

公安テロ情報流出被害国家賠償請求事件

東京地判平成26年1月15日（第一審）、
平成23年（ワ）第15750号等

高橋 義人

はじめに

本件は、国際テロの防止を目的として、公安警察がイスラム・コミュニティを長期にわたって監視対象としていたこと、そして収集した個人情報を含む内部資料を大量に流出させたことについて、イスラム教徒である原告らが国と東京都を相手に国家賠償を請求した事案である。公安警察が、①個人情報を収集・管理（＝データベース化）したこと、②それを（故意または過失により）流出させ、さらに③それを放置して被害を拡大させたことの違法性・違憲性が争われた。本件の問題点は多岐にわたるが、まず注目されるのは公安警察による「監視活動」が憲法上どのように評価されたのかである。

そもそも「監視 surveillance」という言葉は国家間の諜報行為を意味するフランス語（surveiller）に由来し、19世紀のナポレオンのヨーロッパ遠征時に最初に使われたとされている。軍事の分野では「監視」は「諜報＝偵察 spying」とほぼ同義で使用され、この言葉には監視される対象への悪意が含まれている。したがって、人が監視されるときには敵意をもつ他者による可能性が高いといえる⁽¹⁾。もちろん現代の監視はすべて侵害行為になるわけではないが、市民生活にネガティブな影響があることも否定できない。現代の様々な領域で活用されている各種のデータベースは公私の部門における意思決定を改善し、個人の知識や理解を深めるためにも有

用である。しかし、これらデータが人間の行動を記録する場合には、自律・公正・適正手続・連帯・プライバシーなど市民社会の基本価値に対する脅威にもなりうる⁽²⁾。

とりわけ政府による監視を考える上でわかりやすいイメージは、20世紀のディストピア小説が描いた世界である。たとえば、オーウェル(George Orwell)は「ビッグ・ブラザー」が支配する権威主義的情報国家と監視の関係を、カフカ(Franz Kafka)は官僚組織による情報管理に対する個人の脆弱性を、ハクスリー(Aldous Huxley)は娯楽と快楽による環境管理型権力による現代的支配を描いた⁽³⁾。これら小説で描かれたように、政府は個人の私生活(人が弱さや不安を感じるような部分)にどのようにして侵入するのか、そしてどのように(どのような意味で)民主政治を浸食していくのかを考えれば、「監視」が提起しているのは、単に個人の権利・自由をいかに保護するののではなく、むしろ現代の政治のあり方に関わって公私の領域をどのように再定義するのかという問題だと思われる⁽⁴⁾。そこで本稿では、第一に監視が及ぼす直接・間接の作用の観点から、第二に情報の収集・保有における透明性の欠如の観点から、本件判決に含まれている憲法上の問題を整理・検証したい。

I. 事実の概要

1. 情報流出事件

2010年10月28日頃、公安警察の内部資料(114点)がファイル交換ソフトを通じてインターネット上に流出した。これら流出データは、11月25日までに20カ国の1万台以上のPCにダウンロードされたと考えられている。流出データには、2007年9月10日付けの「実態把握強化推進上の要点」などの標題文書をはじめとして、テロ対策に関わって警察が作成した内部資料が含まれ、それらのなかには在日ムスリムを対象として収集されていた個人情報的大量に含まれていた。具体的には、次のような項目が記入さ

れた資料である。

- ①「人定事項」（原票写真、氏名、国籍・本籍、出生地、生年月日、日本国内現住所、勤務先、使用車両、日本国内携帯電話番号・自宅電話番号など）
- ②「入国在留関係」（上陸年月日・旅券番号・旅券発行年月日・在留資格・本国住所・在留期間・登録年月日・登録市区町村・登録番号）
- ③「住所歴・学歴・職歴・勤務先歴」
- ④「家族交友関係」（家族の氏名・住所・勤務先・生年月日）
- ⑤「免許関係」（保有する免許種別・取得年月日・免許番号）
- ⑥「犯罪情報」（検挙年月日・罪名・検挙署・処分結果）
- ⑦「身体特徴」（身長・体格・ひげ・メガネ）
- ⑧「モスクへの立ち入り状況」、「立寄徘徊先」、「行動パターン概要」
- ⑨「容疑」と「対応状況及び方針」
- ⑩「所属団体」（名称・地位・役職・役割など）

データ流出後の10月29日には警察庁と警視庁は調査を開始して、12月に事件に関する「中間的見解等」をまとめているが、データ流出事件の事実関係はいまだ解明されていないままである⁽⁵⁾。

2. 裁判の概要・経緯

本件流出事件によって明らかになったのは、何ら犯罪が具体的に発生していないにもかかわらず、公安警察（警視庁公安部外事第三課）がイスラム諸国の関係者に対して無差別に組織的・包括的な情報収集＝監視活動を長期間にわたって行った上、しかもそれら個人情報を管理・利用していたことである。そこで、イスラム諸国出身者である原告らは、警視庁・警察庁および国家公安委員会が①監視活動によって原告らの信教の自由を侵害

したこと、②「行政機関の保有する個人情報の保護に関する法律」と「東京都個人情報の保護に関する条例」に違反して、個人情報を収集・保管・利用したこと、③それら個人情報をインターネット上に流出させ、適切な損害拡大防止措置をとらなかったことについて国家賠償法上の違法性を主張して、東京都と国を相手に損害賠償を求めた。具体的には、原告は次のような監視活動の実態を指摘した。

