安全保障と個人情報保護
──自衛隊による個人情報の取扱い──

陣内　徹之助

＜要旨＞

近年、個人情報はビジネスだけでなく安全保障においても重視されるようになり、安全保障と個人情報保護のバランスをどうするかという点は各国で大きな議論となっている。法制面から見ると、先進国の多くが安全保障上の政府の情報収集活動を個人情報保護の適用除外としつつ、別途法的に規制する枠組みを構築している。一方、日本の個人情報保護法は安全保障に関する規定を持たず、かつ行政機関が行う情報収集活動の根拠や権限を明確に規定する法令も存在しない。このため、両者の関係が極めて不明確な状態となっている。特に、有事における自衛隊の活動と個人情報保護の関係は一切議論が行われていない。両者の関係が曖昧であることは個人情報保護及び安全保障の両面から大きな問題と考える。本稿は、主に自衛隊による個人情報の取扱いを題材に、日本における安全保障と個人情報保護の関係について必要な対策を提言するものである。

はじめに

インターネットやソーシャルネットワークサービス（以下、「SNS」と表記する。）の発達は個人情報の価値を高め、様々な領域における個人情報の活用が進んでいる。安全保障の文脈においても個人情報は重要性を増しており、特に 2001 年の米国同時多発テロ以降、テロリズムへの対応（以下、「テロ対応」と表記する。）の名目の下、軍や情報機関による大規模な個人情報の収集が日常化するようになった。テロ対応だけでなく、武力紛争の場面においても、ターゲティング[1]や情報作戦[2]に個人情報は積極的に活用されており、現在の安全保障において個人情報は必要不可欠となっている。

一方で、近年の個人情報保護に対する意識の高まりから安全保障と個人情報保護の

1　ターゲティングとは目標選定から発見・攻撃及び成果確認までの一連のサイクルを伴う軍事行動を指す。
2　情報作戦とは軍隊等が情報操作等を通じて敵対者の意思決定に影響を及ぼすことで有利な態勢を獲得する軍事行動を指す。

間には緊張関係が生じており、両者のバランスが重要となっている。先進国の多くは、個人情報保護制度において安全保障あるいは国防に関する政府の活動は規制の対象外とする一方で、安全保障目的による情報収集活動の根拠法を整備し、一定の歯止めが掛かるよう配慮している。

しかしながら、日本の個人情報の保護に関する法律（以下、「個人情報保護法」と表記する。）は安全保障に関する例外規定を持たない。また、行政機関が行う安全保障上の情報収集活動の権限を規定し、活動範囲を規制する根拠法も存在しない。このため、安全保障と個人情報保護の関係が不明確であり、安全保障目的での行政機関による個人情報の収集や利用がどの程度許容されるのか明確な基準がない状態となっている。特に、武力攻撃事態[3]において自衛隊が行う国土防衛作戦と個人情報保護の関係については一切議論が行われていない。安全保障における個人情報の重要性は今後増々増大すると考えられる一方で、行政機関が明確な法的根拠なしに無制限に個人情報を収集・利用することが許されるわけではない。本稿は、主に自衛隊による個人情報の取扱いを題材とし、日本における安全保障と個人情報保護の関係について問題提起及び提言を行うものである。

1．研究概要

（1）先行研究の状況

国際法分野における安全保障と個人情報保護を巡る議論は、そもそも個人情報保護を規定する拘束力を有する条約等が整備されていないこともあり、活発とは言い難い。このため、個人情報保護法制度は、主に各国の国内法制を通じて発展し、安全保障と個人情報保護の関係も各国の国内法を中心に議論が行われてきた。とりわけ、個人情報に関する権利意識の高い欧州においては様々な研究及び判例の蓄積が存在する[4]。特に欧州人権裁判所等における判例は実態が把握しづらい国家による情報収集活動を論ずる上で貴重な資料となっている[5]。一方で、国内における研究状況に目を向けると、欧米諸国の判例及び法制に関する研究や国内判例に係る研究は若干確認されるもの

3　武力攻撃事態等及び存立危機事態における我が国の平和と独立並びに国及び国民の安全の確保に関する法律（以下、「事態対処法」と略する。）2 条 2 項で定める事態。

4　一例として “Bulk Collection: Systematic Government Access to Private-Sector Data,” eds. Fred H. Cate and James X. Dempsey (Oxford: Oxford University Press, 2017).

5　一例として Big Brother Watch and Others v. United Kingdom 58170/13; 62322/14; 2460/15 Eur. Ct. H.R. 2021 (Big Brother Watch).

の[6]、正面から当該問題をテーマとした研究はほとんど行われていない[7]。特に武力攻撃事態等における個人情報保護を取り扱った研究は管見の限り存在しない。この点において本稿は新規性・有益性を有すると考える。

（2）本稿の焦点及び論文構成

各国の状況に鑑みれば、多くの国が安全保障領域において個人情報保護の例外を設けることに一定の合理性があると考えているものと推測される。一方で、たとえ有事であっても個人情報の収集・利用が無制限に行われて良いわけではないことは明らかである。この両者のバランスをどのようにとるか、ということが本稿の主題である。このバランスは平素[8]から有事に至る一連の流れにおいて流動的に変化するものであり、平素から最も烈度の高い外国からの武力攻撃への対応までの広い範囲を考察の幅とすることが必要である。一方で、紙面の関係からも一連の全状況を考察することは不可能であることから、本稿では現状日本ではほとんど議論がなされていない、武力攻撃事態等[9]を中心にした自衛隊による個人情報の取扱いを焦点とした考察を行う。

なお、個人情報保護の問題はプライバシー保護と関連が深い。両者は重なる部分が多く、個人情報の不適切な取扱いが同時にプライバシーの侵害となることも多い。しかし、一般的に両者は別々に考えることが必要とされる[10]。具体的には、プライバシーとは「私生活をみだりに公開されないという法的保障ないし権利」とされ個人の主観が大きく反映される概念であるが[11]、個人情報とは「氏名、生年月日その他の記述等により特定の個人を識別することができる」情報又は特定の個人を識別できる「個人識

6 自衛隊による情報収集に関する国内判例研究として、岡山公法判例研究会「情報保全隊による情報収集・保存が違法とされた事例（仙台地方裁判所平成二四年三月二六日判例時報二一四九号九九頁）」『岡山大 学法学会雑誌』第 63 巻第 1 号（2013 年 8 月）等が存在する。

7 警察による情報収集については若干の研究例があり、田村正博「警察における情報の取得及び管理に対する行政法的統制」『産大法学』50 巻 1・2 号（2017 年 1 月）等が存在。

8 本稿においては、平素とは、異常な事態が生起していない状況を指す。一方で、平時は有事の反意語であり、法的な観点から武力攻撃事態が認定されていない全ての状況を指す。

9 武力攻撃事態等とは武力攻撃予測事態を含む概念である。武力攻撃予測事態は武力攻撃事態には至っていないが、事態が緊迫し、武力攻撃が予測されるに至った事態とされる（事態対処法 1 条及び 2 条 3 項）。なお、平素の段階における対象国からのサイバー攻撃を含む情報作戦への対応は、現状、自衛隊の任務ではない。しかしながら、武力攻撃事態等においては自衛隊自らが対応する必要性が生じる可能性があり、本稿の検討対象に含めている。この場合、「通信の秘密」を含む様々な課題が生じることが予想されるが、本稿では個人情報保護に焦点を絞るため詳細については触れていない。

