Title	装着型GPS捜査とプライバシー : 情報プライバシー侵害の段階的分析を通じて
Sub Title	The use of technology of Global Positioning System in criminal investigation and right to privacy
Author	尾崎, 愛美(Ozaki, Aimi)
Publisher	慶應義塾大学大学院法学研究科内『法学政治学論究』刊行会
Publication year	2016
Jtitle	法學政治學論究 : 法律・政治・社会 (Hogaku seijigaku ronkyu : Journal of law and political studies). Vol.111, (2016. 12) ,p.39- 69
JaLC DOI	
Abstract	
Notes	
Genre	Departmental Bulletin Paper
URL	https://koara.lib.keio.ac.jp/xoonips/modules/xoonips/detail.php?koara_id=AN10086101-20161215-0039

装着型ＧＰＳ捜査とプライバシー
――情報プライバシー侵害の段階的分析を通じて――

尾崎愛美

一　はじめに

近時、車両にＧＰＳを装着して位置情報を取得する捜査（このような捜査を「装着型ＧＰＳ捜査」ないし「装着型」と称する）の適法性について判断した裁判例が相次いで示されている。[1] 後述のように、下級審裁判例は、プライバシー侵害の大小を装着型の適法性判断基準としている点において共通するが、プライバシー侵害の内容については一致をみない。

一般に、プライバシーは、当初、「一人で放っておいてもらう権利（伝統的プライバシー権）」として捉えられてきたが、[2] 一九六〇年代頃からコンピュータが社会に導入され始められるようになると、「自己情報コントロール権（現代的プライバシー権）」がプライバシーという概念の中に新たに組み込まれた。[3] さらに近年では、ビッグデータの分析を通じたプロファイルの自動作成（いわゆる自動プロファイリング）によって生じるリスクもプライバシーリスクとして考慮すべきことが指摘されている。このようなプライバシーの多義性が、下級審裁判例の結論の差異を招いた一因となっているように思われる。したがって、プライバシー侵害を適法性判断基準として用いる場合、当該捜査が、プライバシーのどの側面を侵害するかを具体的に明らかにしなければならない。[4]

従前、別稿にて大阪地裁平成二七年一月二七日決定[5]と大阪地裁平成二七年六月五日決定[6]を素材として、装着型ＧＰＳ捜査の被侵害利益の具体化を試みた。すなわち、装着型ＧＰＳ捜査では、ＧＰＳ位置情報が一定量収集されるが、収集された情報に基づいて自動プロファイリングが行われた場合、自動プロファイリングのみに依拠して評価されたり、その評価に基づいて個人に関する決定がなされたりされ得る。これらのプロファイリングリスクが、装着型におけるプライバシー侵害となり得ることを示唆した。

本稿では、かかるプロファイリングリスクの回避を視野に入れた法的規律のあり方を具体的に模索することにしたい。そこでまず、最近のプライバシーを取り巻く状況について概観することとする（「二」）。そして、ＧＰＳ捜査において主として問題となる情報プライバシー侵害について、情報の収集段階、データマイニング段階、プロファイリング段階に分けて分析を行った上で（情報プライバシー侵害の段階的分析）、プロファイリングに関する国際的動向についても紹介する（「三」）。さらに、装着型ＧＰＳ捜査の現状と課題について検討し、わが国において装着型ＧＰＳ捜査に関する法的整備をすすめるにあたっての基本的視座の提示を試みたい（「四」）。

二　ビッグデータ時代におけるプライバシー侵害

㈠　プライバシーを取り巻く状況の変化

ＩＣＴ技術の進歩により、今日では、大量に生成される情報（いわゆるビッグデータ）を活用して、個人の動向の監視を行うことが可能となった。このようなビッグデータの利活用は、商業分野のみならず犯罪の捜査・防止や安全保障の分野でも活発に進められている。たとえば、九・一一以降、監視の強化が課題とされた米国では、米国防総省高等研究計画局（Defense Advanced Research Projects Agency, ＤＡＲＰＡ）により、全情報探知システム[7]（Total Information Awareness System, ＴＩＡ）や、ライフログ・プログラム[8]（Life Log）が計画された。これらの計画は、個人の生活に関わるあらゆる情報を収集、データベースに保存し、ネットワーク化し、個人の行動を明らかにしようとするものであったが、プライバシーに対する侵害が顕著であるとして開発が中止された。

このようなビッグデータ時代の監視がもたらす問題を、宮下教授は、以下の三つに整理する。「第１に、ビッグ

データによって大量のデータが常時自動処理され、二次利用されることによって、データに基づく差別や選択肢の減少が行われるおそれがある[9]」こと（データの二次利用）、「第2に、ビッグデータは個人が予期しないところでのデータ処理によって自らのデータへのアクセスや消去といったコントロールを弱体化させてしまう[10]」こと（ユーザー・コントロールの喪失）、「第3に……個人情報の収集、分析、利用、蓄積、提供のそれぞれのプロセスにおいて従来とは異なる形で個人に対して影響を及ぼす。たとえば……ビッグデータは大量の個人情報からこれまで以上に正確な個人像を浮き彫りにする[11]」ことである（プロファイリングによる差別と偏見）。

それでは、このようなビッグデータ時代におけるプライバシー侵害に対しては、どのような対応が求められるだろうか。一つの方向性としては、通説的見解である自己情報コントロール権説を時代に適したものへ再構成するというアプローチが挙げられる[12]。たとえば、ニッセンバウム教授は、どのような場面において自分自身に関する情報を開示することが適切かという「場面上の統一性」に基づき、情報をコントロールすべきと主張する[13]。従来の自己情報コントロール権説が、自己情報に関するアクセスの制限に重点を置くのに対し、ニッセンバウム教授は、「人々が非常に気を配るには、単に情報の流れが制限されていることだけでなく、その流れが適切であると保障されることである」として、情報の流れの適切さを重視する点に違いがある[14]。

(二)　従来の学説とプライバシーの社会的側面

この点、山本教授は、現在の日本の通説的見解である自己情報コントロール権説は、情報プライバシー論の主唱者の一人であるフリードの「情報プライヴァシー論的自己決定論」の影響を強く受けていると指摘する[15]。そして、このような「個人主義的なプライヴァシー観」では、ビッグデータ時代におけるプライバシー侵害という問題に対処できないと主張する。同教授は、その理由として、以下の四つの点を挙げる。第一に、「そもそも……フリード説は、

ウェスティンの情報プライヴァシー論と異なり……コンピュータによるデータ処理に強い関心を示すものではなかった[16]」こと。第二に、「高度情報化社会においては、情報の検索・凍結・解析などが技術的・費用的にきわめて容易となり、氏名・住所・生年月日など、それ自体は単純な個人情報が重要な意味をもつ。しかし……『通説』では他者との関係性構築によって直接的な影響を及ぼす情報のみが（プライバシー固有情報として）まずは保護され、上述のような単純情報は（プライバシー外延情報として）2次的に、あるいは手段的にしか保護されない[17]」こと。第三に、「『データベイランス（dataveilance）』においては『データは人の目に晒されることなく、人格を持たないコンピュータによって処理されるため』運用それ自体によっては……具体的な不利益を被ることもない……ため……このような……抽象的な侵害（generalized harm）を権利『侵害』と捉えることは困難となる[18]」こと。そして、第四に、「高度情報化社会の問題が、情報システムの脆弱な構造やアーキテクチャそれ自体によっても生じ得るとすれば、プライヴァシー訴訟における救済は、構造設計的・制度改革的な性格を帯びる必要がある[19]」こと、である。そこで、山本教授は、「プライヴァシーが本来有する社会的・客観的側面に光を当てる[20]」べきであると主張する。