- a. 警視庁及び警察庁(以下、警察)は、イスラム諸国出身者の国籍・氏名・生年月日・住所などを横断的・網羅的・機械的・体系的に収集する作業を大規模かつ組織的に実施した。その際に、外国人を雇用している企業・会社への定期訪問、イスラム諸国出身者が経営する店舗への「巡回連絡」も行われた。平成20年5月31日時点で都内イスラム諸国外国登録数14254人のうち約12677人の個人情報が収集され、データ化された。その後も、同年7月に開催された北海道洞爺湖サミットにおけるテロ予防を目的として全国に拡大継続され、最終的にはイスラム諸国出身者約72000人(把握率98%)の個人情報が収集された。
- b. 警察は、平成20年6月23日以降、国際テロ対策として「モスク出入り者の不審動向」を発見するために「モスク班」(捜査員43名)を配置し、モスクを監視した(8:30~19:30)。サミット終了後もモスクへの網羅的な監視を継続した。
- c. 警察は、「イスラム関係団体等」(イスラム関係のNGO・NPO、食料品店、飲食店、イスラム関係企業)のイスラム・コミュニティを監視対象として各団体の所在地・代表者・財務状況などの情報を収集した。
- d. 警察は、照会文書なく都内レンタカー業者4社から利用者情報を収集したほか、ホテルから外国人旅券の写しを、銀行からイラン大使館職員給与振込履歴を、複数の大学からイスラム諸国留学生の個人情報を収集し、ムスリムおよびイスラム関係団体等から各種情報を収集した。

以上のような情報の収集と管理（＝監視活動）について、原告らは主として信教の自由（憲法20条）、信条に基づく差別の禁止（憲法14条）、「信仰内容・信仰活動に関する情報」を含めて「何人もその承諾なしに公権力によってみだりに私生活に関する情報を収集、管理されることのない自由」＝情報コントロール権（憲法13条）に対する侵害を主張した。

これに対して、東京地裁判決は、一方で公安警察による本件情報収集活動および情報の保管・分析など（データベース管理）について、「犯罪の予防をはじめとする公共の安全と秩序の維持を責務とされている警察」が「国際テロの発生を未然に防止するために必要な活動」だと判示した。同時に他方では、原告らの情報を流出させたことについては、警視総監に情報管理上の注意義務を怠ったという過失があること、したがって流出によって被告らのプライバシーや名誉などを侵害したとして、被告（東京都）の国家賠償法上の責任を認めた（国への請求は棄却）⁽⁶⁾。

II. 判決の要旨

1. 警察による個人情報の収集・保管・利用の違法性

①本件情報収集活動と原告らの信教の自由（憲法20条1項）の侵害

「国家によって信教の自由が侵害されたといえるためには、国家による信教を理由とする法的又は事実上の不利益な取扱い又は強制・禁止・制限といった強制の要素が存在することが必要である」。本件の情報収集活動は「あくまで任意の情報収集活動であり、それ自体が原告らに対して信教を理由とする不利益な取扱いを強いたり、宗教的に何らかの強制・禁止・制限を加えたりするものではない」。

それに対して、「日本国内において国際テロが発生する危険が十分に存在するという状況、ひとたび国際テロが発生した場合の被害の重大さ、その秘匿性に伴う早期発見については発生防止の困難さに照らせば、本件モスク把握活動を含む本件情報収集活動によってモスクに通う者の実態を把握

することは、警察法2条1項により犯罪の予防をはじめとする公共安全と秩序の維持を責務とされている警察にとって、国際テロの発生を未然に防止するために必要な活動である」。

本件情報収集活動は、「イスラム教における信仰内容それ自体の当否を問題視していることに由来するもの」ではない。「イスラム教徒のうちのごく一部に存在するイスラム過激派によって国際テロが行われてきたことや、宗教施設においてイスラム過激派による勧誘等が行われたことがあったことといった歴史的事実に着眼して、イスラム過激派による国際テロを事前に察知してこれを未然に防ぐことにより、一般市民に被害が発生することを防止するという目的によるもの」である。「イスラム教徒の精神的・宗教的側面に容かいする意図」ではない。

また、本件モスク監視は「捜査員が自らモスクへ赴いて、原告らのモスクへの出入状況という外部から容易に認識することができる外形的行為を記録したにとどまり」、強制に情報を入手したわけではない。よって、信教の自由に対する影響は「せいぜい警察官がモスク付近ないしその内部に立ち入ることに伴い嫌悪感を抱くこととなった」にすぎない。これらを総合すれば、本件情報収集活動は「国際テロの防止のために必要やむを得ない措置」として憲法20条に反しない。

②本件情報収集活動と「信条に基づく差別の禁止」(憲法14条)

警察が「少なくとも第一次的にはイスラム教徒であるか否かという点に着目して決していたこと」、「信教に着目した取扱いの区別をしていたこと自体は否めない」。「信教に着目した取扱いの区別に合理的な理由があるか否かについては、慎重に検討することが必要である」。

そこで検討すると、本件情報収集活動は「イスラム過激派による国際テロを事前に察知してこれを未然に防ぐことにより、一般市民に被害が発生することを防止するという目的によるものであり、イスラム教徒の精神的・宗教的側面に容かいする意図によるものではない」。また、原告らの

信教の自由への影響は「察官がモスク付近ないしその内部に立ち入ることについての嫌悪感にとどまる」。

したがって、「憲法14条1項後段の列挙事由にわたる区別であること」や「信教の自由の重要性を考慮しても、その取扱いの区別は、合理的な根拠を有するものであり、同項に違反するものではない」。そして「本件情報収集活動によって収集された情報が、外部に開示されることの全く予定されていないものであること」は明らかである。よって、「本件情報収集活動それ自体が、国家が差別的メッセージを発するものであるということとはできない」。

