総務省 学術雑誌『情報通信政策研究』 第４巻第１号
Journal of Information and Communications Policy Vol.4 No.1

寄稿論文

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

小向　太郎[1]

要　旨

本稿では、捜査機関が犯罪捜査を行う際に、第三者に関する情報を保有する企業や団体に対して情報提供を求めることに関して、どのような問題があるかを検討する。情報技術の発達により、膨大な量の情報が収集・保存されるようになった。こうした情報は、犯罪捜査にも役に立つ場合が多い。一方で、第三者が保有する情報は、本人が認識していない状態で捜査当局に提供されることも多い。そのため、プライバシーや個人情報保護上の問題が懸念される場面が増えている。本論文は、米国、EU、日本における、第三者が保有する個人情報への捜査によるアクセスに関する関連法規を比較し、わが国の制度検討への示唆を得ようとするものである。

キーワード：犯罪捜査、強制処分法定主義、プライバシー、個人情報、第三者法理

１．第三者が保有する情報に対する捜査の論点

１．１．情報に対する捜査

本稿では、捜査機関が犯罪捜査を行う際に、第三者に関する情報を保有する企業や団体に対して情報提供を求めることについて、どのような問題があるかを検討する。

現在、人に関する様々なデータがコンピュータシステムで収集され、処理されている。IoT（Internet of Things）の発展によって様々なデータが収集されるようになり、そのような情報がビッグデータ技術やAIによって蓄積・処理され、次々と新しいデータが生み出される。爆発的に増加するデータ活用は、今後さらに拡大していくことが予想される[2]。

こうした情報は、犯罪捜査にとっても有効であることは疑いがなく、捜査機関による第三者からの情報収集は、どの国でも行われている。データの利用が増えたことで、法執行当局がアクセスできる情報も膨大になった。捜査当局は、犯罪が発生した際にさまざまな方法で手がかりを探し、新技術によって生成されたデータも含めて、犯罪に少しでも関係する可能性のある人物の情報を収集している。例えば、現在では犯罪捜査のために監視カメラやドライブレコーダで録画された映像を確認することは、ごく一般的に行われている。メールやSNSのメッセージ、ウェブサービスやウェブショップの利用履歴、位置情報、アクセスログなどの情報システムにも大量の痕跡が残されている。これらの情報を照合して、犯罪を犯す可能性のある人物のリストや行動履歴を作成し、容疑者を特定することができれば、犯罪捜査にとっては、非常に有用であろう。

現在、多くの企業が保有するコンピュータには、大量の個人に関する情報が蓄積されてい

[1] 中央大学国際情報学部教授

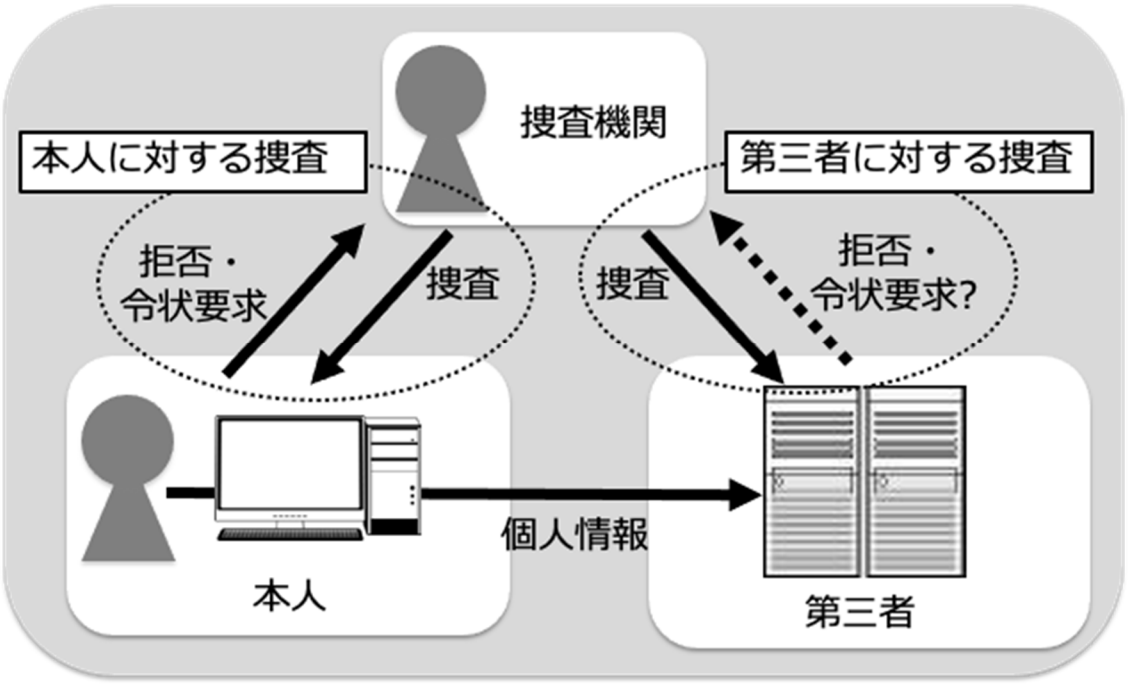
[2] Richard A. *Posner, Privacy, Surveillance, and Law*, 75 U. CHI L. REV. 245, 248 (2008).