㈢　新しい情報プライバシー権説

プライバシーの社会的・客観的側面について、実利主義的な分析（プラグマティック・アプローチ）を加えたのが、近年の米国の情報プライバシー学派を牽引するソローヴ教授である[21]。ソローヴ教授は、『プライバシー』という見出しのもとに収められる多方面にわたる事実からプライバシーの本質もしくは中核となる特徴を定義しよう」とする伝統的な方法（いわゆる還元説）は具体的な問題の解決にはほとんど貢献しないとして、ボトムアップの手法によってプライバシーを多元的に理解するプライバシー理論を提唱した。

これ以前にも、プライバシーを多元的に理解しようとする試みは行われてきた。プロッサー教授は、米国の不法行

為法に関する判例・裁判例を整理し、プライバシーを不法侵入、私的事実の公開、公衆の誤認、盗用の四類型に分類した[22]。しかし、ビッグデータ時代には、このような四類型におさまりきらない侵害が登場しており、時代にそぐわないことが指摘されている。また、ルーベンフェルド教授は、情報に関するプライバシー（例えば、第四修正の保障するプライバシーや不法行為法上のプライバシー）と権利主体自身の行為に固有なプライバシー（例えば、婚姻や妊娠中絶のような自己決定権的なプライバシー）とを区別して論じ[23]、情報や権利主体といった、事物の内在的特性に着目してプライバシーを分類している。しかし、ソローヴ教授は、事物の内在的特性に焦点を当てるべきではないと主張する。また、ソローヴ教授は、合衆国最高裁判例においてしばしばみられてきたような、情報の性質に焦点を当てたプライバシーの分類方法も否定する。ソローヴ教授は、その理由として、情報や事物の性質に焦点を当てた場合、それ自体ではプライバシーに属するものとは見なされない情報の断片を組み合わせることにより、大量の情報の中から私たちのパーソナリティや行動を描写できるだけのかなりの詳細な情報が浮かび上がってくる問題を説明することができないからであるとしている。

ソローヴ教授は、プライバシーは個々の問題によって引き起こされるのであるから、諸問題をボトムアップから検討することでプライバシー理解を発展させていくべきであるが、プライバシーの価値は一様ではなく、プライバシー保護が問題となる事象の本性がどのようなものかによって多様なものとなると指摘した。このようなプライバシーの多様性に鑑み、ソローヴ教授は、プライバシー侵害となる活動を四つに類型化した。すなわち、①情報収集、②情報処理、③情報拡散、④侵襲である。さらに、ソローヴ教授は、①情報収集の形態を（1）監視と（2）尋問に、②情報処理の形態を（1）集約、（2）同定、（3）非セキュリティ状態、（4）二次利用、（5）排除に、③情報拡散の形態を（1）守秘義務関係破壊、（2）情報開示、（3）暴露、（4）アクセス可能性の増大、（5）脅迫、（6）盗用、（7）歪曲に、④侵襲の形態を（1）侵入と（2）意思決定の介入に分類している。ソローヴ教授のプラグマティッ

ク・アプローチは、情報の流れを観察し、その過程ごとのプライバシー侵害を具体化しようとするものであるといえる。その意味で、ソローヴ教授の見解は、情報プライバシー権の再構築化と捉えることができる（新たな情報プライバシー権説）。

本論のテーマであるＧＰＳ捜査は、ソローヴ教授が指摘した「集約」という問題を内包している。「集約」とは、「あちこちに散らばった情報の断片一つずつからはたいしたことがわからないものの、結びつけると、データのかけらがある個人の肖像を描きだ」[24]し、「予期せぬ仕方でデータを組み合わせ、従来だったらたやすく知ることができなかった個人についての事実を明らかにする可能性がある」[25]ものである。同様に、単一のＧＰＳ位置情報は、人の滞在日時・場所を示すにすぎないが、この位置情報の滞在時間や滞在回数を集計することによって、利用頻度の高い位置情報が判明する。利用頻度の高い位置情報から人の住所や仕事先などの生活拠点が推定できる[26]。このような行動履歴から私的な性格をもった行き先も明らかとなり、交友関係・思想・信条・嗜好といった個人像を浮き彫りにすることができる。のみならず、将来、人がどのような場所に向かうのかという行動予測を立てることも可能となる。そこで、次章では、このような情報の「集約」がもたらす問題について、具体的に検討を加えていくことにしたい。

三　情報プライバシー侵害の段階的分析

情報の収集段階で個人に関する大量の情報が収集されるとすれば、全情報探知システムやライフログ・プログラムに対してなされたような批判が加えられよう。二〇一四年に提出されたＮＳＡ報告書も、「現在の政府による大量のメタデータの保管は、市民の信頼、個人のプライバシー、そして市民的自由への危機をもたらす」[27]として、大量のデータセット（データのまとまり）は、使用目的に関係なく、それ自体がプライバシー侵害にあたりうることを示唆

している。しかし、情報の断片が収集される段階ではプライバシー侵害を検知することは困難である。さらに、ビッグデータ時代の監視には、高度なデータマイニング技術が用いられているが、どのようなアルゴリズムによって情報の処理が行われているのか（少なくとも一般人には）不明確であり、それゆえ、情報集約の段階でどのような侵害が生じているのか、集約された情報が利用される段階でどのようなプライバシー侵害が生じるかを明確に把握することは困難である。したがって、情報収集・集約・利用の各過程で生じる侵害の内容について詳細に分析しなければならない。

(一)　情報の収集段階

情報集約の前段階である情報の収集段階では、さまざまな種類の情報が収集されるが、それらがどのような性質を有するものであるのかを明らかにする必要がある。そこで、まず、情報の種類について整理することにする[28]。

情報は、大きく分けて、個人の生活の履歴であるライフログと、モノにまつわるセンシングログ、その他データに分けられる（ビッグデータとは、これらのデータの集合体である）。ライフログはパーソナルデータとも言われる。一般に、パーソナルデータは、その生成プロセスから、提供データ、測定データ、推定データの三つに分類される[29]。提供データは、利用者自らが提供したデータである。具体的には、個人が自ら提供する氏名、住所、電話番号等が挙げられる。測定データは、センサーやカメラ等で個人の行動を観測することによって記録されるデータである。推定データとは、「ある個人に関する断片的な情報に関係ある他者の情報や何らかの統計情報を組み合わせ、その個人がどういう人かを推定するデータ」[30]をいう。推定データにはプロファイリングデータも含まれる。パーソナルデータは、「個人に関する情報」[31]の最も広い集合である。個人情報保護法は、パーソナルデータのうち、生存する個人に関する情報であって、当該情報に含まれる氏名、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もの（他の情報と

容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む[32]）を「個人情報」と定義する。個人情報を非特定化したものが識別・非特定情報であり、識別・非特定情報を非識別化したものが匿名情報となる。このように、個人情報はデータを加工処理することにより性質が変化する（状態推移[33]）。

総務省「パーソナルデータの利用・流通に関する研究会」は、プライバシーの保護というパーソナルデータの利活用の基本理念を踏まえて実質的に判断される個人識別性（実質的個人識別性）という概念を提唱し、実質的個人識別性をメルクマールとして、保護されるパーソナルデータの範囲を決定すべきとした[34]。実質的個人識別性とは、一見匿名に見えるが、実質的には特定の個人が識別される蓋然性が高いことをいう。実質的個人識別性を有する情報の具体例としては、Suica の乗降履歴が挙げられる[35]。Suica の乗降履歴は、「秒単位でどの駅に行ったという人のデータ[36]」であり「データの内容が詳細であるため、ほとんどのデータについて2つとして同じものがな[37]」い。このような履歴は、特定の人物の地理的な行動範囲を明らかにするものであって、その人物の将来の行動の予測をも可能としうるものであるゆえに、保護の対象となるのである。