③本件情報収集活動と情報プライバシー（憲法13条）

「警察法2条1項により公共の安全と秩序の維持を責務とする警察には、国際テロ防止のための情報収集活動の一環として、モスクに出入りする各人について、その信仰活動を含む様々な社会的活動の状況を広汎かつ詳細に収集して分析することが求められるというべきである」。しかも、国際テロが発生した場合の被害の重大さを考慮すれば、「本件情報収集活動によって収集された原告らの情報が社会生活の中で本人の承諾なくして開示されることが通常予定されていないもの」だとしても、「本件情報収集活動は国際テロの防止の観点から必要やむを得ない活動である」。

「日本国内において国際テロが発生する危険が十分に存在するという状況」があるのに反して、「テロ事件に関する情報を事前に入手し、又は民衆に紛れたテロリストを発見して、国際テロの発生を未然に防止すること」は容易ではない。したがって「原告らが、その信仰内容や信仰活動に関する情報のみならず、犯罪歴等のプライバシーに関する情報について収集されたとしても、本件情報収集活動の上記性質等に照らし、やむを得ない制約に当たるといふべきである」。そして、情報収集は「違法又は特段不相当な方法」によるわけでもないから、憲法13条に反するとはいえない。

④警視庁・警察庁による個人情報保有と憲法13条

「情報収集活動は、当該活動によって得られた情報を蓄積し、分析するために行われるものである」。本件情報収集活動が憲法13条・20条に違反しない以上、「適法な活動により得られた情報を警察が保有して分析等に利用することができることは当然のことであるから、当該情報の保有が憲法13条に違反することはない」。

2. 個人情報が流出したことについての国家賠償法上の違法性

①被告東京都の国家賠償法上の違法性

本件流出データには「原告らがイスラム教徒であることを直接明らかにするのみならず、その信仰の深ささえも指し示す情報という、個人の内面ひいては人格的自律に直接関わる事柄や、犯罪歴という人の名誉、信用に直接に関わる事項まで含まれていた」。「これらの情報は、個人のプライバシーのうちでも最も他人に知られたくないものに当たるといえる」。そして、「そのような情報がいったんインターネット上に流出すると、その伝播性・波及性の高さから、不特定多数の者に伝播する危険があり、その情報のすべてを後から回収することも極めて困難で、ほとんど不可能である」。「警視総監には、情報管理上の注意義務を怠った過失があり、国家賠償法上違法であるといわざるを得ないから、この点について被告東京都は責任を負うというべきである」。

②被告国の国家賠償法上の違法性

「警察庁の監査責任者は、所要の通常監査を行っていた上、(インターネット上の情報流出事案について)考え得る対策を講じていた」といえるので、被告国の責任は認められない。

③本件流出事件発生後の被告らの不作為についての国家賠償法上の違法性

「その(流出したデータを全面的には削除することができなかった)原因は、本件流出事件において、海外のサーバーを多数経由するなど流出元

が容易に特定できない方法が用いられ、情報の回収が不可能とされるファイル共有ソフトであるウィニーが使用されており、流出した情報が掲載されたサーバー上のデータを警察が強制的に削除することはできず、海外のプロバイダーに任意の削除を求める方法しかとり得ないなどの複数の事情が相まったことによる」。これら事情を考慮すると、警視庁及び警察庁は「尽くすべき義務は尽くしたものとみるのが相当であり」、損害拡大防止義務を怠ったとはいえない。

III. 判決の検討

1. 情報収集活動の態様の問題

まず本件情報収集活動の実態について、裁判所は「原告ら個人がいかなる手段・方法によって個人情報を収集されたのか」を厳密に特定する必要はないが、「何らかの方法によって警察官に個人情報を収集されたこと自体は動かしがたい事実」と認めた点はまず注目されよう。ただ、同時に「原告ら以外のイスラム教徒やイスラム関係団体等に関していかなる情報収集活動が行われたか」は本件の判断とは無関係だと説示した。確かに警察の情報収集活動の詳細をすべて明らかにすることはできないとしても、公権力行使の違法性を判断するためには、目的に対して、問題となる情報収集の対象範囲や時間的な継続性、また具体的な情報収集の手段とそれが及ぼす影響などの様々な要素（時間・総量・性質・程度）を総合的に考慮しながら、その必要性や相当性を判断する必要があると思われる。

本件情報収集活動の実態は必ずしも明確ではないが、流出データを参照するかぎり、「物理的監視」のほかに「トランザクション監視」が行われていたことが推測される（図表1）⁽⁷⁾。

図表1【本件の監視類型】

物理的監視	a. 人	「イスラム諸国会議機構の国籍を有する者及びその他の国籍を有するムスリム」、「OIC諸国出身者約72000人(把握率98%)」
	b. 場所	都内の各モスク、外国人を雇用している企業、イスラム諸国出身者が経営する店舗などイスラム・コミュニティ全般
トランザクション監視	a. 「イスラム関係団体等」(イスラム関係のNGO・NPO、食料品店、飲食店、イスラム関係企業)などの各団体の所在地・代表者・財務状況等の情報。 b. 第三者からの情報=都内レンタカー業者大手4社から照会文書なしで利用者情報、ホテルから外国人旅券の写し、銀行からイラン大使館職員の給与振込履歴、複数の大学からイスラム諸国入留学生の個人情報など。 c. 収集した監視情報のデータベース化。	