る。これらの企業が捜査機関から協力を求められた場合に、その企業が、利用者のプライバシーを利用者本人と、全く同じレベルで尊重すると考えるのは無理がある。企業が、「権限を持った正規の捜査機関からの要請に協力するのは市民の義務である」と考えたとしても、少なくとも日本の一般的な感覚として、それほど違和感のあるものとはいえないであろう。

捜査当局が情報の本人に情報の提供を要請した場合、本人は自分にどのような影響があるかを考えて、その要請に応じるか拒否するかを決めることができる。しかし、さまざまな分野で膨大な情報が収集され、その内容も多岐にわたるようになると、新しい問題が懸念されるようになる。情報について利害を有するものと、情報を保有する者が必ずしも一致しないことが増えるからである[3]。

つまり、この問題の本質は、第三者が保有する個人情報に対して捜査が行われた場合に、本人が認識していない間にデータが入手され、本人が関与する機会も与えられないことがあり得るということである。

図１．第三者保有の情報に対する捜査の問題点



（出典）筆者作成

１．２．アプローチ

安全で秩序ある社会のためには、法執行機関による適切な捜査が必要であることは言うまでもない。一方で、法執行機関による人権侵害や権力の濫用を防止するためには、個人の人権を守る仕組みを持つことも重要である。第三者が保有する情報について捜査が行われる際に、本人の権利を保護するためには、過度な捜査を抑制したり、透明性を確保したりす

[3] 小向太郎「ビッグデータと捜査機関との情報共有」山本達彦・横大道総・大林啓吾・新井誠編『入門・安全と情報』成文堂（2015 年 6 月）85-105 頁。

る事が必要となる。これを実現するための具体的な制度的アプローチとしては、次のようなものが考えられる。

（1）捜査手続きに関する制度
（2）個人情報保護制度
（3）特別な情報に対する法的保護

第一に、法執行機関が犯罪捜査を行う場合には、法律が定める手続に基づいて行われなければならない。多くの国で、捜査機関が強制的な捜査を行うためには、令状等を取得し捜査対象者に提示することが求められている。ただし、捜査機関が強制捜査を行うのは、通常は、捜査対象者が任意協力を拒む場合である。捜査対象者が第三者である場合には、捜査機関や第三者によって、本人の権利への配慮がなされ得るかどうかが問題となる。

第二に、個人情報の重要性が急速に高まっていることから、ここ数十年の間に多くの国で個人情報保護制度が導入されている。個人情報保護制度では、利用目的を明確にする義務が規定されていることが多い。しかし、犯罪捜査のために法執行機関に情報を提供することは、「法的義務の履行」等を根拠として許されることが多い。個人情報保護制度では、法執行機関の職務執行のために個人情報の提供を認めるための、例外規定をおいていることが一般的である。そこで、捜査機関に対する個人情報の提供が、どのような場合に個人情報保護制度の適用除外になり、どのような義務が除外されるのかが問題となる。

第三に、特に厳格な保護が必要であると考えられている情報については、特別な法律によって保護がされている場合がある。例えば、電気通信事業者が取扱う情報については、通信の秘密の保護を求めている国が多い。特に、通信傍受については、厳格な手続きを定める法律が定められていることが一般的である。通信事業者が保有している利用者に関するデータとしては、この他にも、通信履歴、位置情報、契約情報、利用者の ID 情報等がある。通信以外の分野でも、医療情報、DNA データベース、金融機関の取引履歴、最近では購買履歴等について、特別な保護が法定されることがある。どのような情報について、どのような特別な保護がなされているかが問題となる。