さらに、継続的に収集される位置情報について、総務省「パーソナルデータの利用・流通に関する研究会」は、「仮に氏名等の他の実質的個人識別性の要件を満たす情報と連結しない形で取得・利用される場合であったとしても、特定の個人を識別することができるようになる蓋然性が高く、プライバシーの保護という基本理念を踏まえて判断すると、実質的個人識別性の要件を満たし、保護されるパーソナルデータの範囲に含まれる[38]」とされる。継続的に収集される位置情報は、単一で取得される位置情報よりも要保護性が高く、それ自体（すなわち、収集時点で）保護の対象となり得るのである。他方、収集がなされたとしても、それが蓄積されることなく、短期間で消去されるのであれば、要保護性は減少するのである。

そこで、プライバシーへの影響を図る上では、情報の種別だけではなく、それらがどのように取り扱われるかについても考えるべきである[39]。特に、今日の監視は技術への依存傾向があるため[40]、情報処理の技術的な過程を把握することが必要である。

まず、収集された情報には、情報の集合体として単に蓄積されるにとどまるものもあるが（散在情報）、何らかの基本属性をキーとしてデータベース化処理されるものもある（処理情報）。さらに、収集された情報の中には、データマイニングの過程を経て別種の情報へと変化するものもある。

データマイニングとは、膨大な量のデータから新たな知見を得るための、一つまたは複数の電子化されたデータベースへの問い合わせ・探索・分析処理を指す。データマイニングのプロセスは、①データウェアハウジングと呼ばれる、データマイニングの目標を設定し、必要なデータを選択するプロセス（データ獲得・選択）、②目標データからノイズ等を除去し、知識発見アルゴリズム[41]が適用できるように変換を施すプロセス（前処理とデータ変換）、③知識発見アルゴリズムを適用してパターンを発見するプロセス（パターン発見）、④抽出したパターンを解釈・評価して知識を得るプロセス（データ解釈と評価）に大別できる[42]。データマイニングは、知識が得られるまで①～④を繰り返す、連鎖プロセスとなっている。データマイニングは、人間が取り扱うよりも大量のデータを高速に処理できるが（大量高速データ処理）、人間の行う分析や推論と異なり、知識発見アルゴリズムが何故そのようなパターンを導いたのかという論理性が不明確なまま、大量のデータから特定のパターンが導かれることもある（論理性の欠如）。そして、人間の行う分析と同様に、知的発見アルゴリズムは完璧ではない（不正確性）。また逆に、データマイニングは、当初の目的よりも詳細かつ正確な知見を導くこともある（過度の正確性）。さらに、データの獲得・選択プロセスの段階で、

(二)　データマイニング段階――目標設定からパターン発見まで

マイノリティに対する先入観が意図せずに挿入される危険性があることも指摘されている[43]。したがって、データマイニングを利用するにあたっては、データマイニングの解釈の方法や、データマイニングの限界とその影響について理解が求められる。データマイニングについて理解した上で、データマイニングの結果を参照することができるようにすべきである。

㈢　プロファイリング段階

1　データ解釈と評価

データマイニングの手法の一つである機械学習アルゴリズムは、大量のデータからプロファイルを作成するプロセスを自動的に行うことを可能にするものであり、商業分野ではユーザの嗜好に応じたレコメンドサービスを提供するのに多用されているが、捜査の分野ではプロファイリングに応用されている。従来、犯罪捜査の場面において、プロファイリングとは、行動科学的な知見に基づいて、「犯行現場や被害者、その他の入手可能な情報を詳細に評価することにとって、犯罪者の特徴を見出し、犯罪捜査に活用可能な形で情報を提供しようとする[44]」捜査手法を意味する言葉として用いられてきた（いわゆる「犯罪者プロファイリング」）。これに対し、本論では、データマイニング技術を用いて抽出したパターンから、将来の犯罪が発生する場所・時間帯や、犯罪を犯す可能性のある犯罪者・犯罪集団を予測する手法をプロファイリングと称することにする（なお、犯罪者プロファイリングと区分する場合には、このような手法を「自動プロファイリング」と称する）。

2　具体例

(1)　犯罪の発生する場所・時間帯の予測

二〇〇五年から、テネシー州メンフィス市では、Blue CRUSH（Criminal Reduction Utilizing Statistical：統計履歴を用いた犯罪の低減）というプログラムが運用されている。これは、アルゴリズムとリアルタイムの犯罪データを用いて、常時アップデートできる犯罪マップを作成し、犯罪発生前に警察官を特定の場所に配置することを可能とするものである[45]。具体的には、犯罪のヒートマップ（指標の高い場所ほど赤く、低い場所ほど青く表示する）を使って、警官のカバー領域の変更に伴う現在の犯罪量や犯罪発生レベルの変化を観察するもので、同プログラムの使用により、メンフィス市では、重大犯罪が全体で三〇パーセント、凶悪犯罪が一五パーセント減少した[46]。カリフォルニア州サンタクルスでは、同様の手法により、強盗事件の二五パーセントについて、発生場所が正確に予測された[47]。さらに、バージニア大学の予測技術研究所（Predictive Technology Lab）は、イリノイ州シカゴの一平方キロメートルごとに区分した特定の地区の位置情報がついたツイートと、同市の犯罪データベースを分析することによって、犯罪が発生する可能性が高い地域についての有用な予測を行うことができたとの研究報告を発表した[48]。

また我が国でも、二〇一五年一〇月から京都府警で予測型犯罪防御システムが導入された[49]。これは、過去一〇年間の統計や犯罪理論を組み合わせて分析し、新たな事件が起きる可能性の高い地域、時間帯などをコンピュータで予測するシステムである。今後、人口減少社会の到来が予想される中、捜査機関においても人的資源不足が懸念される。このような、プロファイリングによって犯罪が起こりそうな場所や時間帯を予測し、犯罪発生前に警察官を特定の場所に配置する手法は、限られた人的資源を有効に用いる方法といえる（限られた資源の配分の最適化[50]）。

(2)　個々の犯罪者・犯罪集団を対象とした予測

ロサンゼルス警察本部とカリフォルニア大学ロサンゼルス校は、三〇以上の犯罪組織があるとみられる地区におけ

る約一〇年間の犯罪データから、犯罪組織同士の関係をモデル化し、八〇パーセントの確率で犯罪を犯す可能性の最も高い三つの組織を特定した[51]。また、シカゴでは、暴力犯罪の行為者と被行為者とを予測するアルゴリズムを用いて犯罪を犯す可能性が高いと予測された人間に対し、警告等を与えるプログラムが実施されている[52]。

我が国では、個別の犯罪者を特定することを目的としたシステムはいまだ実施されていないようであるが、二〇一四年に経済産業省経済産業政策局が作成した資料によれば、ビッグデータ利活用の将来的な目標として、事前に被害者・加害者を予知し、犯罪実行の予定者を未然に逮捕する犯罪予知システムの構築が示唆されている[53]。

それでは、このような個々の犯罪者を対象とした予測については、どのような侵害が想定されるだろうか。社会学の分野では、このようなプロファイリングが、特定の個人ないし集団を評価し、人々を分類する「社会的仕分け」を生じさせることが指摘されている[54]。そして、社会的に危険であるとカテゴライズされた場合、差別的に取り扱われる可能性がある[55]。このような差別的取扱いが、プロファイリング段階における侵害といえる[56]。なお、後述するＥＵ捜査等データ保護指令は、プロファイリングに基づく差別の禁止を権利として保障している。

この点、プロファイリングの運用にあたっては、まずは、特定の個人に対して何らかの評価や決定が下される場合に、対象者がこれに異議を申し立てる権利が認められて然るべきである（異議申立の機会）。さらに、このような権利行使の機会を保障するためには、プロファイリングの過程でどのような基準で社会的仕分けが行われたのかが明らかにされることが求められる（透明性の確保）。この点、ライアン教授は、「組織が責任をもって公平に個人データを扱うよう義務づけること。極めて重大な結果を招くデータベースのコード化の過程が透明化されるよう確保すること。そして、それによって最も攻撃されやすい立場の人々が、さらなる社会的排除と周辺化にさらされるリスクを減少させるだけでなく、ネットワーク化された技術の可能性をすべての人々に利益をもたらすように最大限化すること[57]」が求められるべきと主張する。また、プロファイリングは傾向と可能性を語るものにすぎないことから、プロファイリ