被告は、このような情報収集活動の目的を「国際テロを未然に防止すること」であり、「一般市民に被害が発生することを防止すること」と説明し、そのためには「未だテロ行為が具体的に特定されていない時期から、一見テロとの関連性が乏しいような情報であっても幅広く情報を収集し、これらを分析する作業」は必要不可欠だと主張した。

高い秘匿性と情報の断片性という特殊性を有する国際テロの未然の防止のためには、①未だテロ行為が具体的に特定されていない時期から、②一見テロとの関連性が乏しいような情報であっても幅広く情報を収集し、③これらを分析する作業が必要不可欠である。その結果、ある個人や法人、施設等について、テロと何ら関わりがないことが事後に判明することもあるが、上記のようなやり方は、国際テロの上記特殊性を踏まえたうえで国際テロを未然に防止するためにやむを得ない方法というべきである。(下線・番号は引用者)

この主張からうかがわれる広範囲の包括的・網羅的・継続的な情報収集に

についての考え方にはいくつかの問題が含まれている。

まず①②について、本件情報収集は長期間にわたってイスラム・コミュニティ全体に向けて行われていたこと（継続期間と対象範囲）が問題となる。つまり、原告の主張によれば、都内のイスラム諸国の国籍保持者14245人のうち12677人の個人情報収集された。最終的には、全国的に拡大して継続された結果、およそ72000人が監視対象とされたという。加えて、テロが警戒された北海道洞爺湖サミット後も監視が継続された可能性もある。被告ら自身も認めているように、情報を収集・分析した結果、「ある個人や法人、施設等について、テロと何ら関わりがないことが事後に判明する」こともあるとするならば、国際テロの防止を理由として、このような対象範囲を限定しない長期間にわたる包括的・網羅的な情報収集をすべて肯定できるのかはより慎重に検討すべきであろう。

次に③について、収集したデータを「集約・結合」することは「収集」とは別に検討すべき問題である。テロリストの行動に共通点があるとすれば、人の行動を網羅的・継続的に監視し分析すること（プロファイリング）によって、テロリストを特定できるかもしれない（データ・マイニングによる行動予測）。ただ、そのような情報処理が常に正確だという保証もない。犯罪捜査の領域においてデータ・マイニングが有用だとしても、それが効果的だといえるのは「偽陽性」（本当はテロリストではないが、テロリストのプロファイルに適合すること）が少ない場合である。通常、企業が市民の消費行動を予測するような場合には高度の正確さは不可欠ではないとしても、犯罪捜査において警察が間違ふことのコストは大きい。かりに本件のような包括的・網羅的な情報の収集・分析＝監視がテロ対策として必要だったとしても、どのような場合に、どの程度までなら許されるか、憲法上許容される範囲（手段の相当性）を厳密に画定すべきであろう。

2. 監視と精神的自由

監視は、「人の行為をみたり、きいたり、記録する行為」として、調査権力の最も包括的な形態であり、通常の搜索・調査の範囲を超える権力行使だといえる。対象が限定された搜索・調査と異なり、監視は包括的で網羅的な搜索であって、本来の範囲を超えて大量の情報を全方位で収集できることが特徴である。したがって、監視は人の日常生活の振る舞いや人間関係から言論活動まですべて記録できるという点で、監視者は強力な権力をえていることになる。

監視にはいくつかの状況が考えられる。①人が監視されていることを自覚している場合には、収集情報がどう処理されるのかわからないので、人を不安にさせることはもとより、人の行動を変えさせる原因になるという意味で、監視は自己抑制を促す。とりわけ言論や人間関係を形成する自由に対して萎縮効果を及ぼし、行動の選択と意思決定の自由(自己決定権)に影響するおそれがある。たとえば、テロリストのプロファイリングには、その人の言論・宗教に関わる活動や人間関係の情報が含まれることがあるが、このような情報を収集することは、言論の自由や信教の自由への不当な干渉になりうる。社会的多数者から支持されない書籍の購読や少数者の宗教活動を躊躇・抑制させるためには情報をリークする必要はない。人の書籍購入履歴、発言内容、交友関係などを警察が調査して、人の行動を予測するためにデータを分析できるという可能性があるだけで人は萎縮させられるのである。

②人が監視されていることを漠然と自覚しているが、監視の実態は隠されている場合(いつ・どこで・どのように監視されているのかわからないような場合)には、萎縮効果はより効果的に及ぶと考えられる(パノプティコン効果)⁽⁸⁾。

あるいは③監視が完全に隠されている場合には、対象者は監視されていることを自覚できない状態にあるので不安感や萎縮効果を生じないが、人

の日常生活上の振る舞い、行動履歴、人間関係、多種多様な言動などを記録できるという意味では完全な監視が可能になる。この場合には、監視者は本来の目的を超えて情報を詳細に収集できるので、人は違法行為や不道徳な行いを記録されるかもしれない。政府はそうした情報を利用して人を攻撃・脅迫するかもしれないし、過失から、あるいは報復手段として意図的に情報をリークするかもしれない。これら監視のリスクは、監視されていることだけでなく、監視者の権力を制御できないことに由来している。このように、物理的・強制的な方法がとられたかどうかだけでなく、過度に広汎な情報収集活動が個人の自由に及ぼす萎縮・抑制効果を憲法上は警戒する必要があるだろう。