10 新保史生「ネットワーク社会における個人情報・プライバシー保護の在り方」『IEICE Fundamentals Review』第 6 巻第 3 号 (2013 年 1 月) 201 頁。

11 東京地判昭和 39 年 9 月 28 日判時 385 号 12 頁。なお、プライバシー権に関しては、近年、行政や企業等が保有する個人情報の開示・訂正・削除を求める等の自己情報コントロール権が含まれるとする説が有力に主張されている。しかしながら現段階では明確な概念として確立しているものではないとされているため、本稿では旧来のプライバシー権の概念を使用する。第 204 回国会衆議院内閣委員会（2021 年 3 月 12 日）近藤正春内閣法制局長官答弁。

別符号が含まれる」情報[12]であり、個人情報保護法制は主として事業者や政府・地方公共団体を規制するものである。つまり、個人情報保護は、プライバシー保護が個人に対する個別具体的な法益侵害を主に対象とすることに対し、社会全体における個人情報取扱いの信頼性という、より客観的かつ公益性を重視した概念と考えられる[13]。プライバシー保護は重要な問題であるが、本稿においては論点を明確にする観点から考察の対象外とする。

2．安全保障領域における個人情報の利用の現状

（1）国外の状況

2001 年に発生した米国同時多発テロ事件は、各国が安全保障を理由とした個人情報の大規模収集を積極的に行うようになった契機となった。特に 2013 年の元米国国家安全保障局（NSA）外部契約社員エドワード・スノーデン（Edward J. Snowden）による暴露は、国家機関による個人情報の取得の現状の一端を明らかにし、大きな衝撃を与えた。上記暴露によれば、米国 NSA、英国政府通信本部（GCHQ）及び様々な通信関連企業が協力し、PRISM や Boundless Informant といったシステムを開発・運用し、世界中の個人・組織を対象とした大量の通信データの傍受・収集を行っていたとされる[14]。このような活動は機密度が高いため正確な把握は困難であるが、現在でも同様の活動が各国で継続されていると考えることが自然であろう。個人情報の大量収集は間接的な通信傍受にとどまらず、直接的な生体認証情報の収集という形態でも行われている。生体認証情報はテロ対策において極めて重要な意義を有しており、米国国防総省はイラク、アフガニスタン等で「敵の戦闘員やテロリストを特定し、標的を定め、混乱させる」ために生体認証技術を使用してきたことを認める[15]。一例では、検問等を利用して収集した指紋等の生体認証情報により軍事施設への地元住民のアクセスを制限する運用が行われていたとされる[16]。また、一般住民に紛れて潜伏したテロリストの識別を目的として、虹彩、指紋、顔の画像などの情報を採取し数百万人分のデー

12 個人情報保護法 2 条。
13 新保「ネットワーク社会における個人情報・プライバシー保護の在り方」202 頁。
14 Glenn Greenwald, *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State* (New York: Metropolitan Books, 2014).
15 “Biometric Technologies and Global Security,” U.S. Congressional Research Service, January 30, 2023, https://crsreports.congress.gov/product/pdf/IF/IF11783.
16 Rawlson O’Neil King, “Biometric and National Security White Paper,” *Biometrics Update Special Report*, Biometrics Research Group, Inc, 2013, https://www.biometricupdate.com/wp-content/uploads/2014/03/Biometrics-and-National-Security.pdf.

タベースを作成し、テロリストの身元の割り出しに活用されたとも言われる[17]。さらに極端な例としては、司法手続きなしにテロリスト等を、無人機等を使用して殺害する標的殺害においては、通信情報の傍受や無人機等を使用した監視により収集された顔画像等の生体認証情報や生活パターン等の個人情報が使用されている[18]。

対テロ作戦だけでなく国家間の紛争の場面においても、個人情報が活用されるようになっている。商業領域におけるマイクロ・ターゲティングの手法が応用され、サイバー手段を用いて個人の行動様式、趣向、政治信条といった個人情報を収集、特定個人にカスタマイズされた高度な偽情報を生成・配布することで、従来の放送・ビラ撒きといった大衆向けの宣伝手法とは比較にならない効果的な世論操作や情報操作が可能となったとされ、それが紛争に活用されている[19]。実際、米国大統領選におけるロシアによる選挙干渉でもこのような手法が使用されたとされる[20]。また、国家間武力紛争の場面においても個人情報の活用は進んでいる。ロシア - ウクライナ紛争では捕虜の顔画像や氏名・階級等の個人情報が容易に判別できる動画や、戦争犯罪容疑者の氏名・階級をインターネット上に公開する等の情報作戦が展開されている。このような個人情報の軍事利用は、国際人道法上は明確には違法とはされていないもののプライバシーや個人情報保護の観点からの問題が指摘されている[21]。

（2）日本における状況

日本において安全保障上の情報収集活動を実施する行政機関として代表的なものに、内閣情報調査室、外務省、公安調査庁、警察及び自衛隊が存在する。しかしながら、日本には米国の中央情報局（CIA）、国家安全保障局（NSA）、あるいは英国の秘密情報部（MI6）等の対外情報収集活動を専門に担う情報機関は存在しない。このため、上述の様々な組織がそれぞれ独自に情報収集部門を持ち、それぞれの組織活動に必要な情報収集を行っている。上記組織の中では規模及び能力の観点から警察と自衛隊が

17 “To Track Militants, U.S. Has System That Never Forgets a Face,” *The New York Times*, July 13, 2011, http://www.nytimes.com/2011/07/14/world/asia/14identity.html; “The Eyes Have It: Biometric Data and the Afghan War,” *The Economist*, July 7, 2012, http://www.economist.com/node/21558263/print.

18 標的殺害の概要は以下の記事が参考になる。Jane Mayer, “The Predator War,” *The New Yorker*, October 19, 2009, https://www.newyorker.com/magazine/2009/10/26/the-predator-war.

19 Tim Hwang, *Maneuver and Manipulation: On the Military Strategy of Online Information Warfare* (Pennsylvania: US Army War College Press, 2019),pp. 34–39.

20 Samuli Haataja, *Cyber Attacks and International Law on the Use of Force* (New York: Routledge, 2019), pp. 178–182.

21 “Ukraine: Respect the Rights of Prisoners of War,”Human Rights Watch, March 16, 2022, https://www.hrw.org/news/2022/03/16/ukraine-respect-rights-prisoners-war.

