて/2「B. 監督」について/(1)「1) 行個法に基づく監督」について 参照。

「公共の安全と秩序の維持」のために具体的な犯罪事実がなくとも個人情報の収集が行われている。事業者に対し、安全保障目的で強制的な情報収集はできないが、警察からの任意の協力を断る事業者は少ない。また、警察を含む政府から個人情報提供要請を受けた件数やこれに応じた件数を公開する事業者も極めて少ない。

実際に、警察は、テロ対策名目でムスリムの個人情報を大量かつ無差別に収集・保有し、データベース化している。

いずれにせよ問題は、個別の法律がなく、具体的な規律がほとんど及んでいないことにある。

2 「B. 監督」（22 頁以下）について

（1）「1) 行個法に基づく監督」（22 頁以下）について

政府報告書では、「行政機関の長は、日本の公的部門において、当該行政機関での行個法の遵守に係る監督及び施行について権限を有する」。また「総務大臣は、同法第 49 条及び第 50 条に基づいて法の施行状況を調査し、各行政機関の長に対して、資料の提出及び説明を求めることができるほか、同法第 51 条に基づいて意見を述べることができる」と記載されている。

記載に誤りはないこと、しかし安全保障関連はほとんど対象から除外されていること、実際に、個人情報保護委員会が警察や防衛省、公安調査庁に対して立入検査を実施したことではなく、何らかの指導や勧告をしたこともないことは、既述のとおりである。

（2）「2) 公安委員会による警察に対する監督」（23 頁）について

政府報告書では、「独立した都道府県公安委員会が都道府県警察の活動を管理」し、「警察庁については、国家公安委員会による管理に服して」いること、「国家公安委員会は、特に『個人の権利と自由を保護』する職責を負う」ため、「警察法第 5 条第 4 項各号に掲げる事務の運営の準則その他当該事務を処理するにあたり準拠すべき基本的な方向又は方法を示す大綱方針を、特に定めるものとされている」こと、「国家公安委員会は、都道府県公安委員会と同じ程度の独立性を有する」ことなどが記載されている。

国家公安委員会は警察庁を管理すると定められているが（警察法 5 条 4 項）、その管理権限は、警察行政機関の所掌事務について大綱方針をさだめ、その大綱方針に即して警察庁を事前事後に監督することであり、事務執行の細部についての個々の指揮監督は予想されていない（高木勇人「警察における政官関係と公安委員会制度」（立花書房、講座警察法第 1 卷、2014 年）。国家公安委員会の定例会議は原則として週 1 回木曜に開催され、平均会議時間は 90 分前後である。国家公安委員会には事務局が無く、庶務は警察庁において処理するとされており（警察法 13 条）、警察庁からの独立性には限界がある。

（3）「3) 防衛監察本部による防衛省の監督」（23 頁以下）について

政府報告書では、「防衛監察本部」は「防衛大臣直轄の特別の機関」であり、「防衛省全組織の法令遵守を確保するため、独立した立場から監察を行う」（「防衛監察」）こと、「自主的な透明性ある方法として、防衛監察の結果は防衛省ウェブサイトで公表さ

れている」こと、防衛監察には「(i) 定期的に行う『定期防衛監察』(ii) 改善結果の状況について点検する『点検防衛監察』(iii) 防衛大臣が命ずる事項について実施する『特別防衛監察』」の三種類が存在すること、「防衛監察は、関係者に対して報告や書類提出を求め、監察に必要な場所の立ち入り、官房長等への説明要求を行うことができる」ことなどが記載されている。

法令上の記載として誤りはないが、これらの監督に関する情報公開は極めて限られており、外部者がその実態にアクセスすることはほぼ不可能である。そのため、記載内容の検証すらできず、これ以上の分析はできない。

(4) 「4) 公安調査庁の監督」(24頁)について

政府報告書では、「公安調査庁は、本庁内部部局及び地方支分部局等…の業務運営について、定例監査と特別監査の両方を実施する」こと、「定例監査の目的のため、部長及び／または課長が監査者として任命され」、「このような監査は、個人情報の管理についても関係している」ことなどが記載されている。

法令上の記載として誤りはないが、これらの監督に関する情報公開は極めて限られており、外部者がその実態にアクセスすることはほぼ不可能である。そのため、記載内容の検証すらできず、これ以上の分析はできない。

(5) 「5) 国会による監督」(24頁)について

政府報告書では、「法執行のための情報収集と同様に、国会は所管委員会を通じて、国家安全保障分野における情報収集活動の適法性を検証することができ」、「国会の調査権限は、憲法第62条並びに国会法第74条及び第104条に基づいている」と記載されている。

国会の監督がほとんど機能していないことは前述のとおりである。むしろ捜査機関に対する以上に、ナショナル・セキュリティに関する国会の監督は機能していない。日本には、法令上のセキュリティ・クリアランス制度が設けられておらず、大臣等に就任した国会議員等が免除されているのみで、国会議員に対して機密情報を開示することがほとんど行われていない。

3 「C. 個人の救済」(24頁以下)について

政府報告書では、「個人の救済は、法執行の分野と同じ方法で行使され…EU市民の苦情を処理して解決するため、個人情報保護委員会が管理して監督する新たな救済メカニズムも含まれている」ことが記載されている。また、「国家安全保障分野で利用可能な個別の救済手段がある」との指摘もある。この記載方法は誤解を招きかねないが、そこで記載されている事項は、一般的な個人情報保護法上の制度であり、国家安全保障分野に固有の制度があるわけではない。政府報告書では、続けて、国家安全保障目的のために行政機関が収集した個人情報について、保有個人情報の開示請求権等の対象となるものの「開