本件では裁判所は信教の自由（憲法20条）に対する侵害の可能性を検討しながら、宗教活動への萎縮効果を否定した。警察が「モスク」という宗教施設に着目して、「金曜礼拝」や「ラマダーン」という重要な宗教的儀式を重点的に監視していたことも確認したが、そのことによって原告らの宗教活動が萎縮させられたという事実はないと判断したのである。テロリストを早期に発見し、国際テロを防止するためには、場合によってはイスラム・コミュニティに立ち入って内部の宗教活動を把握する必要があることを説示する一方で、本件情報収集活動は「あくまで任意の情報収集活動」であって、捜査員が「外部から認識することができる外形的行為を記録したにとどまる」こと、したがってその効果は「原告らが嫌悪感を抱き得るにとどまる」だけだと断じた。その上で、「モスク把握」を含む情報収集活動が宗教活動に影響を及ぼすとしても、それは「国際テロの防止のために必要やむを得ない措置」だったと結論づけたのである。

しかし、範囲が広汎で、かつ長期間にわたるという意味で過剰ともいうべき制約＝監視によって、萎縮効果が生じたかどうかは慎重に判定しなければならない。そもそも萎縮効果論とは、とりわけ表現規制立法に対して求められる議論である。つまり、表現活動に対して過度に広汎な規制や漠

然として不明確な条文による規制を行うと(そのような立法があるだけで)、本来許されているはずの表現活動が自己抑制され、結果として民主的政治過程が窒息させられてしまう。したがって、こうした危険性を除去するためには表現規制立法は明確で必要最小限でなければならない⁽⁹⁾。表現規制では萎縮効果がどの程度発生するのかは規制の態様・強度や表現の種類によっても異なる。同じように、宗教活動に対して監視による萎縮＝自己抑制の作用が発生するかどうかについては、個別具体的な状況(場所・時間帯・期間・手段・態様など)を考慮しながら、過度に広汎な情報収集が行われなかったかどうかを丁寧に検証することがまず必要だろう。原告らの信教の自由への影響を「嫌悪感」にとどまるなどと過小評価すべきではない。また、かりに萎縮効果が生じなかったとしても、信教の自由の歴史的的重要性を真剣に捉えるならば、宗教的少数者の心理的負担を軽減する配慮も裁判所には求められていたと思われる。

3. 監視と情報プライバシー

①情報の収集

原告は、「自身の信仰内容・信仰活動に関する情報」を含めて「個人に関する情報を行政機関にみだりに収集・管理されない自由」を「情報コントロール権」(情報プライバシー)として主張した。まず信仰に関する情報は「個人の内面ひいては人格的自律に直接関わる事柄」として「社会生活の中で本人の承諾なくして開示されることが通常予定されていない情報」であること、そして「国籍・本籍地・犯罪歴」は本来保護されるべき個人情報であることを裁判所も認めた。ただ、その反面で、これらプライバシーに関わる個人情報が収集されたとしても、本件では「やむを得ない制約」だと結論づけた。なぜやむを得ないといえるのかについては、①本件情報収集活動の目的は国際テロの防止であること、そのための②情報収集の手段は違法または不当な方法ではないことを繰り返して説明している

だけである。

①の目的に関しては、特に「テロ事件に関する情報を事前に入手し、又は民衆に紛れたテロリストを発見して、国際テロの発生を未然に防止すること」は容易ではないことが判決では繰り返し指摘されている。容易ではないからこそ、「モスクに出入りする各人について、その信仰活動を含む様々な社会的活動の状況を広汎かつ詳細に収集して分析すること」が必要だと裁判所はいう。②の手段については、「原告らに対して信仰の証明を要求したり」、「不利益な取扱いを強いたり、宗教的に何らかの強制・禁止・制限を加えたりするもの」ではないことが同じように強調されている。

確かに「国際テロの防止」という目的そのものは正当だといえようが、しかし裁判所の推論では、プライバシーを過小評価しすぎているように思われる。裁判所も認めたように、本件で収集された情報はきわめて重要な個人情報である。信仰の程度など個人の内面に強く関わる情報であり、あるいは国籍・本籍地・犯罪歴など社会的差別の原因となりうる情報が含まれている。もちろん個人情報は多種多様なので、その種類によってコントロールできる程度も異なると考えられるが、こうした個人情報については完全に私的で、原則的には非開示であるべきことにまず異論はないだろう⁽¹⁰⁾。したがって、本件の制約についてはより厳格な審査が原則的には求められていたと解される。本件情報収集の態様・範囲が「国際テロの防止」のために必要最小限度のものといえるのか、より制限的でない別の手段はなかったのかを検討すべきであろう⁽¹¹⁾。特定のテロに関する具体的な情報を警察が入手していた場合は別として、そうでないならば宗教施設を継続して包括的に監視するという手法がなぜ必要だったのかを少なくとも説明しなければならない。この点で、裁判所は他国のテロ事件を参照することによって、まず宗教施設を媒介としてイスラム過激派からの勧誘が行われている可能性を指摘した。その上で、「一般人としての日常生活を装っているテロリスト」を早期に発見するためには、イス

ラム・コミュニティの内実を把握する必要があること、また「平穏なイスラム教徒」からテロリストを識別するためには、「その者の宗教的儀式への参加の有無、教育活動への参加の有無、その者が宗教的なコミュニティの中でいかなる立場にあるか」などの情報が必要であること、そのためにはモスクの「内部に立ち入って、その活動実態をある程度継続的に把握する」ことが不可欠だと説示する。しかし、宗教施設で過激派による勧誘がありうるという可能性を指摘するだけで、テロのリスクがまだ特定・具体化していない段階から「平穏なイスラム教徒」を含むコミュニティ全体を予防的に包括的に監視するという強硬な手法をはたして正当化できるのか。コミュニティにおける大多数の「平穏なイスラム教徒」に不利益を与えないように、宗教的少数者を威嚇しないような別の方法もあったのではないかという疑念が残る。ムスリム全体に対する偏見があることを疑われないためには、さらに説得力ある理由付けが求められるだろう。