ングの偏重についても懸念されるべきである。たとえば、先述したような、事前に被害者・加害者を予知し、犯罪実行の予定者を未然に逮捕する犯罪予知システムは、プロファイリング結果を過度に信用するものにあたるといえる。このようなシステムの導入は、捜査の手法を、犯罪予防を目的とする未来志向型のものに変容させるおそれがある。プロファイリングは、あくまで意思決定の質を向上させるにとどまるべきであり、プロファイリングのみに基づいて意思決定を下すべきではない（運用条件の慎重性）。

3　プロファイリングに関する国際的動向

プロファイリングに基づく社会的排除という侵害は、ビッグデータ時代に顕在化した新たなプライバシーの侵害形態であるが、わが国では、このような侵害に対する法的整備の段階には至っていない[58]。米国では、スノーデン事件を受けて、二〇一四年五月、ビッグデータとプライバシーに関する五つの勧告が提出された。同勧告では、ビッグデータがもたらす新たな差別の類型の防止が、課題として挙げられたが、このような侵害に対する法的保障ないし権利の確立には至っていない。

(1)　EU一般データ保護規則

他方、欧州評議会では、二〇一〇年、プロファイリングに関する勧告が提出され、二〇一三年九月に開催された第三五回データ保護プライバシー・コミッショナー国際会議においてもプロファイリングに関する決議が採択された[59]。このような動向を踏まえ、二〇一六年に採択されたデータ保護規則[60]は、二二条の見出しを「プロファイリングを含む自動化された個人意思決定（Automated individual decision-making, including profiling）」とし、一項で「データ主体は、当該データ主体に関する法的効果をもたらすか又は当該データ主体に同様の重大な影響をもたらすプロファイリングなどの自動化された取扱いのみに基づいた決定に服しない権利を持つ」ことを明らかにした。また、二一条一項前段で、

「データ主体は、当該データ主体のそれぞれの状況に関する理由を根拠として、第六条（一）（ｅ）号又は（ｆ）号に基づくプロファイリングを含む当該条項を根拠とした自己に関する個人データの取扱いに対して、いつでも異議を唱える権利を有する」ことを定めた。そして、本規則のいうプロファイリングとは、「自然人に関するある一定の個人的な側面を評価するために、特に、自然人の業務実績、経済状況、健康、個人的嗜好、興味、信頼、行動、所在又は移動に関連する側面の分析又は予測をするためになされる、個人データの利用から成る個人データのあらゆる形態の自動的な処理をいう（四条（四）項）」ものであるとされた。

⑵　ＥＵ捜査等データ保護指令

先に挙げた規則は、ＥＵにおける一般的なデータ保護の枠組みであり、欧州委員会は、刑事犯罪の防止、捜査、探知、若しくは訴追又は刑事罰の執行の目的で処理される個人データの保護に関して、別途指令を作成した。それが、ＥＵ捜査等データ保護指令（正式名称「刑事犯罪の防止、捜査、探知もしくは訴追又は刑事罰の執行の目的のための管轄機関による個人データ処理に係る個人の保護及び当該データの自由な移動に関する欧州議会及び理事会の指令[61]」）である。本項では、刑事データ保護指令のうち、プロファイリングについて定めた一一条（「自動化された個人意思決定」）について述べる。

一一条一項本文は、「加盟国は、プロファイリングを含む、データ主体に対する不利な法的効果を生じ又は重大な影響を与える自動処理のみに基づく決定を禁止するよう定めなくてはならない」と定める。一一条二項は、「本条一項に関する決定は、一〇条に規定する特別カテゴリーの個人データのみに基づくものであってはならない」と定め、一一条三項は、「一〇条に規定する特別カテゴリーの個人データに基づく自然人に対する差別を引き起こすプロファイリングは、ＥＵ法に従って禁止する」としている。なお、一〇条一項は、加盟国が、人種、民族的、政治的思想、宗教、信念、労働組合員資格を明らかにするような個人データの処理、そして、遺伝データ、自然人を一意的に特定することを目的としたバイオメトリックデータ、健康に関するデータ、自然人の性生活に関するデータ、性的嗜好につ

いてのデータの処理を禁止しなければならない旨を定めている。規則が加盟国へ直接適用されるのに対し、指令は国内法化され、具体的な規制の手段と方法については加盟国の法律上の慣習が尊重され、加盟国に一任されるという性質を有する。そのため、規則二二条一項はデータ主体に向けられ、捜査等データ保護指令一一条一項は加盟国に向けられたものとなっている。このような差異はあるものの、捜査等データ保護指令一一条一項は、規則二二条一項とほぼ同一の内容を定めたものとなっている。また、プロファイリングの定義についても、規則と捜査等データ保護指令は同様の定義を有している（捜査等データ保護指令三条（四）項）。また当初、指令案では、差別を引き起こすプロファイリングを禁ずる条項はおかれていなかったが、データ保護指令二九条に基づいて設置される個人データの取扱いに係る個人の保護に関する助言機関（二九条作業部会）において、センシティブ情報（極秘データ）のみに基づいてプロファイリングおよび自動的判断してはならないとの保護条項を挿入すべきであるとの指摘を受け[62]、一一条三項が設けられている。なお、一一条三項にあたる条文は規則にはおかれていない。自動化異議を申し立てる権利および意見を表明する権利。

このように、EUでは、プロファイリングに基づく差別の禁止が法的権利として保障されるに至っており、参考とすることができると考えられる。

四　わが国における装着型GPS捜査

ここまで、GPS捜査が抱える情報の「集約」という問題について、情報プライバシー侵害というマクロ的な視点から考察してきた。それでは、わが国では、このような問題を内包するGPS捜査――特に装着型GPS捜査――について、どのような取り扱いがなされているのであろうか。

㈠　現行法上の対応――移動追跡装置運用要領

まず、装着型ＧＰＳ捜査については、警察庁の策定した移動追跡装置運用要領[63]（以下、「要領」という）が存在する。本項では、要領において規定された移動追跡装置（ＧＰＳを指す）の使用要件・手続等を概観することにする。要領は一条から五条までおかれ、まず、一条において、「この要領は、移動追跡装置を用いた任意捜査に関し、その使用要件、手続その他必要な事項を定めることにより、その適正を確保することを目的としたものである」とし、装着型を任意捜査と定めている。二条は移動追跡装置の定義について定めたものであるが、詳細は明らかにされていない。三条は「任意捜査を行うにあたり、移動追跡装置を用いるについては、次の各号に定める要件を満たさなければならないものとする」として、移動追跡装置の使用要件を定める。三条一号は、「次に掲げる犯罪の捜査を行うに当たり、犯罪の嫌疑、危険性の高さなどにかんがみ速やかに被疑者を検挙することが求められる場合であって、他の捜査によっては対象の追跡を行うことが困難であるなど捜査上特に必要があること」とし、同条二号は、「犯罪を構成するような行為を伴うことなく、この要領に掲げられている物のいずれかに取り付けること」としている。なお、どのような犯罪の捜査に移動追跡装置を用いることができるかについては明らかにされていない。このように、要領によれば、移動追跡装置を用いた任意捜査では、①犯罪の嫌疑、危険性の高さなどにかんがみ速やかに被疑者を検挙することが求められる場合（緊急性）、②他の捜査によっては対象の追跡を行うことが困難であるなど捜査上特に必要があること（必要性）、③犯罪を構成するような行為を伴わない取り付け（相当性）の三要件を使用要件としていると考えられる。ここでいう必要性は、犯罪捜査のための通信傍受に関する法律[64]三条一項の補充性（「他の方法によっては、犯人を特定し、又は犯行の状況若しくは内容を明らかにすることが著しく困難であるとき」）よりも緩やかなものであると解されるが、他に取り得る手段がないかどうかといった補充性についての検討は求められているものと考えられる。四条は使