なお、現在では、プラットフォーム事業者をはじめとするさまざまな事業者が、利用者の情報を大量に収集して利用しており、特別な規制を受けていない事業者であっても、膨大な数の個人データを保有している可能性がある。そのため、情報の種類を特定して、その情報に対する特別な保護を立法的に定めることは、次第に難しくなる傾向にある。

１．３．日本の関連制度と課題

上記の 3 つのアプローチについて、日本の制度の概要と課題を確認する。

（1） 捜査手続に関する制度

日本では、犯罪捜査における捜査対象者の権利の保護は、刑事訴訟法を中心とする犯罪捜査手続に関する制度によって図られており、その中核となるのが令状主義の考え方である（憲法 35 条）。この制度の趣旨は、国家権力による強制を伴う捜査に際して、捜査の目的・対象・方法等が適正であることを司法の監督によって担保し、捜査対象者に対して捜査の範

囲を明らかにして処分の適法性を争う機会を与えることで、刑事手続きによる権利侵害の適正な抑制を図ることだと考えられている。第三者が本人のプライバシー等に配慮して要請を拒否した場合は、捜査機関が当該情報を取得するために、令状などの正当な権限に基づく強制捜査を行う必要がある。この場合は、捜査が適切であるかどうかについて、司法によるチェックが行われる。ただし、この場合でも、情報の本人に捜査が行われていることは知らされないことが多い。

一方で、日本の犯罪捜査においては、人権の侵害や制約を伴う強制処分をできる限り回避すべきであるという考えから、任意捜査の原則が採用されている[4]。この原則を背景に、わが国の捜査機関にとって、調査当局への市民の自発的な協力は、むしろ望ましいものだと考えられてきた。捜査当局が企業や団体に、顧客やサービス利用者に関する情報の提供を求め、企業や団体が任意にそれに応じることは、少なくともわが国ではあまり問題とされてこなかった。そして、第三者が保有する情報に対する捜査では、情報に対して最大の利害を有する本人は、直接の捜査対象となる第三者ではない。一般に、情報を保有する第三者は、捜査機関から捜査を受けた場合に、これを拒否する動機を、本人と同程度には持っていない。また、本人に対するプライバシー侵害を追及されるという懸念も、このような場合にはあまり歯止めにならないと考えられる[5]。

最高裁判所は「強制の処分」とは，「有形力の行使を伴う手段を意味するものではなく，個人の意思を制圧し，身体，住居，財産等に制約を加えて強制的に捜査目的を実現する行為など，特別の根拠規定がなければ許容することが相当でない手段[6]」であるという考えを示している。本人の意思に反して個人情報を取得することは強制処分であるという考え方もありうるが、捜査当局が個人情報を保有する第三者に情報を求めることは、一般的には強制的な処分ではないと考えられている。刑事訴訟法 197 条２項は、「官公庁又は公私の機関は、調査に必要な事項について報告を求めることができる」と規定しており、検察や司法警察は、捜査関係事項照会書による照会を行うことができる[7]。この照会は任意協力の要請であり、

---

[4] 犯罪捜査規範第 99 条は「捜査は、なるべく任意捜査の方法によって行わなければならない」と定めている。また、刑事訴訟法 197 条第１項（「捜査については、その目的を達するため必要な取調をすることができる。但し、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」）も、強制の処分ができることを法律の定めがある場合に限定することで、捜査の原則は任意捜査であることを示すものと理解されている。

[5] コンビニエンスストアが防犯カメラの画像を警察官の求めに応じて提供した事例であるが、コンビニエンスストアとは関係のない犯罪に関する被疑者が撮影された画像を警察官に提供することについて、防犯というカメラ設置の目的を逸脱したものとはいえず違法なものではないとした判決がある（名古屋地判平成 16 年 7 月 16 日判タ 1195 号 191 頁）。

[6] 最三小決昭和 51 年 3 月 16 日刑集 30 巻 2 号 187 頁。

[7] 捜査関係事項照会に基づく個人データの第三者提供は、日本と EU の間の相互の個人データ移転枠組み構築に関する取り組みの過程でも議論になっている。日本と EU の間では、相互に個人情報保護が十分な国と認める方向で検討が行われ、2019 年 1 月 23 日には、欧州委員会が、日本に対する十分性を認める決定をしている。その過程で、欧州委員会からの要請に応じて、日本政府による情報のアクセスに係る法的枠組みについて説明が求められており、法務省が、欧州委員会のベラ・ヨウロパー委員（司法・消費者・男女平等担当）に、概要を説明する書簡を送付している。このなかで、「任意協力の要請を通じた個人情報の収集」として捜査関係事項照会をあげ、強制力がないものであることや、プライバシー権等に