②情報の保有

原告は「個人情報のデータベース化による保有自体が、個人に関する情報をみだりに第三者に開示又は公表されない自由の制約に当たる」ことを的確に主張していたが、裁判所は「適法な活動により得られた情報を警察が保有して分析等に利用することができることは当然」だと応答した。つまり、情報収集の目的は正当であり、方法も相当である以上、収集した情報を分析・共有することもまた当然に正当だという考え方である⁽¹²⁾。確かに情報の「収集」と「分析」は連続するプロセスだが、しかしプライバシー侵害の行為類型としては別の観点から論じられるべき側面があるだろう。裁判所が当然だという情報の「分析・共有」には、「集約」など情報の操作・利用に関する処理のあり方が含まれているからである(図表2)⁽¹³⁾。

まず、情報処理における「集約」とは「データ主体のあちらこちらに拡散した情報の断片を結合して、その人物像を編集すること」をいう。情報の集約では、もとの情報にプライバシーの価値があるかどうかというより

図表2 【プライバシー侵害の類型例】

侵害の基本類型	意味	侵害のサブカテゴリ
①情報収集	個人、企業、政府による情報収集行為	監視、調査
②情報処理	情報を加工、蓄積、捜査、調査、利用する行為	集約、特定、不安定化、二次利用、排除
③情報伝搬	情報を他者に伝達し、公開する行為	機密性の侵害、開示、暴露、アクセスの拡大、脅迫、盗用、歪曲
④領域の侵犯	個人の領域を直接的に侵害する行為	空間への侵入、意思決定への介入

See Daniel J. Solove, *Understanding Privacy* (Harvard University Press, 2008), pp103-105.

も、新しい情報を創り出すことによってデータ主体自身が予期していなかった方法で情報を補充することが問題となる（データ結合）。通常、人は日常生活のなかで自己のデータを断片的に開示しているので、これら断片的な情報を結合することによって、個人情報をも全面的に開示していなくても、データ主体に関する新しい「事実」を分析できる。この集約・結合という情報処理の方法は新しいわけではないが、コンピュータ技術に基づくデータベースが可能になった現代では特別な意味をもつ。大容量のデータ集約とそのアクセスや移転が容易になったからである。このようなデータ処理による監視の一類型がデータ・マイニングといわれる手法である。データ・マイニングは個人や集団に関する情報を集約・結合する私的・公的なデータベースを構成する手法や技術を意味している。このプロセスには、膨大な情報（たとえば、銀行、クレジットカード、通信、不動産、納税、旅行などの記録）の分析が含まれる。政府や企業は、多種多様な記録から行動パターンを解析することで犯罪捜査などに利用するのである⁽¹⁴⁾。

さらに「集約・結合」から生成された情報をリークや不当なアクセスから保護することを不注意で怠るような場合には、データ主体のプライバシーを「不安定化」させるおそれがある。また、収集された情報をデータ主体の同意なく本来の収集目的とは別の目的に利用する場合には「二次利

用」となる。データ主体が自分について他人が持っているデータの内容を知ること、またその処理・使用に加わることを認めないことは「排除」を意味する。これらプライバシーの侵害類型では、情報はすでに収集されているので、「収集」や「開示」は直接的な原因ではない。情報を管理・利用する方法に関わって侵害のリスクが生じることに注意すべきである。

4. 透明性の欠如とデータベース化

本来は着目すべきであったにもかかわらず、裁判所がほとんど考慮しなかったのは透明性の問題であろう。「透明性 (transparency)」=「公開性 (openness)」は政府の「説明応答責任 (accountability)」を高めて、権限濫用を防止するという意味で、民主政治の維持には必要不可欠なコンセプトである⁽¹⁵⁾。公安警察の本件活動はこの透明性=説明応答責任を欠いている点で問題である⁽¹⁶⁾。

これら(本件情報収集活動の具体的な内容)が外部に明らかになれば、情報収集活動自体の遂行が困難になる上、国際テロ対策に支障をきたし…犯罪の予防、公共の安全と秩序の維持を達成することが著しく困難になること等から、これらを個別的に明らかにすることはできない。…本件データには個人又は団体に関する情報、外国との協力関係に関する情報、警察による情報収集活動等に関する情報が含まれており…(これらを)個別的に明らかにすると、当該個人若しくは団体の権利利益が害され、又は当該外国との信頼関係が損なわれるおそれがあるほか、公共の安全と秩序の維持及び警察による情報収集活動等の適正な遂行に支障を及ぼすおそれがあるため、これらを個別的に明らかにすることはできない。(被告の主張)

確かにテロ対策に関わる警察情報をテロリストに知られないためには、情報収集活動の実態をすべて明らかにすることもできない。しかし、他方で

は公共的な説明応答責任を政府に求めて民主政治を維持すること（行政への民主的統制）もまた憲法上の重要な要請であることに留意しなければならない。透明性＝説明応答責任がなければ、司法審査を受けないまま、政府が市民の情報を自由に収集し、データベースを管理できることになる。「国際テロの防止」や「公共の安全や秩序の維持」のような安全保障上の公益と憲法上の権利との比較衡量は実質的にはほとんど不可能になるだろう。