用手続等についての定めである。四条一号は、「所属長は、任意捜査を行うに当たり移動追跡装置を用いる必要があるときは、あらかじめ、警察本部捜査主管課長（以下、「主管課長」という。）に申請してその承認を得なければならない」とする（「警察本部捜査主幹課長による事前承認」）。四条二号は運用状況の報告について定めたものであり、同号アによれば、「捜査主任官は、所属長に対し、毎日の移動追跡装置の運用状況を報告しなければなら」ず、同号イによれば、「所属長は、主管課長に対し、移動追跡装置の運用状況を一週間に一回以上報告しなければならない」。四条三号は、「捜査主任官、所属長及び主管課長は、捜査の状況を踏まえ、移動追跡装置の運用について必要な見直しを行い、使用の継続の必要性がなくなったときは直ちにその使用を終了する措置をとらなければならない」とする（「使用の必要性の検討」）。さらに、要領は、「移動追跡装置を使用した捜査の具体的な状況については文書管理を含め保秘を徹底」すると規定するが（五条）、保秘管理の具体的内容は明らかではない。

㈡　下級審裁判例の状況

捜査機関は、前記要領に従い、装着型ＧＰＳ捜査を任意捜査として実施してきた。しかし、昨今、装着型ＧＰＳ捜査の適法性が争われる事件が増加している。下級審の判断は、装着型ＧＰＳ捜査を強制捜査と捉える見解（強制処分説）と任意捜査と捉える見解（任意処分説）に大別される。例えば、わが国においてはじめて装着型ＧＰＳ捜査の適法性についての判断を下した大阪地裁平成二七年一月二七日決定は、装着型ＧＰＳ捜査を「通常の張り込みや尾行等の方法と比して特にプライバシー侵害の程度が大きいものではな」い適法な任意処分であると判示したが（任意処分説）、別途起訴されていた共犯者についての裁判において、大阪地裁平成二七年六月五日決定は、「目視のみによる捜査とは異質なものであって、尾行等の補助手段として任意捜査であると結論付けられるものではなく、かえって、内在的かつ必然的に、大きなプライバシー侵害を伴う捜査」であると判示した[65]（強制処分説）。また、名古屋地裁平成二

七年一二月二四日判決[66]は、「本件ＧＰＳ捜査は、対象車両の使用者のプライバシー等を大きく侵害するものであるから、強制処分にあたる」とし、その控訴審判決（名古屋高裁平成二八年六月二九日判決[67]。以下、「名古屋高裁判決」という）も、「本件ＧＰＳ捜査は、ＧＰＳ捜査が内包しているプライバシー侵害の危険性が相当程度現実化したものと評価せざるを得ないから、全体として強制処分に当たる」と判示した（強制処分説）。他方、広島高裁平成二八年七月二一日判決[68]（以下、「広島高裁判決」という）は、車体へのＧＰＳ装着につき、「磁石による発信器の装着は、通常、車体の損傷を来すものとはいえず、財産権の実質的な侵害を伴う可能性は一般的に小さく、この観点から本件ＧＰＳ捜査が強制処分であると解される余地はない」として、ＧＰＳ捜査の財産権侵害性を否定する[69]。そして、広島高裁判決は、「車両の使用者にとって、その位置情報は、基本的に、第三者に知られないですますことを合理的に期待できる性質のものではなく、一般的にプライバシーとしての要保護性は高くない」として、プライバシー権侵害性についても否定し、本件ＧＰＳ捜査は任意処分と解するのが妥当とした（任意処分説）。

㈢　装着型ＧＰＳ捜査の段階的分類の必要性

下級審裁判例は、主としてプライバシー侵害の大小を適法性判断基準としながらも、それへの評価は必ずしも一致をみない。この点、先述したように、情報収集・集約・利用の各過程における情報プライバシー侵害の態様およびその内容には差異がある。したがって、装着型ＧＰＳ捜査の適法性を判断するにあたっても、当該捜査が、どのような段階においてなされた、どのような内容の捜査であるのかを把握する必要がある。

1　尾行補助手段型のＧＰＳ捜査

まず、尾行中に被疑者を見失った際に、ＧＰＳ位置情報から被疑者の現在位置を探索する場合について検討する。尾行・追跡捜査が任意捜査として認められていることに鑑みれば、尾行の補助手段としてのＧＰＳ位置情報の活用も任意捜査として許容され得ると考えられる。しかし、既に述べた通り、継続的に収集される位置情報は、収集時点で保護の対象となる。そこで、このような尾行補助手段型が適法な任意捜査として許容され得るためには、継続的な位置情報の収集がないことが要件となると考える。要領四条三号には具体的な終期が定められておらず、名古屋高裁も指摘するように、この点が捜査の長期化の要因となっていると解される。したがって、要領には、具体的な終期に加え、情報の保存期間や削除に関する規定が盛り込まれることが望ましいと考える。なお、広島高裁判決は、ＧＰＳ捜査の基本的性格について「現場での尾行や張り込みによる行動観察、それに伴う採証活動等であり、発信器の利用は、捜査官が対象車両を探索する範囲を絞るための効率的手段にすぎない」として、本件ＧＰＳ捜査を尾行の補助手段としての捜査と位置づけたものと考えられる。

2　情報集約型のＧＰＳ捜査

つぎに、捜査中、ＧＰＳ位置情報を継続的に収集した場合、ないし、データマイニング技術を用いてＧＰＳ位置情報を分析した場合について考察する。これらの場合、被疑者の居住地や勤務先などの活動拠点、犯行現場への移動手段や経路といった地理的な活動範囲が明らかとなり得る。さらには、次の犯行地域を推定することも可能となるかもしれない（データマイニングを用いた「地理的プロファイリング」[70]）。この点、名古屋高裁判決は、「ＧＰＳ端末を利用した捜査は、対象者に気付かれない間に、容易かつ低コストで、その端末の相当正確となり得る位置情報を、長期間にわたり常時取得できるだけでなく、その結果を記録し、分析することにより、対象者の交友関係、信教、思想、信条、

趣味や嗜好などの個人情報を網羅的に明らかにすることが可能であり、その運用次第では、対象者のプライバシーを大きく侵害する危険性を内容する捜査手法である」として、かかる捜査手法を実現する可能性を有した本件ＧＰＳ捜査を強制処分としている。名古屋高裁は、ＧＰＳ捜査を通じた情報集約の実現可能性に着目して、前記の判断を下したものと思われる。(71)

3　捜査終了後の犯罪予測を目的とした保有位置情報の利用

それでは、捜査終了後、収集したＧＰＳ位置情報（保有位置情報）を犯罪予測に利用する場合についてはどうか。前述したように、このような予測は、犯罪の発生する場所・時間帯を予測するものと個々の犯罪者・犯罪集団を対象とするものに分類されるが、犯罪の発生する場所・時間帯を予測する方法については、警察官が該当地域を巡回するにとどまるのであれば、行政警察活動に区分されることになろう。他方、犯罪を犯す可能性のある特定人・集団を対象とした予測については、特定の人物・集団に対する差別的取扱いを助長することに繋がりかねない。このような利用に向けられた位置情報の継続的収集を検証と捉えると、不服申立手段や事後通知規定が欠如することになる。したがって、新たな立法による統制が必要となると考える。そして、このような差別的取扱いを回避する対策としては、プロファイリングリスクについて配慮したデータ保護制度の設計が進められているＥＵの政策を参考にすることができると考えられる。