突出しており、安全保障上の情報収集の大部分は両組織が担っていると考えられる[22]。しかし、両者の活動の中には行政訴訟に発展したケースが多数存在する。代表的なものとして、自衛隊が情報公開請求を行った者をリスト化し部内で閲覧可能な状態にしていたことが問題となった防衛庁リスト事件[23]、海外におけるイスラム過激派の活動激化に伴い、国内におけるイスラム教徒の動向を監視した情報が流出した公安テロ情報流出被害国家賠償請求控訴事件[24]、風力発電所建設を巡る反対活動に対し公安情報として個人情報の提供を警察が企業に依頼した大垣警察市民監視国家賠償請求事件[25]及び自衛隊のイラク派遣への抗議活動に対する自衛隊情報保全隊による監視活動が問題となった監視活動等停止請求事件[26]等が存在し、いずれも安全保障に関連して、行政機関による本人同意なしでの個人情報の取得や不適切な取扱いが行われ、その違法性が問われた事件である。これらの事件は日本においても安全保障上の観点から警察や自衛隊が平素から様々な個人情報を収集しており、その活動により個人情報保護への侵害に対する懸念が実際に生じていることを示す。

（3）安全保障領域における個人情報の意義

中国やロシア等のいわゆる非民主主義国家では、国家による個人情報の収集・利用はほぼ無制限で行われている。しかし、非民主主義国家だけでなく、民主主義国家においても国家による国民監視とも言うべき個人情報の収集・利用が密かに行われていることは、安全保障において個人情報が必要不可欠となっていることを示している。個人情報保護への意識が高いとされる EU 諸国においても敵対する外国の国家機関やテロ組織、あるいは国内過激派との関係を調査するにあたって、氏名・年齢・性別・職業といった個人を特定するための基本的な情報に加え、通信記録や生活パターン、あるいは銀行口座といった情報を情報機関が収集していたことが明らかになっている[27]。これらの情報は極めてセンシティブな性格を有する一方で、外国から干渉・侵害や国内反政府活動等への関与を厳格に証明し、じ後の訴追手続き等を適正に行うためには必要不可欠な情報であると考えられる。加えて武力紛争時においては、前述のイラク、アフガニスタン等での例に見られるような、生体認証情報等のより機微な個

22 内閣情報調査室は基本的に情報集約機関であり、衛星情報を除き独自の収集能力を有しない。また、外務省及び公安調査庁は収集能力が人的情報に限定され、かつ所属員が外務省約 6,000 人、公安調査庁約 1,500 名程度と、警察（約 26 万）及び自衛隊（約 24 万）と比較すると圧倒的に小規模であると言える。
23 東京地判平成 16 年 2 月 13 日判時 1895 号 73 頁；新潟地判平成 18 年 5 月 11 日判時 1955 号 88 頁。
24 東京地判平成 26 年 1 月 15 日判例時報 2215 号 30 頁。
25 岐阜地判令和 4 年 2 月 21 日判時報 2548 号 60 頁。
26 仙台地判平成 24 年 3 月 26 日判例時報 2149 号 99 頁。
27 一例として小川原正道「ドイツにおけるテロ・過激主義とテロ対策」『国際安全保障』第 32 巻第 4 号（2005 年 3 月）42 頁。

人情報の収集が行われている。これは、戦闘行為において敵を正確に識別・攻撃する必要性があり、生体認証情報等を無関係な者が巻き込まれる被害を防止するために必要な情報として各国が認識していることを示している。

上記を踏まえると、外国からの武力攻撃やテロ等に対応する自衛隊にとっても、事態の緊迫度に応じて国内外の個人情報を収集・保管し、武力攻撃事態等において有効に活用できるように準備することは極めて重要な活動と考える。特に、今後日本周辺の安全保障環境が厳しさを増すにつれ、あるいは国内に所在する外国人数が増加するにつれ、その必要性は増大していくことが考えられる。

軍や情報機関による個人情報の収集・利用は個人情報保護を含む権利侵害の可能性を多分に伴うものであり、厳正なルールに基づく適切な取扱いが必要であることは言うまでもない。一方で、個人情報の収集が、テロや外国軍隊による活動を未然に防止する、あるいは、正確な識別により誤射や付随的損害を防止するという公益性を有するものであることも事実である。重要なことは、両者のバランスをどのように保持するかであり、かつそのバランスを法の支配の下で誰もが理解できるように具現化することであると考える。

（4）自衛隊による個人情報収集の必要性

これまで、安全保障を目的とした個人情報の収集・利用に関し国内外の状況を概観し、その意義について述べてきた。一方で、紛争等を抱える外国は別とし、ここ日本において、自衛隊が個人情報を収集・利用する必要性があるのか、警察や自治体からの情報提供で事足りるのではないか、という疑問が生じることが予想される。このため、その必要性について補足を行う[28]。

「２．（２）日本における状況」内で触れた通り、安全保障領域において情報収集を主に担うのは警察と自衛隊であるが、両組織の間には任務上の大きな違いが存在する。警察が「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たる」[29]一方で、自衛隊は「我が国の平和と独立を守り、国の安全を保つため、我が国を防衛することを主たる任務とし、必要に応じ、公共の秩序の維持に当たるものとする。」とされる[30]。これは、簡単に言えば、警察は犯罪対応が主である一方、自衛隊は外国からの脅威、特に武力攻撃

28 なお、自衛隊が作戦行動に関連する個人情報を収集すること自体の合法性については、後述の監視活動停止等請求控訴事件において、仙台高裁はイラク派遣反対活動参加者の個人情報を自衛隊情報保全隊が収集すること自体に違法性はないと判示する。仙台高判平成 28 年 2 月 2 日判例時報 2293 号 38 頁。
29 警察法 2 条。
30 自衛隊法 3 条。

に関連する活動への対応を主とするということである。このため、収集すべき情報の種類・対象・収集基準及び要領には差異が生じる。個人情報の収集という観点からは、まず対象とする個人に大きな差異が生じ、国内の犯罪者を主対象とする警察に対し、自衛隊の対象は外国の軍隊や情報機関といった国家機関と関連を有する者、具体的には、上記組織等に属する、あるいは何らかの繋がりを有する外国人やその関係者等が考え得る。これらの対象は、何らかの訓練等を受け、特別な技能を有する可能性が高く、当然、収集要領等に差異が生じる。特に、警察による刑事捜査のように公の手法ではなく、対象に収集活動の存在自体を知られない秘匿性が求められることが予想され、共有自体が困難であることが考え得る。また、収集対象の地理的範囲がほぼ国内に限定される警察に比し、自衛隊の場合は、対象国を含めた広範な領域を対象としなければならない。これは、地方警察を主体とする現状の警察組織では能力上も不可能であり、大規模・組織的な収集機能を有する自衛隊が実施せざるを得ないであろう[31]。特に、個人情報の収集において重要な役割を果たす通信情報の収集に関する組織ではその差異は極めて大きく、自衛隊独自の収集が必要不可欠である。

また、日本の行政組織では、個人情報の保有・管理の多くは地方自治体が担っているが、あくまで行政サービスの提供の観点から地域住民の個人情報を保有・管理しているにすぎず、安全保障に関連する能動的な収集機能は保有していない。このため、自衛隊が必要とする外国の国家機関と関連を有する外国人等の情報の提供を地方自治体に期待することは困難であろう。

上記の観点から、警察や地方自治体との情報共有のみでは不十分であり、自衛隊が独自に個人情報を収集することは不可欠と考える。当然ながら、両組織と自衛隊が協力関係にあり、収集領域が重複する可能性、あるいは相互の情報共有が不可欠であることは言うまでもない[32]。

31 警察の主力は都道府県警察であり平素は警察庁による一元的な指揮統制下にはないという特性がある。加えて、警察活動の大部分は刑事警察活動であることから公安情報の収集に当たる警察官数は極めて限定される。一方で自衛隊は内閣総理大臣の一元的な指揮権の下、国内外において機動的に作戦を展開するため、警察が自衛隊の作戦行動に追随しながら情報を随時随所に提供することは組織態勢上困難である。従って、個別具体的な作戦行動においては自衛隊自らが収集を行う必要が生じると言える。特に、有事になれば警察活動が困難な地域が生じる蓋然性は極めて高く、その必要性は高まると言えよう。