示することにより、国の安全が害されるおそれ…があると行政機関の長が認めることにつき相当の理由がある情報について開示請求権等は認められず、「権利の行使には一定の制限が課せられている」こと、請求が却下された場合、個人は却下の決定について審査請求をすることができ、行政機関の長は「専門性の高い独立した機関」である情報公開・個人情報保護審査会に諮問するものとされていること、同審査会の答申に拘束力はないが、ほとんどの事例において行政機関は答申にしたがった判断をしていることが記載されている。さらに、行政機関が個人情報の開示をしないことの決定に対して、個人は取消しを求める訴訟を提起できることなどが政府報告書に記載されている。

これらの点も検査機関における記載と同様である（「（4）「4）行個法・刑事訴訟法に基づく個人の救済」（15頁以下）について」（本レポート25頁）参照）。条文上、「国の安全が害されるおそれがある情報」ではなく、「（そのような）おそれがあると行政機関の長が認めることにつき相当の理由がある情報」とされており、行政機関の長の判断を踏まえた基準が採用されているため、情報公開・個人情報保護審査会や裁判所は、行政機関の長の裁量を広く認める判断を出している³⁴。その際、検査機関に対する以上に国家安全保障の活動に対して大きな裁量を認めていると思われ、違法性を認めるることはほとんどない。また、法執行分野と同様、国家安全保障分野においても、本人への開示が拒絶された場合に監督機関が代わって確認を行う「間接アクセス制度」は存在しない。このため、日本では、安全保障を理由としてブラックボックス化しており、欧州のような公的なチェック機能を伴わずに放任されているというのが実情である。

第4 「定期レビュー」（26頁）について

政府報告書においては、「十分性認定の定期的なレビューの枠組みにおいて、個人情報保護委員会及び欧州委員会は、当該レターに記載された条件を含む十分性認定の条件下でのデータ処理に関する情報を交換する」と記載されている。

この点については、項目を分けて、次の「おわりに」の項目でコメントする。

おわりに

以上述べてきたとおり、政府報告書は、法令や制度の一般的な説明としては、基本的に誤りを含んではいないと言いうるかもしれない。しかし、個人データが実質的に保護されているか否かを検証する観点からすれば、当然記載されるべき事項を欠いていたり、実際とは大幅にニュアンスが異なる記載を含んでいたりする。その意味で、政府報告書は、日本の実態を知らない人々に対して、日本では、実際以上に個人データが保護されているという印象（誤解）を与えるものになっている。実態に目をむけてみると、少なくとも検査手続における個人データの取り扱いに関する限り、日本におけるEU市民に対する個人デ

³⁴ 政府報告書には「過去3年間の調査結果では、関係行政機関が審査会の答申と異なった裁決を行った例は無いが、さらに過去に遡れば、極めて少ないが事例としては存在する（行個法が施行された平成17年から、約2千件のうちわずか2件のみ）。」という記載があり（脚注35）、EDPB意見書パラグラフ241は、この政府報告書記載に基づき、"there were only two out of 2000 cases, where an administrative authority took a decision that differed from the Board's conclusion."という点に注目している。しかしながら、政府報告書は触れていないが、情報公開・個人情報保護審査会の答申の多くが行政機関の判断を是認しているのであるから、そのような答申に行政機関が不服があるはずはなく、ほとんどの場合に従うのは当然である。

ータの保護は、およそ EU における保護と同程度とは言えないものと思われる。とりわけ捜査を妨げる恐れがなくなつて以降も開示、訂正、利用停止などの権利の保護を欠くことや、警察法という抽象的な組織法を取り扱いの法律の根拠として DNA 型の取り扱いすら具体的な法律の根拠を欠いて行われていること、身体拘束下、あるいは身体拘束の恐れがある状態での個人データの提供すら同意に基づくものとして法律の根拠も令状もないままに適法とされていることなどは、およそ EU における権利の保護と同等とはいえないものである。

今後、十分性認定の定期的なレビューのために個人情報保護委員会及び欧州委員会間でおこなわれるデータ処理の情報交換にあたっては、本カウンターレポートで指摘した事項や視点に留意したうえで、十分な検証がおこなわれることを期待したい。そのようなプロセスを経ることで、日本において、EU 市民を含めたすべての人々の個人データが、十分に保護される制度や運用が実現することを願うものである。

以上

【参考文献一覧】

指宿信「講演録データ駆動捜査時代の規律方法～令状主義との決別？」情報法制レポート 2 号（2022 年 2 月）<https://www.jilis.org/report/2022/jilisreport-vol4no2.pdf>
Laura Drechsler・横田明美「EU 法からみた日本の個人データ越境移転の課題——欧州データ保護法研究者と越境研参加者の討議記録」、指宿信・板倉陽一郎 編『越境するデータと法 サイバー捜査と個人情報保護を考える』所収（法律文化社 2023 年）341 頁
小向太郎「捜査機関による第三者保有の個人情報に対するアクセスと本人の保護」総務省 学術雑誌『情報通信政策研究』 第 4 卷第 1 号

様式第48号（刑訴第197条）

捜査関係事項照会書

年 月 日

殿

警察署

司法

印

捜査のため必要があるので、下記事項につき至急回答願いたく、刑事訴訟法第197条第2項によって照会します。

なお、みだりに本照会に関する事項を漏らさないよう、同条第5項によって求めます。

記

照 会 事 項

【照会警察署の所在地】〒

【担当者氏名】

（電話

）

（注意）本文後段の記載は、必要がないときは削ること。

（用紙 日本工業規格A4）