五　おわりに

本稿では、ＧＰＳ捜査が抱える情報の「集約」という問題を考察するにあたり、情報収集・集約・利用の各過程で

生じる侵害の内容の分析を行った（情報プライバシー侵害の段階的分析）。また、このアプローチを装着型ＧＰＳ捜査の適法性判断にも応用し、装着型ＧＰＳ捜査を、尾行補助手段型のＧＰＳ捜査と情報集約型のＧＰＳ捜査に分類した。尾行補助手段型のＧＰＳ捜査は任意捜査として許容される。他方、情報集約型のＧＰＳ捜査については、強制処分となり得ると考えられるが、どの程度の詳細な位置情報が取得されれば情報集約にあたるのかについては、個別具体的な判断に拠るところが大きく、抽象的な基準を示すことは難しい。それゆえ、情報集約型の制度設計については、プライバシーへの影響を前もって評価することにより（プライバシー影響評価）、プライバシーリスクを最小限に抑えた捜査の実施が求められる。プライバシー影響評価（Privacy Impact Assessment, ＰＩＡ）とは、「個人情報の収集を伴う情報システムの導入又は改修にあたり、プライバシーへの影響を「事前」に評価し、問題回避又は緩和のための運用的・技術的な変更を促す一連のプロセス」[72]と定義される。ＰＩＡは、一九九〇年代からカナダで実施され、わが国でも、携帯電話のＧＰＳ位置情報の取扱いにつき、プライバシー影響評価の実施が検討されている[73]。そこで、今後は、携帯電話等に内蔵されたＧＰＳを利用した捜査（内蔵型ＧＰＳ捜査）との比較を行いつつ、情報集約型のＧＰＳ捜査のあり方について検討を加えていきたい[74]。

また、捜査終了後に、収集した位置情報（保有位置情報）を利用して犯罪の発生する場所・時間帯を予測する場合、警察官が該当地域を巡回するに留まるのであれば、行政警察活動の範疇にあるが、特定人・集団を対象とするものについては、差別的取扱いが助長される可能性がある。なお、この点に関し、ニューヨーク州では、市警と宗教団体との間で、「宗教のみを理由とした捜査を禁じる」との和解が成立している[75]。他方、我が国の最高裁は、テロを防止するために特定の宗教集団を監視する捜査手法を合憲とする決定を下している[76]。そこで、自動プロファイリングの結果、特定の個人・集団がある犯罪傾向を有していることが明らかになり、特定人・集団に対して捜査が開始されることが、そもそも、差別的な取扱いにあたり得るのか否かについては、今後の課題とし、諸外国との比較検討を行っていきたい。

（1） 下級審裁判例の状況について、中谷雄二郎「位置情報捜査に対する法的規律（特集 捜査における位置情報の取得）」刑事法ジャーナル四八号（二〇一六年）五一－五五頁、太田茂「ＧＰＳ捜査による位置情報の取得について（特集 捜査における位置情報の取得）」刑事法ジャーナル四八号（二〇一六年）六一－六六頁等。

（2） Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890). なお、邦訳として、サミュエル・Ｄ・ウォーレン／ルイス・Ｄ・ブランダイス（外間寛訳）「プライヴァシーの権利（一）」法律時報第三一巻第七号（一九五九年）。

（3） Alan Westin, *Privacy And Freedom*, (Atheneum, 1967), Charles Fried, *Privacy*, 77 YALE L.J. 475 (1967-1968). わが国におけるものとして、佐藤幸治『現代国家と人権』四八九－四九〇頁（有斐閣、二〇〇八年）。

（4） 宮下紘「判批」重判平成二七年度（ジュリ臨増一四九二号）一三頁（二〇一六年）。

（5） LEX/DB 文献番号 25506264。本決定の評釈として、前田雅英「判批」捜査研究六四巻四号五六頁（二〇一五年）、羽渕雅裕「判批」ＴＫＣ Ｗａｔｃｈ憲法№１００（二〇一五年）、宮下紘「判批」時の法令一九七三号五〇頁（二〇一五年）、黒川亨子「捜査方法としてのＧＰＳの利用の可否」法律時報八七巻一二号一一七頁（二〇一五年）、山本和昭「ＧＰＳを使用した証拠収集の適法性をめぐる二つの決定」専修ロージャーナル一一号四九頁（二〇一五年）、清水真「ＧＰＳと捜査」法学教室四二七号四一頁（二〇一六年）等。

（6） LEX/DB 文献番号 25540308。本決定の評釈として、緑大輔「判批」ＴＫＣ Ｗａｔｃｈ刑事訴訟法№１００、「判批」法学セミナー七二八号三頁（二〇一五年）、指宿信「ＧＰＳ利用捜査とその法的性質――承諾のない位置情報取得と監視型捜査をめぐって」法律時報八七巻一〇号五八頁（二〇一五年）、黒川・前掲注（5）一一七頁等、中島宏「判批」法学セミナー七二九号一三〇頁（二〇一五年）、土本武司「判批」捜査研究六四巻七号一二七頁（二〇一五年）、亀石倫子「判批」季刊刑事弁護八五号九六頁（二〇一六年）、清水・前掲注（5）四一頁、宮下・前掲注（4）一二頁、亀石倫子「捜査による位置情報の取得と弁護（特集 捜査における位置情報の取得）」刑事法ジャーナル四八号（二〇一六年）七七－八二頁。なお、本決定の後、大阪地裁平成二七年七月一〇日判決は、「本件ＧＰＳ捜査の違法を量刑上特に考慮すべきものとはいえない」と判示した（Westlaw Japan 文献番号 2015WLJPCA07106001）。

（7） John Markoff, *Pentagon Plans a Computer System That Would Peek at Personal Data of Americans*, N.Y. TIMES, NOV 9, 2002 at A12. 邦語による文献として、横山恭三「米国のサイバー・カウンターインテリジェンスについて――通信傍受の法

的及び技術的側面」防衛取得研究第四巻第四号（二〇一一年）一二頁。

（8）横山・前掲注（7）一二頁。なお、わが国では、個人のネット通販の購買履歴や健康情報などを一括管理する「情報銀行」の創設が検討されている（日本経済新聞朝刊「『情報銀行』創設へ指針　政府、通販データ管理などで」二〇一六年九月一一日）。

（9）宮下紘『プライバシー権の復権』（中央大学出版部、二〇一五年）二六八頁。

（10）宮下・前掲注（9）二六八－二六九頁。

（11）宮下・前掲注（9）二六九頁。

（12）その他、米国では、「①情報を『財産』として保護しようとする財産権的アプローチ、②表現の自由とのかかわりの中で保護しようとする修正一条からのアプローチ、③個別の情報ではなく、一定の領域全体にバリアをかけようとする空間論的アプローチ」等が存在する（山本龍彦「アメリカにおける対テロ戦略と情報プライバシー――自己情報コントロール権論の再構成に向けて」大沢秀介、小山剛編『自由と安全――各国の理論と実務』（尚学社、二〇〇九年）一五四頁参照）。

（13）Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, (Stanford University Press, 2010).

（14）大谷教授は、このようなニッセンバウム教授の見解を踏まえて、公共空間においては、匿名性が維持されていることが情報の流れが適切であると保障された状態であると捉え、被監視者の匿名性が保持された状態であればかかる監視は許容されうる可能性があることを指摘する（大谷卓史「公共空間におけるプライバシーとしての匿名性：倫理的に許容されうる監視システムはあるか？（ソーシャル・ネットワークと情報教育関係）」電子情報通信学会技術研究報告一〇九巻三三〇号（二〇〇九年）四九－五四頁）。

（15）山本龍彦「プライヴァシー――核心はあるのか」長谷部恭男編『人権の射程』（法律文化社、二〇一〇年）一四二頁。

（16）山本・前掲注（15）一四三頁。

（17）同右。

（18）同右。

（19）山本・前掲注（15）一四四頁。

（20）同右。

（21） Daniel J. Solove, Understanding Privacy, (Harvard University Press, 2008). 邦訳として、ダニエル・Ｊ・ソローヴ著、大谷卓史訳『プライバシーの新理論――概念と法の再考』（みすず書房、二〇一三年）。

（22） William L. Prosser, Privacy, 48 CAL. L. REV. 383 (1960).