32 警察も警察庁などで一部国外情報を収集するほか、外国国家機関と関連する者の情報が犯罪者の情報と関連する可能性は高く、警察との情報共有は極めて重要性が高いと考えられる。また、自治体で正規に登録された地域住民の個人情報は、災害派遣等で必要なほか、自衛隊が必要な情報を効率的に取集するためのスクリーニングの観点からも有益と考えられる。

3. 個人情報保護法制と安全保障法制の関係

（1）各国の国内法の状況

前述の通り、個人情報保護法制度は各国の国内法を中心に発達してきた。1980 年に OECD にて「プライバシー保護と個人データの国際流通についてのガイドラインに関する OECD 理事会勧告」が採択されたことを皮切りに、各国はそれぞれ国内法の整備を進め、とりわけ EU における一般データ保護規則（General Data Protection Regulation、以下「GDPR」と表記する。））の登場は、その規制の厳しさから各国に大きな影響を及ぼしたと言える。

個人情報保護に対する各国の考え方は必ずしも一致しているとは言えず、国によって異なる側面がある [33]。特に EU と米国の間では認識の差異が顕著であり、GDPR の十分性認定をめぐり度々摩擦が生じていた。欧州司法裁判所は 2015 年に EU と米国のデータ移転に関するセーフハーバー決定を [34]、さらに 2020 年にも修正版ともいえるプライバシーシールドフレームワークを無効とする判断を下している [35]。この背景には前述の PRISM 等を使用した政府による個人情報の大規模収集への懸念が存在し、両者間の認識の差異を浮き彫りにした [36]。しかし、そのような状況においても、大部分の国が安全保障領域における政府・軍における個人情報の取得・利用に関してはそれぞれの個人情報保護法制において例外規定を設けている。その上で情報収集活動に関する個別の権限法等に基づき、政府・軍が収集・利用可能な個人情報の種類、収集手段等に一定の制約を設けている場合が多い。

EU では、個人情報保護は基本的人権の重要な一部として認識されており、政府機関であっても厳しい規制が課せられる。ただし、GDPR 23 条は安全保障等の領域では国内法による個人情報保護の制限を認めており、これを受け、EU 加盟各国の国内法は安全保障上の政府の活動は個人情報保護の対象外とする [37]。また、政府等に

33 諸外国の個人情報保護法制に関する動向は以下を参照。近藤里南「個人情報保護法制に関する欧米の動向 ―立法措置と監督機関の比較―」『調査と情報』1216 号（2023 年 2 月）。

34 Case C-362/14, Maximillian Schrems v Data Protection Commissioner ECLI:EU:C:2015:650.

35 Case C-311/18, Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems, ECLI:EU:C:2020:559.

36 渡辺翔太「欧州司法裁判所 Schrems II 事件判決が越境データ流通に与える影響の考察―我が国の推進する DFFT 構想への影響を中心にして―」RIETI 独立行政法人経済産業研究所 https://www.rieti.go.jp/jp/publications/summary/21070017.html。なお、米国と EU 間では 2023 年に米欧データ・プライバシー・フレームワークが成立し、EU から米国への個人データ移転を合法的にできることなったため、両者間の差異は縮小していると評価できる。米欧データ・プライバシー・フレームワークの詳細については下記を参照。斉藤邦史「欧米データ・プライバシー・フレームワーク」『ジュリスト』1593 号（2024 年 2 月）34 頁。

37 一例として、ドイツの連邦データ保護法（Federal Data Protection Act）23 条 (1) は国家安全保障における個人データ処理の例外を認める。また、英国のデータ保護法（Data Protection Act, EU 離脱前の 2018 に制定）も 26 条において国家安全保障と国防における例外を定める。

よる情報収集に関する権限法の一例として英国は、捜査権限規制法（Regulation of Investigatory Powers Act 2000）により国内外の通信傍受を規定し、さらに 2016 年には調査権限法（Investigatory Powers Act 2016、以下、「IPA」と表記する。）[38] を成立させ政府の権限を拡大している。特に IPA は、受信及び発信者の一方が海外の場合、情報機関に対し特定個人を対象としないバルク・パーソナル・データセットの収集権限を付与する。バルク・パーソナル・データセットとは大量の個人データが収録されている電子的なデータベースのことであり、医療情報のようなセンシティブ・データも含むとされる [39]。一方で、収集にあたっては国務大臣が発出する令状が必要とされる。さらに、その令状発出には司法部門の出身者から選出される司法コミッショナーの承認を要するとされる等、運用にあたって厳格な要件が設けられている [40]。

ドイツでは、信書、郵便及び電気通信の秘密の制限に関する法律（基本法 10 条関係法、Gesetzzur Beschränkung des Brief-, Post-und Fernmeldegeheimnisses, Artikel 10-Gesetz）に基づく国内の通信傍受が、また、対外的な情報収集に関して連邦情報庁（BND））による同法及び連邦情報庁法（Gesetz über den Bundesnachrichtendienst (BND-Gesetz)））に基づく監視活動が可能となっている。また、米国同時多発テロ事件を受け 2002 年に成立した、第 2 次テロ対策法（Gesetz zur Bekampfung des Intemationalen Terrorismus）は情報機関に対して、民間の通信事業者や金融機関、航空会社から国際テロ防止のために必要な個人情報を収集する権限を与えている [41]。加えて 2006 年 12 月より施行されたテロ対策データベース法では情報機関等が収集するテロ組織及びその支援集団の加入者及び支援者等の基礎データ（氏名、旧姓、他の名前、仮名、異なる表記による氏名、性別、生年月日、出生地、出生国、現国籍及び旧国籍、現住所及び旧住所、身体的な特徴、言語、方言、写真、身分証明書に関する事項）及び拡張基礎データ（通信端末機の番号等、電子メールアドレス、銀行口座、登録車両、家族状況、民族、宗教、爆薬や銃器の製造や取扱いに関する知識等）情報をデータベース化し警察等と共有することを認める [42]。一方で、情報機関等による活動は連邦議会の議員から構成される議会監督委員会による監督下に置かれ、情報入手状況について議会監督委員会に報告が義務付けられている [43]。

38 なお、英国は 2021 年に EU を離脱しているが、法案成立時の状況として EU 諸国に含めている。
39 田川義博「英国 IPA2016 と調査権限をめぐる司法判断 ～調査権限（ガバメント・アクセス）の人権制約の許容度を探る～」情報セキュリテイ大学院大学（2024 年 4 月）22 頁、https://lab.iisec.ac.jp/~hayashi/240507.pdf。
40 同上、25 頁。
41 渡辺富久子「ドイツにおけるテロ防止のための情報収集」『外国の立法』269 号（2016 年 9 月）26 頁。
42 同上、28 頁。
43 小川原「ドイツにおけるテロ・過激主義とテロ対策」42 頁；渡辺富久子「ドイツの連邦情報庁法―対外情報機関の活動の法的根拠」『外国の立法』275 号（2018 年 3 月）58 頁。