照会を拒んでも罰則等がかせられることはない[8]。

捜査当局が企業に対して、顧客やサービス利用者に関する情報の提供を任意で求めることは広く行われており、顧客の住所氏名電話番号等の他、サービスの利用履歴、商品の購買履歴、ポイントの利用履歴、オンラインゲームから取得したGPS位置情報等が収集されている例もあるという指摘もある[9]。

（２） 個人情報保護制度

個人情報保護法23条1項は、個人情報取扱事業者が本人から事前の同意を得ずに個人データを第三者に提供することを原則として禁止している。ただし、捜査機関が捜査の目的で提供を求める場合には、「法令に基づく場合（1号)」として本人の同意がなくとも提供ができると考えられている。なお、捜査関係事項照会書に応じて情報提供することも、「法令上の根拠がある場合」に該当するとされており[10]、手続が適正に行われている限り個人情報保護法上の問題は生じない[11]。

（３）特別な種類の情報の保護

関する個人の意識の高まりを受けて「照会への回答が慎重になされる傾向が顕著となっている」こと、各種の制限が課せられることなどが、強調されている。個人情報保護委員会「日EU間・日英間のデータ越境移転について」、
https://www.ppc.go.jp/enforcement/cooperation/cooperation/sougoninshou/

8 捜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「捜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てた書簡では、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仮訳では、「刑事訴訟法の下では、照会先は捜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ためであろう。

9 共同通信社会部取材班「丸裸にされる私生活　企業の個人情報と検察・警察」世界921号(2019), 106-114頁. このレポートは、共同通信が入手した、検察庁と警察が照会可能な情報や企業毎の照会方法をまとめたとされるリストをもとに、企業等に対して行った取材をまとめたものであり、早急なルール作りが必要であると警鐘を鳴らしている。

10 宇賀克也『個人情報保護法の逐条解説』（有斐閣，第6版，2018年）166-167頁）

11 一般財団法人情報法制研究所は、2020年3月17日に「捜査関係事項照会対応ガイドライン（案)」を公表している。このガイドラインは、個人情報保護法第23条第1項の「法令に基づく場合」に該当するのは、「適法になされた捜査関係事項照会に対して、必要かつ相当な範囲で個人情報の提供等を行った場合」に限られるという考えのもとに、事業者が捜査関係事項照会を受けた場合に、捜査との関連性や相当性を確認のうえで判断すべきであり、そのための体制整備を行うべきである、という提言をしている。また、捜査関係事項照会に基づく個人データの第三者提供については、個人情報保護法上の記録作成義務の対象になっていないが、開示記録を作成・保管することが望ましいという考えも示されている。一般財団法人情報法制研究所「捜査関係事項照会問題」研究タスクフォース「捜査関係事項照会対応ガイドライン（案）への意見募集（2020年3月17日)」
https://jilis.org/proposal/pages/2020-03-17.html

通信の秘密に関して、電気通信事業法は、「電気通信事業者の取扱中に係る通信の秘密」に関して特別の保護を規定している（第４条，第 179 条）。そして、通信の秘密には、通信内容以外に、個別の通信の通信当事者がどこの誰であるかということや、いつ通信を行ったかということも含まれると考えられている[12]。

総務省のガイドラインによると、通信の秘密に当たる情報については、捜査関係事項照会に応じることは適当でなく、裁判官の発付する令状により強制処分として捜索・押収等がなされる場合に限って提供されるべきであるとされており[13]、電気通信事業者の実務もこれに従っている。

携帯電話に関する位置情報については、携帯電話事業者が取得しうる位置情報のうち「個別の通信を行った基地局の位置情報」は，通信の秘密であると考えられている。通信の秘密に該当する情報については、「通信当事者の同意を得ている場合、裁判官の発付した令状に従う場合その他の違法性阻却事由がある場合を除いては、他人への提供その他の利用をしてはならない」とされ、基本的には令状の取得が求められている。また、「位置登録情報（端末所在地を基地局単位等で把握する情報）」や「GPS 位置情報」についても，「ある人がどこに所在するかということはプライバシーの中でも特に保護の必要性が高い上に、通信とも密接に関係する事項であるから，通信の秘密に準じて強く保護することが適当である」ため，「利用者の同意を得る場合又は違法性阻却事由がある場合に限定することが強く求められる」としており[14]、令状によることが原則であると考えられる。