（23） Jed Rubenfeld, *The Right to Privacy*, 102 HARV. L. REV. 737 (1989). 邦訳として、ジェド・ルーベンフェルド著、後藤光男、森下史郎、北原仁共訳「プライヴァシーの権利」（敬文堂、一九九七年）七頁。

（24） ソローヴ、大谷・前掲注（21）一六二頁。

（25） ソローヴ、大谷・前掲注（21）一六三頁。

（26） Apple サポート -Apple Support「プライバシーと位置情報サービスについて」https://support.apple.com/ja-jp/HT203033（二〇一六年八月一六日最終取得）。

（27） Richard A. Clarke, Michael J. Morell, Geoffrey R. Stone, Cass R. Sunstein & Peter Swire, *The NSA Report: Liberty and Security in a Changing World prinston*, pronston university press, 2014 p. xviii.

（28） 小向太郎「ビッグデータと捜査機関との情報共有」大沢秀介監修、山本龍彦、横大道聡、大林啓吾、新井誠編集『入門・安全と情報』（成文堂、二〇一五年）八五頁。

（29） 世界経済フォーラム「パーソナルデータ：新たな資産カテゴリーの出現」http://www.weforum.org/reports/personal-data-emergence-new-asset-class（二〇一六年八月一六日最終取得）。邦語によるものとして、城田真琴『パーソナルデータの衝撃――一生を丸裸にされる「情報経済」が始まった』（ダイヤモンド社、二〇一五年）二一頁。

（30） 坂内正夫『角川インターネット講座７　ビッグデータを開拓せよ　解析が生む新しい価値〈角川インターネット講座〉（角川学芸出版全集）』（ＫＡＤＯＫＡＷＡ、二〇一五年）二一九－二二〇頁。

（31） 個人情報の保護に関する法律（平成十五年五月三十日法律第五十七号　最終改正：平成二八年五月二七日法律第五一号）二条一項。

（32） なお、容易照合性の容易の判断には明確な定義がない。

（33） 小林慎太郎『パーソナルデータの教科書』（日経ＢＰ社、二〇一四年）三九頁。

（34） 総務省「パーソナルデータの利用・流通に関する研究会報告書～パーソナルデータの適正な利用・流通の促進に向けた方策」二頁。http://www.soumu.go.jp/main_content/000231357.pdf（二〇一六年八月一六日最終取得）。

（35）　ＪＲ東日本が日立製作所に鉄道利用客の乗降履歴データを販売した事案では、特定の個人を識別することを禁止する契約が締結され、SuicaID番号・利用者氏名・利用者電話番号・生年月日・性別といった情報は削除され、乗降駅名、利用日時・鉄道利用額のみが販売されていた。しかし、乗降履歴から個人の識別が可能であることが指摘され、販売は中止された（Suica に関するデータの社外への提供についての有識者会議「Suica に関するデータの社外への提供について中間とりまとめ」参照）。http://www.jreast.co.jp/chukantorimatome/20140320.pdf（二〇一六年八月一六日最終取得）。

（36）　鈴木正朝、高木浩光、山本一郎著『ニッポンの個人情報「個人を特定する情報が個人情報である」と信じているすべての方へ』（翔泳社、二〇一五年）七七頁。

（37）　同右。

（38）　総務省・前掲注（34）二五頁。

（39）　稲谷准教授は、「情報処理プロセスを規律する法のあり方を考察するにあたっては、情報処理プロセスの各段階における様々な規律手段の長所と短所を出来る限り把握し、それらをどのように組み合わせるのが最も優れているかを分析する必要がある」と指摘する（稲谷龍彦「警察における個人情報の取扱い」大沢秀介監修、山本龍彦、横大道聡、大林啓吾、新井誠編集『入門・安全と情報』（成文堂、二〇一五年）一〇頁）。

（40）　デイヴィッド・ライアン著、田島泰彦訳『監視スタディーズ――「見ること」「見られること」の社会理論』（岩波書店、二〇一一年）三二頁。

（41）　ディシジョン・ツリー（決定木）、ルール機能、ニューラル・ネットワーク、遺伝的アルゴリズム、機械学習アルゴリズム等の理論が利用される。

（42）　元田浩、山口高平、津本周作、沼尾正行著『データマイニングの基礎』（オーム社、二〇〇六年）八－九頁。なお、データマイニングには、本稿で挙げた仮説検証（目的志向）的データマイニングの他、目的変数を有しない知識発見（探索）的データマイニングもある。後者は主に商業分野に用いられる（例、マーケットバスケット分析）。

（43）　例えば、フィラデルフィアで導入されている再犯予測モデルには、犯罪者の郵便番号が組み込まれているが、郵便番号、すなわち、どの地域に居住しているかというデータは人種と関係が深い。また、テロリストを予測するモデルには宗教が考慮されている。このように、人種や宗教といった要素がデータマイニングの過程に入り込むことによって、データマイニングが特定の集団に対する差別をつくりだすとされる。

（44）渡辺昭一『犯罪者プロファイリング――犯罪を科学する警察の情報分析技術（角川ｏｎｅテーマ21）』（角川書店、二〇〇五年）。

（45）*Memphis Police Department: Keeping ahead of criminals by finding the "hot spots"* http://www-03.ibm.com/software/businesscasestudies/se/sv/corp?synkey=G863182I77772S93（二〇一六年八月一六日最終取得）。ネイサン・イーグル、ケイト・グリーン著、ドミニク・チェン監訳『みんなのビッグデータ：リアリティ・マイニングから見える世界』（エヌティティ出版、二〇一五年）一〇三頁。

（46）同右。

（47）同様のシステムは、リッチモンド、シカゴ、ニュージャージー州バインランドでも導入されている。

（48）http://www.businessinsider.com/twitter-crime-predict-2014-4（二〇一六年八月一六日最終取得）。

（49）宮川佐知子「犯罪予測システム京都府警、全国初の導入へ」毎日新聞二〇一六年二月一〇日（http://mainichi.jp/articles/20160210/k00/00e/040/210000c 二〇一六年五月一六日最終閲覧）。

（50）エリック・シーゲル著、矢羽野薫訳『ヤバい予測学――「何を買うか」から「いつ死ぬか」まであなたの行動はすべて読まれている』（ＣＣＣメディアハウス、二〇一三年）一一二頁。

（51）Carrie Kahn, *At LAPD, Predicting Crimes Before They Happen at lapd predicting crimes before they happen* http://www.npr.org/2011/11/26/142758000/at-lapd-predicting-crimes-before-they-happen（二〇一六年八月一六日最終取得）。

（52）山本龍彦「予測的ポリシングと憲法：警察によるビッグデータ利用とデータマイニング」慶應法学三二号（二〇一五年）三二五頁。

（53）日本の『稼ぐ力』創出研究会「第７回ビッグデータ・人工知能について事務局説明資料」経済産業省経済産業政策局二〇一四年一〇月二四日 http://www.meti.go.jp/committee/kenkyukai/sansei/kaseguchikara/pdf/007_03_03.pdf（二〇一六年八月一六日最終取得）。

（54）ディヴィッド・ライアン著、田島泰彦、清水知子訳『９・11以降の監視』（明石書店、二〇〇四年）一四三頁。また、ライアン教授は、「今日の監視によって表象されている主要なリスクは、プライバシーの侵害ではない……直接の注意を必要としているのは、等級化とプロファイリングの過程」であるとも指摘する（デイヴィッド・ライアン著、田島泰彦、小笠原みどり訳『監視スタディーズ――「見ること」「見られること」の社会理論』（岩波書店、二〇一一年）二九八頁。