米国では個人情報保護そのものよりは政府からの自由、即ちプライバシーの保護に重きが置かれており、個人情報の取扱いは各分野ごとの規制による。このため、統一した基準を定めた連邦法等は未整備である。プライバシー保護法（The Privacy Act of 1974）[44] が政府等によるプライバシーを侵害する情報の収集を禁止しているが、刑事捜査及び対外諜報活動に関しては例外規定が設けられている。また、政府による情報収集の権限を定めたものとして、外国の情報収集活動に関する法的枠組みである外国情報監視法（Foreign Intelligence Surveillance Act、以下、「FISA」と表記する。）[45] が存在し、通信情報を取得可能な対象に関する制限を設けている。FISA は、主に非米国人である外国勢力及び外国勢力のエージェントに対する政府による電子的監視を認めるものであるが、これらの勢力に関係する米国人も対象とされている [46]。FISA では基本的に司法長官からの許可及び外国情報監視裁判所（FISC）による監視命令の発出を必要とする。しかしながら、FISA は米国人と非米国人とでは手続きに明確な差異を設けており、申請時に求められる情報が異なるほか、非米国人間等での通信傍受等、米国人が対象ではない場合は FISC の監視命令が不要とされる [47]。これらの活動において収集可能な情報の内容に関する規定はないが、メタデータだけでなく通信内容までも把握可能であることから、アドレス・電話番号等の基本的な情報だけでなく、顔画像等の生体認証情報、さらには交友関係等の広範な個人情報を収集していると考えられる。また、連邦軍が国外で作戦行動を行う場合は、基本的には行動は軍法により規定され、米国内法の制約を受けない。このため、国外で作戦を行う軍の情報部隊などはほぼ無制限での個人情報を収集可能と考え得る。

総括すれば、多くの国が、個人情報保護に関しては安全保障目的による政府等の活動を適用対象外とする一方で、無制限な権利侵害が発生しないよう一定の制約を課す法制度及び議会・司法による監督枠組みが整備されていると言える。

（2）日本における個人情報保護法制度

日本で最初に制定された個人情報保護法である、行政機関の保有する電子計算機処理に係る個人情報の保護に関する法律は、行政が保有する電子データのみが対象であった。しかし、その後民間部門にまで保護が拡大され、直近では、令和３年度のデ

44 U.S.C. § 552a (2012).
45 50 U.S.C. ch. 36.
46 川澄真樹「対外諜報目的での電子的監視―アメリカ合衆国の FISA を題材として―」『比較法雑誌』第 50 巻第 3 号（2016 年 12 月）280 頁。
47 川澄真樹「国家安全保障のための対外諜報目的での電子的監視法制定に向けての一考察」『法学新報』第 127 巻 9･10 号（2021 年 3 月）300 頁。

ジタル社会形成整備法案による個人情報保護法改正（令和 4 年 4 月 1 日一部施行）により、それまで公的部門と民間部門で別々となっていた法律が一本化されることとなった。

個人情報保護法第 5 章は行政機関による個人情報の取扱いを定める。関連する主要な規定について概観すると、まず 61 条「個人情報の保有の制限等」[48] において、行政機関による個人情報取扱いにあたって、当該個人情報の利用目的を特定し、利用目的を超える保有及び利用目的変更に関する制限が規定されている。利用目的の特定に関し、判例等からは個別具体的なものであり、保有する個人情報は利用目的と適切な関係を有することが必要とされる [49]。次に、個人情報の取得に関し、64 条「適正な取得」は「行政機関の長等は、偽りその他不正の手段により個人情報を取得してはならない。」とし、取得手段に制約を設けている。「偽りその他の不正な手段」が具体的にどのような手段を指すかは明確ではないが、一般的に「不正な手段」とは、暴行・脅迫等の手段により取得した場合、個人情報の取得について定めた個別の法令に違反して取得した場合等であるとされる [50]。個人情報の利用に関しては、69 条「利用及び提供の制限」により、法令で明示された場合を除く目的外利用及び第三者提供を原則禁止し、同条 2 項 1-4 号において例外事由を定める。この内 2 号及び 3 号は、法令が定める事務又は業務に必要な限度において、かつ「相当な理由」がある場合、行政機関内部での目的外利用及び他の行政機関等への提供が可能であることを定める。「相当な理由」とは、行政機関の恣意的な判断を許容するものではなく、社会通念上、客観的にみて合理的な理由があることが求められるとする [51]。ただし、その判断は当該行政機関の長等が行うため恣意的な判断を生みかねないとの指摘が考え得る [52]。また、同条 2 項本文において、「本人又は第三者の権利利益を不当に侵害するおそれがあると認められるときは、例外的な利用・提供は認められない」とする例外の例外規定が存在する。「本人又は第三者の権利利益を不当に侵害するおそれがあると認められるとき」が具体的にどのような場合かは不明確であるが、犯罪歴等の具体的な不利益が明確に予想できる場合等が考え得る。なお、当該規定は「できる」規定であり、提供にあたっては、提供側の判断に依ることになることは留意が必要である。

上記以外にも行政機関における個人情報取扱いに関しては多数の規定が存在する

48 保有とは「作成、取得、維持・管理を含む概念」とされる。行政機関電算機個人情報保護法 4 条 1 項及び石井夏生利他『個人情報保護法コンメンタール』（勁草書房、2021 年）1023 頁。
49 仙台高判平成 28 年 2 月 2 日判例時報 2293 号 18 頁。
50 宇賀克也『新・個人情報保護法の逐条解説』（有斐閣、2021 年）460 頁。
51 石井『個人情報保護法コンメンタール』（勁草書房、2021 年）1028 頁。
52 同上、1028 頁。

が、安全保障における例外規定が存在しないことは他国と大きく異なる点である。また、個人情報保護委員会によれば、個人情報保護法の保護対象は居住地や国籍を問わないとされる。また、日本にある個人情報取扱事業者及び行政機関等が取り扱う個人情報は、個人情報保護法による保護の対象となり得るとされており、国内領域だけでなく外国領域にある外国人にも適用されることも留意が必要である[53]。極端な例では、外国兵士やテロリストの個人情報も保護の対象となり得るということである。これらの点は、後述するが、日本の国内法においては、安全保障目的での情報収集活動に根拠法がないこともあり、行政機関による安全保障を目的とした情報収集活動を大きく制約するおそれがある。

（3）日本の安全保障法制と個人情報保護法制との関係

次に、日本の安全保障法制の概要と個人情報保護法制との関係について述べる。まず、安全保障法制上の大きな特色として、平素の自衛隊には国外・国内を問わず特別な行動権限が一切付与されていない。これは、情報機関や軍が平素から積極的な役割を担う諸外国と大きく異なる点である。また、憲法において緊急事態条項がないことも大きな特色である。これは、武力攻撃事態においても現行国内法制度が継続的に適用され続けることを意味し、自衛隊は平素において権限がないだけに留まらず、武力攻撃事態においても平素の国内法秩序に基づく行動を要求されるということであり、個人情報保護法も例外ではない。仮に武力攻撃事態が発生し、自衛隊が外国からの武力攻撃を排除あるいは国内治安維持活動を行うに際し必要な情報収集活動を行うにあたっても、個人情報保護法を無視することはできないということである[54]。加えて、行政機関そのものに他国のような安全保障上の理由による情報収集活動に関する明文上の根拠法令が存在しないことも大きな特色である。一般に、行政機関の行為の全てに根拠法令が必要とされる訳ではなく任意の範囲かつ当該行政機関の責務の範疇であれば可能とされ[55]、そのような行政機関が行う法令根拠のない情報収集活動は、行政法上は任意調査活動として整理されている[56]。任意とは「強制に渡らない」程度と解されているが、かならずしも明示的な同意が必要とされるものではなく、一定の有形力行使ですら認められる場合がある[57]。一方で、本人が認識できないような態様かつ有形力の