このような情報の管理体制そのものが一義的には自己情報コントロール権の侵害になりうるが、さらに複雑な害悪を引き起こす。透明性の問題は、プライバシーを侵害することで言論活動を萎縮させ、宗教活動を威嚇することだけではない。情報の流出・漏洩、少数者への偏見、人種・宗教に基づく差別による不当逮捕、不都合な情報の隠蔽、政府批判への報復、脅迫、妨害、目的の範囲を逸脱した二次利用などの潜在的なリスクも考慮すべきである。つまり、行政組織の間で市民の個人情報が出回っているにもかかわらず、それらがどのように利用され、どのように評価・判断されているのかを本人は知らされることはない。ある人が「疑わしい人物」として警察から特定された場合には、そのプロファイリングの再審査を求めて、自分の意見を述べ、あるいは誤りを訂正する機会を権利として要求できるはずだが（憲法31条）、情報処理のプロセスが秘密であれば、告知・聴聞や弁明の機会は保障されない。データ・マイニングの詳細を知らされないうまま、ある日突然、人はその結果に基づいて、法律上もしくは事実上の不利益を課せられるかもしれない⁽¹⁷⁾。このような意味で民主社会の原理に反する方法で市民と政府との権力関係を変えてしまうことがリスクの本質だと考えられる。しかも、それは支配・抑圧を意図した悪意というより、むしろ行政機関による短絡的な決定や杜撰な管理によって生じうる。全体主義的権力ではなく、政府の意図や目的とは何ら関係なく、実際には悪意や偏見がない場合にも生じる侵害類型であることに注意すべきである⁽¹⁸⁾。

透明性の欠如については、原告は適正手続(憲法31条)の観点から問題を提起した。本件情報収集活動が信教の自由や情報プライバシーに対する重大な制約だとすれば、そのような警察の活動には法律上の根拠が必要となる(「法律の留保」)⁽¹⁹⁾。ところが、本件情報収集活動には、目的と基準を規定した作用法的な授權はない。この点について、裁判所は組織法である警察法2条1項を参照するだけである⁽²⁰⁾。

警察法2条1項が「犯罪の予防」、「その他公共の安全と秩序の維持」を警察の責務として定めていることに照らすと、これらに必要な警察の諸活動は、強制力を伴わない任意手段による限り、一般的に許容されるべきであるところ、本件情報収集活動が上記責務に照らして必要な活動であることは既に説示したとおりである。

公安警察による活動を警察法2条1項で根拠づけられるのかは見解が分かれるところだが、これを肯定するとしても、警察の裁量をできるだけ収縮させるような解釈は必要であろう。「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」があったかどうか、事実関係に基づいて慎重に判断すべきだったと思われる。情報収集活動の実態を説明しながら、手段としての相当性と必要性を厳格に審査すべきだったが、裁判所は公安警察の秘密主義を追認した結果として、政府の説明応答責任を問う可能性を閉ざした点で問題であろう。

むすびにかえて

本件判決では、二つの過小評価の誤りがあったように思われる。一つは監視による侵害の重大性である。確かに警察による情報収集や監視活動がすべて否定されるわけではない。特定の犯罪の発生に関わって個別の情報を警察が入手しているような場合には許されるだろう。しかし、具体的な犯罪がい

まだ特定されていない、抽象的なリスクがあるにとどまる段階から、将来の犯罪を予測するために包括的な情報収集活動を長期間継続することは原則として憲法上は許されないとと思われる。とりわけ精神的自由の保障に関わる事案について、たとえば、政治的言論や宗教に関わる活動、知識や思想に関わる活動の監視に対しては厳格に審査すべきである。情報収集の範囲が重大な公益を達成するために限定されていないような場合には、「過度に広汎」な規制として違憲となりうると解されよう。やむにやまれぬ場合を除いて、こうした個人情報の使用を原則として制限すべきであろう。しかし、本件では裁判所は情報流出事件の責任を除いてほぼ被告の主張を認めた。結果的には、本件監視活動のように、将来起こるかもしれない犯罪予測が間違っていた場合の司法判断の難しさを示したようにも思われる。

もう一つは政府の説明応答責任＝透明性の確保を過小評価したようにみえる点である。民主国家は、市民が政府に対して説明応答責任を問うことを可能にしなければならない。情報へのアクセスを等しく保障することで権力の濫用を抑止する。同じように、専制政治の契機を縮小させるためには、個人の私生活に対する政府の干渉は厳格に審査されなければならない。このように政府を方向づけるという意味で、情報プライバシーの保護（個人情報の収集・管理に対する制限）は監視者の権限を抑制するように解釈されなければならない。本件では、監視者の権限を制限すべきこと＝政府は説明応答責任を負うことを曖昧にすべきではなかったと思われる。

最後に、本稿では触れなかったが、情報管理体制のあり方について、たとえば、監視情報の漏洩・流出・誤用などに対して厳格に審査すること、将来の誤用のおそれを防止すること（一定期間経過後、データの消去すること）、情報の目的外使用＝ミッション・クリープを防止することなど⁽²¹⁾、個人情報保護法制に関わる政府の責務が十分に果たされているかどうかは今後も検証が必要であろうと思われる。