この他に、法律上の守秘義務が課せられている分野がある。例えば、医師等の医療従事者および医療機関は、業務上知りえた他人の秘密を第三者に漏らすことが禁じられており、これに違反すると罰則がある[15]。ただし、「守秘義務を定める刑事・行政上の諸規定では、『正当な理由』があれば義務違反はないとされるのが一般的」であるとされ、任意捜査に対する協力であっても正当な理由があると認められると考えられている。犯罪捜査における医療従事者からの情報提供は、任意捜査であっても、「正当な理由」が認められる[16]。

なお、犯罪捜査にとって重要性を増しているものとして、DNA に関する情報がある。警察庁では、平成 17 年 9 月から、被疑者 DNA 型記録及び遺留 DNA 型記録を登録・対照す

12 「電話の発信場所は，発信者がこれを秘匿したいと欲する場合があり得るから，右の第 2 項にいう『他人の秘密』に該当すべきものと解すべき」昭和 38 年 12 月 9 日内閣法制局一発第 24 号.「通信内容はもちろんであるが，通信の日時，場所，通信当事者の氏名，住所・居所，電話番号などの当事者の識別符合，通信回数等これらの事項を知られることによって通信の意味内容が推知されるような事項全てを含むものである」（多賀谷一照他編著『電気通信事業法逐条解説』（財団法人電気通信振興会，2008）38 頁）。

13 総務省「電気通信事業における個人情報保護に関するガイドライン（平成 29 年総務省告示第 152 号。最終改正平成 29 年総務省告示第 297 号）の解説」（平成 29 年 9 月（平成 31 年 1 月更新）61-62 頁。

14 総務省・前掲注 13）114-115 頁.

15 刑法 134 条（秘密漏示罪）等。

16 米村滋人『医事法講義』（日本評論社、2016 年）143 頁脚注 100。

る DNA 型データベースの運用を開始し、捜査に活用している[17]。DNA に関する情報は、捜査機関以外にも、医療機関や研究機関等者においても蓄積されているが、現在のところ捜査目的でこれらの情報の提供を求めることはされていないものと考えられる。ただし、将来的にはこのような情報が捜査に有効に活用できるようになる可能性は高く、もし利用を考えるのであればルールを明確にする必要があると考えられる[18]。

２．米国

２．１．捜査手続に関する制度

合衆国憲法第 4 修正は、不合理な捜索、押収、抑留を禁止しており、令状が発布されるのは「相当の蓋然性のある根拠（probable cause）」がある場合に限られるとしている。そして、プライバシーに対する合理的な期待は保護される。ただし，第三者に自ら提供した自分に関する情報については，プライバシーの期待が及ばないという「第三者法理（Third Party Doctrine）という考え方が、広く支持されてきた[19]。

この第三者法理については，携帯電話事業者が保有する位置情報（基地局情報）については、この法理が妥当ではなく合理的なプライバシーの期待が保護されるという連邦最高裁判所判決が注目された。問題となったのは、捜査機関が、携帯電話会社に対して、裁判所命令によって位置情報（基地局情報）の提出を求めた事例である。裁判所命令の発布には、「合理的理由（reasonable ground）」があれば足りるとされており、令状の発布に求められる「相当の蓋然性のある根拠（probable cause）」に比べると、要件が緩やかであると考えられている。裁判所は、この位置情報についてもプライバシーの合理的な期待が保護されるとして、提出を求めるには令状に基づかなければならないという判断を示している。ただし、この判決は、第三者法理そのものを否定しているわけではない。携帯電話の位置情報が、対象者の生活全体についての履歴を詳らかにし、内面的な要素も推知させうる情報であるため、これについてはプライバシーの期待を保護すべきだとしており、対象情報の特殊性が特に強調されている[20].