53 個人情報保護委員会 HP、https://www.ppc.go.jp/all_faq_index/faq1-q1-6/。
54 武力攻撃事態が認定され自衛隊法 76 条「防衛出動」が発令された場合、自衛隊には各種の行政法の適用除外が個別に規定されているが個人情報保護法は含まれていない。
55 塩野宏『行政法 I〔第六判〕行政法総論』（有斐閣、2015 年）259 頁。田村正博『警察行政法解説』第 2 版補訂版（東京法令出版、2019 年）333 頁。仙台高判平成 28 年 2 月 2 日判例時報 2293 号 18 頁。
56 宇賀克也『行政法概説 I 行政法総論』第 7 版（有斐閣、2020 年）146 頁。
57 最決昭 51. 3. 16 刑集 30 巻 2 号 187 頁。

行使を伴わない行為であっても、「通信の秘密」やプライバシーを侵害する行為は強制処分に該当すると解されており任意調査活動では実施できないとされる[58]。この点は、個人情報保護法 64 条「適正な取得」と相俟って、行政機関による情報収集活動に大きな制約を課している。また、情報収集活動の根拠法がないことは、個人情報保護法 69 条「利用及び提供の制限」において大きな問題となる。同条では目的外利用及び第三者提供は法令によることが原則とされるため、自衛隊内部での個人情報の利用や警察・自治体等の他の行政機関との情報共有に支障を来たすおそれがある。

ただし、武力攻撃事態が認定され防衛出動が発令された場合は、自衛隊に対して自衛隊法（以下、「隊法」と表記する。）88 条「武力の行使」に基づく包括的な軍事作戦の実行権限が付与される。情報収集活動が上記規定の要件に該当する場合は法令行為と整理される。しかしながら、基本的に隊法 88 条は戦闘地域における敵国軍隊への権限行使を念頭においた規定とされ、日本国民や直接戦闘に関係しない外国人（以下、「日本国民等」表記する。）に対する自衛隊の活動への適用は想定されていないとされる[59]。従って自衛隊による日本国民等に対する情報収集活動は隊法 88 条では正当化されない可能性が高い。この場合、日本国民等への自衛隊による権力行使は、同法 92 条 1 項「公共の秩序の維持のための権限」に依ると考えられる[60]。しかしながら、同権限は警察官職務執行法の準用であり、明示的に情報収集活動の具体的権限を規定した文言は含まれていないことから、根拠法令となり得ないと考えられる[61]。

総括するならば、武力攻撃事態が認定されるまでの間は、外国人を含めて個人情報を取得するための情報収集活動を行う法的根拠がなく、目的外利用及び第三者提供も制約を受けることになる。また、武力攻撃事態認定以降も、戦闘地域における敵国軍隊への権限行使以外においては平時と変わらないということになる。

4. 自衛隊による情報収集活動と個人情報保護における課題

（1）自衛隊が収集する個人情報

次に、自衛隊が個人情報を収集・利用する具体的な場面を想定し、個人情報保護法

58 最大判平成 29 年 3 月 15 日刑集 71 巻 3 号 13 頁。最決平成 11 年 12 月 16 日刑集 53 巻 9 号 1327 頁。川出敏裕『判例講座刑事訴訟法〔捜査・証拠編〕〔第 2 版〕』（立花書房、2021）228 頁。

59 宮崎弘毅「防衛二法と自衛隊の任務行動権限 -3-」『国防』第 27 巻第 2 号（朝雲新聞社、1978 年）94 頁。

60 同上。

61 情報収集活動の対象が、何らかの自衛隊に関連した刑法犯に該当する可能性がある場合は、自衛隊警務隊による刑事訴訟法に基づく情報収集が可能である。ただし、一般の自衛官は司法警察職員ではないため刑事訴訟法に基づく監視・情報収集活動は実施できない。

制との関係における具体的な問題点を考察する。これまで述べてきた諸外国の状況及び日本における安全保障と個人情報保護の関係を踏まえ、自衛隊における個人情報の取扱いと作戦行動との関係を整理すると下記の表1のようになると考えられる[62]。

表1　自衛隊が収集することが想定される個人情報の一例

<table>
<tr><th rowspan="2">区分</th><th rowspan="2">対象地域</th><th rowspan="2">対象者</th><th colspan="2" rowspan="2">利用目的</th><th rowspan="2">取得する個人情報の一例</th><th rowspan="2">取得手段</th><th colspan="2">関連法規</th></tr>
<tr><th>平　時</th><th>有　事</th></tr>
<tr><td rowspan="2">①</td><td rowspan="2">国外（敵国領域）及び国内戦闘地域</td><td>➢外国の軍隊の構成員
➢敵対行為に直接参加する者</td><td>ターゲティング</td><td>直接の攻撃目標として対象を選定、攻撃</td><td>➢ 個人識別符号（生体認証情報）
➢ 行動パターン
➢ 通信情報</td><td rowspan="4">➢ HUMINT
➢ SIGINT
➢ IMINT（無人機・衛星等）
➢ OSINT
➢ サイバー</td><td rowspan="2"></td><td rowspan="2">隊法88条の限度で情報収集可能
➢ ただし、適用基準及び限度が不明確</td></tr>
<tr><td>➢偽情報等の発信者
➢スパイ行為実施者</td><td>情報作戦</td><td>敵対国からの印象操作、情報操作に対応</td><td>➢ SNS等での発信
➢ 交友関係
➢ 通信情報
➢ 個人識別符号</td></tr>
<tr><td>②</td><td>日本国内</td><td>➢対象国や対象組織と関係を有する国内所在外国人等</td><td>情報保全業務
情報作戦</td><td>テロ・破壊活動、スパイ活動等の自衛隊の作戦行動を阻害する行為の防止</td><td>➢ SNS等での発信
➢ 交友関係
➢ 生活パターン
➢ 犯罪歴
➢ 通信情報
➢ 個人識別符号</td><td colspan="2" rowspan="2">監視・情報収集活動の根拠法令なし
個人情報保護法の保護対象
➢ 個別具体的な利用目的が必要
➢ 法令に違反する収集手段の使用は不可能
➢ 目的外利用・第三者提供に制約
※平時と有事の区分は情報収集に関する法的権限の差異からの整理であり、具体的には有事は武力攻撃事態を指し、平時はそれ以外の状況（治安出動等を含む）である。</td></tr>
<tr><td>③</td><td>日本国内</td><td>➢ 所在住民（国籍問わず）</td><td>災害派遣
国民保護</td><td>避難の実施及び避難措置の効率化、緊急時の救命処置等</td><td>➢ 個人識別符号
➢ 正確な所在地
➢ 健康情報</td></tr>
</table>

（出所）筆者作成。

（注）情報保全業務とは秘密保全、隊員保全、組織・行動等の保全及び施設・装備品等の保全並びにこれらに関連する業務をいう[63]。

上記表は、自衛隊が平時から有事にかけて個人情報を取扱うことが必要となる個人情報に関し、対象地域、対象者、利用目的、取得する個人情報の一例及び法的評価の観点から整理したものである。このうち、区分③の災害派遣及び国民保護目的での個人情報の収集・利用は、基本的には警察及び地方公共団体が主となるが、戦闘地域近傍において警察等が活動できない場合、自衛隊自ら収集しなければならない可能性がある。しかしながら、本人の利益となることが明確であることから大きな議論は生じないと考える。