（55）「現代の監視技術は、人々をさまざまな情報の束と扱い、それを分析し、特定のリスク要因をもつ者とそうでない者とに分類することによって、リスクを排除しようとする方向で人々を操作するために用いられている……監視とそれによって得られた情報の分析に基づいたさまざまなサービスは、言い換えれば、われわれが平等に扱われることなく、コンピュータの分類によって優遇されたり、逆に差別的に扱われたりすることになることを表している」とされる（土屋俊監修、大谷卓史編集『改訂新版 情報倫理入門』（アイ・ケイコーポレーション、二〇一四年）一一九頁）。また、山本教授は、プロファイリングの利用がいかなる法的問題を提起するかにつき、プライバシー権の侵害、内心の自由の侵害――意思の操作・誘導、選挙権の侵害、選挙の公正の揺らぎ、民主主義の弱体化、平等原則、個人の尊重原理との抵触を挙げている（山本龍彦「ビッグデータ社会とプロファイリング」論究ジュリスト一八号（二〇一六年）三八－四一頁）。

（56）山本教授は、「プロファイリングの結果は、『真実らしく受け取られる情報』であると解され、その限りにおいて、『データ媒介的覗き見』としてプライバシー侵害を構成するとの見解を示した上で、かかる見解は、「本人の同意なく要配慮個人情報を探索するプロファイリングは、自己情報を開示する相手を選択するという上記権利を侵害するとの見解を示す（山本龍彦「インターネット時代の個人情報保護――個人情報の「定義」とプロファイリングを中心に」阪本昌成先生古稀記念論文集『自由の法理』（成文堂、二〇一五年）五六二頁）。

（57）ライアン、田島、小笠原・前掲注（54）二九五頁。

（58）わが国においては、プロファイリングによる侵害を抑止するために必要な対応策等は、検討課題として整理されるにとどまっている（高度情報通信ネットワーク社会推進戦略本部「パーソナルデータの利活用に関する制度改正大綱」（二〇一四年）一六頁。http://www.kantei.go.jp/jp/singi/it2/info/h260625_siryou2.pdf（二〇一六年八月一六日最終取得）。

（59）35th International Conference of Data Protection and Privacy Commissioners, Resolution on Profiling, 25 September 2013. Available at https://privacyconference2013.org/web/pageFiles/kcfinder/files/2.%20Profiling%20resol ution%20EN%281%29.pdf（二〇一六年八月一六日最終取得）。

（60）REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). なお、EU一般データ保護規則の日本語訳については、一般財団法人日本情報経済社会推進協会作成の仮訳を使用した。https://www.jipdec.or.jp/archives/publications/J0005075

（二〇一六年一一月一六日最終取得）。

(61) Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. 邦語による文献として、宍戸常寿「安全・安心とプライバシー」論究ジュリスト一八号（二〇一六年）五七－五九頁。

(62) ARTICLE 29 DATA PROTECTION WORKING PARTY, *Opinion 03/2015 on the draft directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data*, December 2015, pp. 9–10. Available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp233_en.pdf（二〇一六年八月一六日最終取得）。

(63) 平成一八年六月三〇日警察庁丁刑発第一八四号。

(64) 平成十一年八月十八日法律第百三十七号（最終改正：平成二三年六月二四日法律第七四号）。なお、補充性につき、城祐一郎『盗犯捜査全書―理論と実務の詳解―』（立花書房、二〇一六年）五九一頁。

(65) その後、大阪高裁は、「一審証拠決定がその結論において言うように、このようなＧＰＳ捜査が、対象車両使用者のプライバシーを大きく侵害するものとして強制処分に当たり、無令状でこれを行った点において違法と解する余地がないわけではないとしても、少なくとも、本件ＧＰＳ捜査に重大な違法があるとは解され」ないとした（大阪高判平成二八年三月二日Westlaw Japan 文献番号 2016WLJPCA03026001）。本件の評釈として、前田雅英「判批」ＷＬＪ判例コラム七三号（2016WLJCC011）、中島宏「判批」法学セミナー七四一号（二〇一六年）一一六頁、宇藤崇「判批」法学教室四三一号（二〇一六年）一四五頁等。なお、本件は、二〇一六年一一月一六日現在、最高裁に上告中である。

(66) Westlaw Japan 文献番号 2015WLJPCA12246002。

(67) Westlaw Japan 文献番号 2016WLJPCA06296001。本件の評釈として、前田雅英「判批」ＷＬＪ判例コラム八六号（2016WLJCC024）。

(68) Westlaw Japan 文献番号 2016WLJPCA07216009。本件の評釈として、前田雅英「判批」ＷＬＪ判例コラム八九号

(2016WLJCC027)。

(69) 連邦最高裁としてはじめて装着型ＧＰＳ捜査の適法性判断を行った、二〇一二年の United States v. Jones 判決（以下、「Jones 判決」という）は、車両に対するＧＰＳの装着を有体物に対する物理的侵入とみて、四週間にわたる装着型ＧＰＳ捜査を合衆国憲法第四修正の捜索にあたると判示している（United States v. Jones, 132 S. Ct. 945, 565 U.S. ___ (2012).）。Jones 判決は侵入法理を採用して本件ＧＰＳ捜査の適法性判断を行ったものであるが、広島高裁判決は、このような判断枠組みには与しなかったものといえよう。

(70) 三本照美「地理的プロファイリング」渡邉和美、高村茂、桐生正幸（編著）『犯罪者プロファイリング入門――行動科学と情報分析からの多様なアプローチ』（北大路書房、二〇〇六年）七七－八二頁。

(71) また、名古屋高裁判決の判断枠組みは、米国のモザイク理論とも類似する。モザイク理論に関する邦語文献として、清水真「捜査手法としてのＧＰＳ端末の装着と監視・再論」明治大学法科大学院論集一三号（二〇一三年）一六三－一八一頁、三井誠＝池亀尚之「犯罪捜査におけるＧＰＳ技術の利用：最近の合衆国刑事裁判例の動向」刑事法ジャーナル四二号（二〇一四年）五五－六三頁、堀田周吾「サイバー空間における犯罪捜査とプライバシー」法学会雑誌五六巻一号（二〇一五年）五八九頁以下、柳川重規「捜査における位置情報の取得：アメリカ法を踏まえて（特集 捜査における位置情報の取得）」刑事法ジャーナル四八巻（二〇一六年）三三－三六頁等。

(72) 瀬戸洋一、六川浩明、新保史生、村上康二郎、伊瀬洋昭『プライバシー影響評価ＰＩＡと個人情報保護』（中央経済社、二〇一〇年）一頁。

(73) 総務省「『位置情報に関するプライバシーの適切な保護と社会的活用の両立に向けた調査研究』について」（平成二七年一二月一八日）http://www.soumu.go.jp/main_content/000396689.pdf（二〇一六年八月一六日最終取得）。

(74) 先行研究として、宍戸・前掲注（61）六一－六三頁。

(75) Raza v. City of New York, 998 F. Supp. 2d 70, Hina Shamsi, *Landmark Settlement in Challenge to NYPD Surveillance of New York Muslims: What You Need to Know*. https://www.aclu.org/blog/speak-freely/landmark-settlement-challenge-nypd-surveillance-new-york-muslims-what-you-need（二〇一六年八月一六日最終取得）。

(76) 朝日新聞デジタル「（ニュースＱ３）警察がイスラム教徒監視『やむを得ない』？」二〇一六年八月二日。http://www.asahi.com/articles/DA3S12491207.html（二〇一六年八月一六日最終取得）。

尾崎　愛美（おざき　あいみ）
所属・現職　慶應義塾大学大学院法学研究科後期博士課程
最終学歴　慶應義塾大学大学院法学研究科前期博士課程
所属学会　日本刑法学会
専攻領域　刑事訴訟法
主要著作　「位置情報の取得を通じた監視行為の刑事訴訟法上の適法性――United States v. Jones 判決を契機として」『法学政治学論究』第一〇四号（二〇一四年）