以上

注

- (1) See Viktor Mayer-Schonberger and Kenneth Cukier, *Big Data : A revolution that will transform how we live, work, and think* (John Murray, 2013); 邦訳(斉藤栄一郎)『ビッグデータの正体』(講談社、2013年); Peter P. Swire and Kenesa Ahmad (eds.), *Privacy and Surveillance with New Technologies* (The International Debate Education Association, 2012); Susan Landau, *Surveillance or Security? : The Risks Posed by New Wiretapping Technologies* (The MIT Press, 2010).
- (2) See Julia Lane, Victoria Stodden, Stefan Bender, Helen Nissenbaum (eds.), *Privacy, Big Data, and the Public Good : Frameworks for Engagement* (Cambridge University Press, 2014).
- (3) ジョージ・オーウェル(高橋和久訳)『一九八四(新訳版)』(早川書房、2009年)、フランツ・カフカ(丘沢静也訳)『訴訟』(光文社、2009年)、オルダス・ハクスリー(黒原敏行訳)『すばらしい新世界』(光文社、2013年)を参照。
- (4) See Kevin D. Haggerty and Minas Samatas (eds.), *Surveillance and Democracy* (Routledge・Cavendish, 2010); Daniel J. Solove, *The Digital Person ; Technology and Privacy in the Information Age* (New York University Press, 2004), ch.3; Dennis H. Wrong, *Power : Its Forms, Bases and Uses* (1979); Reg Whitaker, *The End of Privacy : How Total Surveillance Is Becoming A Reality* (The New Press, 1999), ch.7.
- (5) 事件の経緯について、青木理・梓澤和幸・川崎健一郎編著『国家と情報』(現代書館、2011年)も参照。
- (6) なお、原告らは地裁判決を不服として控訴している。
- (7) 通常、法的に問題となる「監視」とは、離れた場所から政府や企業が(私的空間に立ち入ることなく)情報を密かに収集する行為をいう。現代の監視はテクノロジーの発達によって多種多様だが、たとえば、次の三類型が指摘される。①コミュニケーションの監視=通信・情報伝達に対するリアルタイムの傍受、②物理的な監視=物理的な行為のリアルタイムの観察、③トランザクション監視=通信や行為に関わるデータ処理記録へのアクセスである。See Christopher Slobogin, *Privacy at Risk : The New Government Surveillance and the Fourth Amendment* (The University of Chicago Press, 2007); Susan Landau, *Surveillance or Security? : The Risks Posed by New Wiretapping Technologies* (The MIT Press, 2010).
- (8) Michel Foucault (translated by Alan Sheridan), *Discipline and Punish : The Birth of the Prison* (Vintage Books, 1977); 邦訳(田村俣)『監獄の誕生』(新潮社、1977年); Shoshana Zuboff, *In The Age of The Smart Machine : The Future of Work And Power* (Basic Books, 1986); Daniel J. Solove, *Understanding Privacy* (Harvard University Press, 2008); 邦訳(大谷卓史)『プライバシーの新理論』(みすず書房、2013年); Clive Norris, "CCTV, the panopticon, and the technological meditation of suspicion and social control," in David Lyon (ed.), *Surveillance as Social Sorting : Privacy, Risk and Digital Discrimination* (Routledge, 2003).
- (9) 毛利透『表現の自由』(岩波書店、2008年)。

- (10) どのような情報をプライバシーとして保護するのか、情報プライバシーの内実とは、その社会がどのような社会的価値を保護したいのかに関わっている。See Jon L. Mills, *Privacy: The Lost Right* (Oxford University Press, 2008); 川岸令和「プライバシー権とは何のための権利なのか」(『自由への問い③公共性』所収、岩波書店、2010年)。
- (11) 前科照会事件(最判昭和56・4・14民集35-3-620)、講演会参加者名簿提出事件(最判平成15・9・12民集57-8-973)。
- (12) 情報の管理体制について、国際テロの未然防止のためには警察が他の行政機関と情報を共有しても、目的外利用に当たらないことを被告らは主張した。裁判所もこの主張をほぼ全面的に認めている。
- (13) Daniel J. Solove, *Understanding Privacy*, ch.4.
- (14) 人の信用評価、犯罪のプロファイリング、行動の予測などに大規模データベースを活用する情報処理の手法を特に「データバイラン dataveillance」という。データベースによる監視の問題については、See David Lyon and Elia Zureik (eds.), *Computers, Surveillance, and Privacy* (University of Minnesota Press, 1996); Reg Whitaker, *The End of Privacy: How Total Surveillance Is Becoming A Reality* (The New Press, 1999); Roger Clark, “Information Technology and Dataveillance” (1987), retrieved from <http://www.rogerclarke.com/DV/CACM88.html>.
- (15) 松井茂記『情報公開法』(有斐閣、2003年)。
- (16) 公安警察の組織上の問題については、前掲『国家と情報』第1章のほか、鈴木邦男『公安警察の口口』(筑摩書房、2004年)を参照。
- (17) 本件監視活動において公安警察は、何らかの理由で疑わしいと判断した人物について、特に「積極的に事件化」＝「別件逮捕」することによって、さらに情報収集(搜索と押収)を行っていたことが指摘されている。前掲『国家と情報』69-79頁(岩井信執筆部分)参照。
- (18) See Solove, *The Digital Person*, ch.3.
- (19) 塩野宏『行政法 I (第五版)』(有斐閣、2009年) 71頁以下。
- (20) 警察法の規定は次の通りである。「第二条 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つてその責務とする。2 警察の活動は、厳格に前項の責務の範囲に限られるべきものであつて、その責務の遂行に当つては、不偏不党且つ公平中正を旨とし、いやくも日本国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があってはならない」。
- (21) 「ミッション・クリープ mission creep」とは本来の範囲を超えて職務が拡大することをいう。ある目的のために収集されたデータを別の目的のために利用すること、もしくはある目的のために導入された技術を別の目的に使用することをいう。監視の目的を事前に限定して、監視によって収集されたデータは当該目的にのみ用いるべきである。See Daniel J. Solove, *Nothing to Hide: The False Tradeoff Between Privacy and Security* (Yale University Press, 2011), ch. 18.