一方、区分①は主に戦闘行為が発生する可能性がある地域であるため、自衛隊の作戦行動を妨害する等、敵対行為に直接参加する外国人等を正確に識別するための生体認証情報や行動パターン、通信情報等の高いレベルでの個人情報が必要になる。

62 なお表1の考察の前提として、いずれの区分も現行の安全保障法制の枠組みに従い警察力のみでは対処できない状況において自衛隊が作戦行動を行っている場面を想定している。
63 防衛庁訓令第7号「情報保全業務の実施に関する訓令」平成15年3月24日。

しかしながら、有事において自衛隊が必要な情報収集活動を行うための根拠法令となる隊法 88 条が存在するため、法的には大きな問題は生じないと考えられる。隊法 88 条は、武力攻撃認定前は適用できないことや適用基準が不明確という課題は存在するものの、自衛隊が有事において必要な情報収集を行うための一定の法的基盤は整備されていると考えられる。

大きく問題となるのは区分②のケースである。この場合は、外国からの間接侵略等が発生し警察力による対応を超える事態であるものの、戦闘行為等が発生していない状況が想定される。治安出動あるいは公共の秩序維持等の自衛隊の作戦行動を阻害するテロ、破壊活動及びディスインフォメーション活動等に従事する者の個人情報として、SNS や通信情報から発信者を特定することや、対象国や対象組織との関連性を確認するための行動パターンや交友関係といった個人情報が必要となる可能性がある [64]。しかしながら、これまで繰り返し述べた通り、平時・有事を問わず自衛隊には戦闘地域を除き国内で情報収集活動を行う法的根拠が存在しない。その一方で、個人情報保護法による保護は外国人まで含めて極めて広範囲に及んでおり、法令を文字通りに解釈した場合、平時のみならず、有事においても自衛隊による個人情報の取得・利用、警察・自治体等との情報共有に大きな制約が生じる可能性が高い。特に、有事に国内に所在する外国人の個人情報に関し、自国民と同等の取扱いが求められる点については検討の余地があるものと考える。外国人の基本的人権に関する著名な判例であるマクリーン事件 [65] において最高裁判所は、外国人に対する基本的人権の保障は外国人在留制度の枠内で与えられているに過ぎないとし、国家の裁量を比較的広くとらえる見解を示している。従って、安全保障の観点から外国人の個人情報保護に対し一定の制限を加えることは著しく不合理とは言えないであろう [66]。しかしながら上記判例は「権利の性質上、日本国民のみをその対象としていると解されるものを除き外国人にも保障が及ぶ。」とも示しており、具体的な理由なく外国人に対する情報収集活動を無制限に行うことは許されないとも考えられるため、明確な基準が設けられるべきであろう。以下、個人情報の取得、利用のそれぞれの場面における問題点を考察する。

（2）自衛隊による本人同意を得ない個人情報の取得

具体的な課題を検討するにあたって、表 1 区分②における平時の場面を想定する。

64 前述の通り、自衛隊自ら行う収集活動の対象となるのは対象国や対象組織と関係のある外国人等であり、かつ地理的にも自衛隊が作戦行動を行う地域周辺に限定される。
65 最大判昭和 53 年 10 月 4 日民集 32 巻 7 号 1223 頁。
66 安全保障に関連した外国人の基本的人権の規制については以下を参照。杉山幸一「外国人等の権利保障とその規制について－経済的自由をめぐって－」『憲法研究』52 号（2020 年）。

具体的には事態が緊迫し、国内における反政府活動等が活発化、自衛隊情報保全隊等による情報収集活動が行なわれる場面である。

このような場面では多くの課題が考えられるが、第一に、個人情報を保有するにあたっての利用目的の特定が困難という問題が挙げられる。個人情報保護法61条により、個人情報を保有するにあたっては利用目的の特定が必要である。しかし、いずれの事態も認定されていない平素の段階において、さらに自衛隊に特定の任務が付与されていない場合、具体的な利用目的を説明することは困難と考えられる。前述の監視差止請求では、自衛隊のイラク派遣活動という具体的な行動に伴う情報収集活動については合法とされたものの、イラク派遣とは無関係な反原発運動や消費税反対活動等への参加者に関する個人情報の取得は違法とされている[67]。また、公安テロ情報流出被害国家賠償請求事件においても、当時イスラム過激派によるテロ事件が東南アジア周辺において発生していた状況、日本がテロの対象となり得るとの声明、イスラム過激派組織の幹部による不法滞在や在日米国大使館へのテロ計画等に関する供述等の複数の具体的な兆候の存在を踏まえ、日本が「日本国内においてイスラム過激派による国際テロが発生する危険は十分に存在していた」とする具体的な事情が考慮された上で情報収集活動の合法性が認められている[68]。これらの裁判所の判断を踏まえれば、反政府活動等への参加等の理由のみで個人情報を取得することは困難と考えられる。

次に、取得手段の制約の問題が考え得る。情報収集活動の根拠法令の不存在及び個人情報保護法64条に基づき、法令に抵触する手段は禁止されると解される。諸外国で一般的に行われている裁判所の令状無しでの通信傍受、ハッキング等の不正アクセス行為を用いた個人情報の取得は外国人に対してであっても禁止される。また、同条が規定する「偽り」が意味するところが不明確であり、フィッシングメールを用いたソーシャルエンジニアリング、身分を詐称したダークウェブへの潜入や、偽りのサイトを構築しハニーポッド等を設置する等の方法による個人情報の取得に関しては合法か違法かが不明確となっている。

また、第三者からの情報提供の場合にも大きな制約が存在する。警察及び地方自治体は地域における個人情報を大量に保有しており、自衛隊の活動においても両組織からの情報提供は必要不可欠である。しかしながら、個人情報の提供側は前述の通り個人情報保護法69条「利用及び提供の制限」に従うことになる。特に反自衛隊活動を監視する目的での個人情報の提供依頼は、本人の「権利利益を不当に侵害」するとし

67 仙台高判平成28年2月2日判例時報2293号18頁。
68 東京地判平成26年1月15日判例時報2215号30頁。

て提供を拒否される可能性は高い[69]。特に重大な問題として有事における敵国籍保有者に関する個人情報の取得を挙げる。多くの国が平素から外国人に対する情報収集活動に関し自国民より緩やかな制約を課す法律を制定している。また、国際人道法においては、武力紛争間は自国の安全の観点から絶対的な理由がある場合、敵国籍保有者に対する抑留及び居住地指定を行うことが認められている[70]。一方で、日本の国内法上は武力攻撃事態認定以降も敵国籍保有者の個人情報の取得に関し日本国民と同等の制約が課されることになる。

（3）個人情報の目的外利用（軍事利用）への制約

次に、有事における個人情報の目的外利用を考察する。一例として情報作戦やスパイ活動に自衛隊が対処する場面を考える。情報作戦やスパイ活動は外患援助罪等の国内刑法や特定秘密保護法等に違反しない様態で行われた場合、刑事捜査としての対応は実施できないうえ[71]、有事において警察力が期待できない場合も考え得る。そのような場合、自衛隊が上記活動に独自に対処する必要性に迫られる可能性があるが、国民保護名目等で取得した個人情報を利用すれば、上記活動に関与する者を特定することが容易になる可能性がある。具体的には警察や地方公共団体から国民保護等の名目で入手した生体認証情報を含む地域住民の詳細な個人情報を通信情報等と照合したデータベースを構築し、外国や外国人からの不審なアクセスやメッセージ等の働きかけを監視すれば、上記のような不利益活動を行う者を特定できる可能性が高まる。特定した者の情報をインターネット上で共有し注意喚起を行うことでディスインフォメーション等による住民の動揺を防止し、あるいは当該人物の駐屯地や重要防護施設等へのアクセスを禁止することで自衛隊の作戦行動の保全にも活用できる可能性がある。

しかしながら、前述の通り個人情報保護法 69 条は、行政機関内における目的外利用に対し、法令による場合を除き「相当の理由」がある場合かつ「本人又は第三者の権利を不当に侵害するおそれ」がない場合に限定しているため、個々のケースに応じた慎重な判断が必要である。ただし、この場合の判断権者は「組織等の長」である防衛大臣の判断で可能であり、また「本人又は第三者の権利を不当に侵害するおそれ」についても国防に従事する自衛隊の活動であることを踏まえれば一定の公益性がある

69 自衛官募集業務に対する地方公共団体による自衛隊への応募適齢者の提供に関し、個人情報保護法に違反するとの指摘がある。前田定孝「自治体が保有する個人情報の外部提供」『三重大学法経論叢』第 40 巻第 1 号（2022 年 10 月）。
70 ジュネーブ第Ⅳ条約 42 条。
71 一例として、ディスインフォメーション活動は名誉棄損等の刑法上の個別の犯罪類型に該当しない限り違法性はなく、取締りの対象外となる。

と考えられる。このため、行政訴訟等が提起されても国（防衛省・自衛隊）の活動の正当性が認められる余地は少なくないと考える。しかし、懸念すべきは、事態への即応が求められる場面において、多数発生する個別案件に関し、その都度法的判断を自衛隊に求めることが果たして現実的かという点である。明確な基準がない状態で法令の専門家ではない自衛官に判断をゆだねることは、濫用による権利侵害の可能性や、あるいは逆に必要な情報収集活動を躊躇させることにもつながりかねないと危惧される。

5. 具体的な取り組みに関する提言

本稿では、自衛隊による個人情報の取扱いを具体的な例とし安全保障法制と個人情報保護法制の間に存在する法的課題を検討してきた。本稿では、前項までの考察を踏まえ、安全保障を目的とした自衛隊における個人情報の取扱いに関し、具体的に取り組むべき内容について以下の三項目を提言する。

① 自衛隊法改正等による武力攻撃事態時の個人情報保護法適用除外を明記
② 安全保障を目的とした情報収集の根拠令を整備
③ 権利侵害を防止する組織的統制要領の枠組み確立

（1）自衛隊法等改正による武力攻撃事態時の個人情報保護法適用除外を明記

武力攻撃事態時の個人情報保護法の収集、利用、第三者提供等に関する規定の適用除外を隊法に明記すべきである。本文中で確認したように、平時の法制度が有事においてもそのまま適用されることは現実的に大きな問題を孕む。国際法及び各国の個人情報保護法制が安全保障における適用除外規定を設けていることは、一定の合理性があると考える。現状において、自衛隊が他国の軍隊と同様の監視・情報収集活動を実施する権限がないことは明白であり、最低限、防衛出動時における個人情報保護法の適用除外規定や特定の外国籍保有者に対する例外等も認められるべきと考える。さらに、他機関や他省庁も含めた安全保障全般での情報収集の観点からは、自衛隊法の改正に留まらず個人情報保護法自体の法改正等も検討が必要であろう。

（2）安全保障を目的とした行政機関による情報収集活動の根拠法整備

本文中で考察した通り、根拠法の不存在は、国民の権利侵害に容易につながるだけでなく、行政機関による迅速な対応をも阻害する可能性がある。これは自衛隊だけではなく日本の行政機関全体の課題と考える。このため、政府及び各行政機関による安全保障上の情報収集活動を統括する根拠法の整備が急務と考える。この際、平時から有事までの一連の状況を想定するとともに、国民の権利を不当に侵害しないように十分な配慮を盛り込むことが必要と考える。濫用による国民の権利侵害を防止するための具体的な内容として、情報収集の目的、使用可能な手段・限界、各行政機関の役割区分及び適正な手続き及び保障が明文で規定されることが必要と考える。また手続きの制定においては、司法の関与を考慮することが重要であり、刑事捜査と同様の裁判所からの令状発行等の枠組みについて検討することが必要である。特に、通信情報の取得にあたっては、他国の制度を参考に、武力攻撃事態等の緊急時を除き、原則として令状に基づくものとするべきであろう。

（3）権利侵害を防止する組織的統制要領の枠組み確立

権利侵害を防止するための手段として、情報収集活動の根拠法制定のみではなく、有事においても個人情報保護制度の目的を維持できる実効性ある体制・態勢作りを目指すべきと考える。具体的には、第三者機関である個人情報保護委員会に対し、防衛省・自衛隊を含む行政機関の行動に対する指導・監督権限を強化することが考えられる。一例として、行政機関による個人情報ファイルの保有に関する個人情報保護委員会に対する事前通知について、国の安全に関する個人情報ファイルは除外されているが、この規定を見直し、有事においても例外なく個人情報保護委員会が行政機関の保有する個人情報の取扱いに関し適時適切に監督・指導できる権限を付与する等の処置が考え得る。

また、組織面の観点ではサイバーセキュリティ分野における個人情報保護委員会と関係省庁・機関との連携枠組みが参考になる。セキュリティインシデント発生時に内閣官房内閣サイバーセキュリティセンター（NISC）、警察庁サイバー警察局、独立行政法人情報処理推進機構（IPA）は、必要な情報共有を行うための連携に関する覚書を締結[72]している。同様の試みを安全保障領域でも実現し、防衛省・自衛隊と個人情報委員会の間で個人情報取扱いに関する協定を結ぶことも一案と考える。

また、上記制度的枠組を担保するために、積極的な司法の関与を検討すべきと考える。

72 個人情報保護委員会 HP、https://www.ppc.go.jp/personalinfo/legal/supervision/。

日本においては行政に対する司法の関与が限定的であり、行政訴訟等の事後的な対応が主体であるが、個人情報保護は被害者が感知しづらい側面がありじ後的な救済では権利侵害を防止できないと考える。前項で述べた令状発行等も含めた、安全保障上の活動に対する事前の司法機関による承認制度等が必要であろう。

おわりに

個人情報の軍事利用は今後増々活発化するものと考えられ、自衛隊を始めとする行政機関による本人同意のない個人情報の収集・利用が拡大する可能性は否定できない。一方で、個人情報保護は確立された権利であり、例え安全保障の名目であっても明確な法的根拠なしに制限が許されるものではない。しかし、現状は、安全保障と個人情報保護の関係は諸外国に比し十分に議論・検討されているとは言い難い状況である。特に本稿で確認したように自衛隊による個人情報の取扱いに関する検討はほとんど行われていない。明確な基準がないことは行政機関による過度な収集や不適切な利用による不当な権利侵害を引き起こす可能性にとどまらず、行政機関が本来必要な情報収集活動を行なうことを躊躇し、安全保障上の対応に支障を来たす可能性も考えられ、早急な検討・対策が必要と考える。

（陸上自衛隊）