また、捜査機関は、文書提出命令状（subpoena）によって第三者が保有する情報にアクセスすることもできる。命令状発布に求められるのは、「相当の蓋然性のある根拠」よりも

---

17 警察庁『平成 24 年警察白書』（ぎょうせい、2012 年）43 頁。2015 年 4 月からは、身元不明死体に関する資料から作成した DNA 型記録や、特異行方不明者本人、その実子、実父又は実母に関する資料から作成した DNA 型記録もデータベースに登録されている（警察庁『令和元年警察白書』（日経印刷、2019 年）119-120 頁）。

18 DNA を構成する塩基配列データがデジタル化された情報は個人識別情報に当たるため、これを含む情報は個人情報となる（個人情報保護法第 2 条 1 項 2 号、2 項 1 号）。また、情報の内容によっては要配慮個人情報に該当する場合もあり得る（同 3 号）が、要配慮個人情報に該当する場合であっても、個人情報保護法上は、23 条 1 項 1 号に基づく個人データの提供が可能であると考えられる。

19 JOSHUA DRESSELER et al., UNDERSTANDING CRIMINAL PROCEDURE 65-76 (7th ed. 2017).

20 Carpenter v. United States, 138 S. Ct. 2206, 2221 (2018).

格段に緩やかな「合理性（reasonableness)」である。手続きも非常に簡単であり[21]、例えば大陪審命令状（grand jury subpoena）であれば、検察官自身が起案し、あらゆる書籍、文書、資料、データその他の対象物を指定して提出させることができ、「法が侵されていない」ことを確かめるためという理由でも認められる[22]。対象者の異議申立が認められることはほとんどなく、違法収集排除などが認められることも少ないため、第 4 修正がプライバシーの保護に関して有効に機能していないという指摘がある[23]。

犯罪捜査における捜査の必要性と本人のプライバシー保護のバランスを図るためには、制度的差止命令を積極的に検討することや[24]、公的収用に正当な補償をもとめる収用条項（第 5 修正）の考え方を用いて本人への金銭的補償と、コスト負担によるプライバシー侵害の抑制を図ること[25]なども提言されている。ただし、こうしたアプローチはいずれも、少なくとも本人が捜査機関による情報の取得を認識していることが前提になる。

また、アメリカ法律家協会（ABA : American Bar Association）は、第三者の保有するデータに対する捜査について、2011 年に「犯罪捜査機関の第三者保有記録へのアクセスに関する基準」を公表している[26]。これは、捜査機関による第三者保有情報へのアクセスの必要性を認めつつ、適切なルールが必要であるという考え方に基づくものである。この基準では、対象となる情報の私事性（private）のレベルを 4 段階（高度、中程度、最小限、なし）に分けて、それぞれのレベルに応じた保護を講じるべきであるとしている（基準 25-4.1)。どのレベルに属するかを判断するには、当該第三者にどのような背景で提供された情報であるか、情報が公開された場合に本人がどのような不利益を被るか、通常親密なものにしか公開されていない情報であるかどうか、政府以外の機関に提供されているかどうか、法律による特別な規制や手続があるかどうか、といった要素が考慮される。ただし、こうしたレベルは、技術の進歩や社会状況、情報に対するニーズによって変化するため、個別の情報のレベル判定に明確な答えを出すものではない（「基準 25-4.1 の解説」)。高度または中程度の私事性をもつ情報が含まれており、本人の同意その他の提供が許容されるための条件を満たさない場合には、裁判所命令や召喚状に基づく必要があり、特別に高度な私事性を有する場合にはさらに制約が課せられ得るとしている（基準 25-5.3)。また、法執行機関が、中程度以上の私事性を持つ情報にアクセスした場合には、本人に 30 日以内に通知するべきであるとしている。ただし、生命や身体の安全の危険や、捜査上の必要性、法律の特別の規定などがある場合には、情報へのアクセスを許可した裁判所が、通知の延長を行うことが想定されて

---

[21] Andrew E. Taslitz and Stephen E. Henderson, *Reforming the Grand Jury to Protect Privacy in Third Party Records*, 64 AM U L REV 195, 199 (2014).
[22] United States v Morton Salt Co, 338 US 632, 643 (1950).
[23] Michael C. Pollack, *Taking Data*, 86 U. CHI. L. REV. 77, 90 (2019).
[24] 稲谷龍彦『刑事手続におけるプライバシー保護　熟議による適正手続の実現を目指して』（弘文堂、2017 年）217-222 頁。
[25] Pollack, *supra* note 23, at 99-106.
[26] AMERICAN BAR ASSOCIATION, LAW ENFORCEMENT ACCESS TO THIRD PARTY RECORDS STANDARDS (3rd. ed. 2013) available at https://www.americanbar.org/groups/criminal_justice/standards/law_enforcement_access/

いる。

２．２．個人情報保護

米国には、後述の EU における「個人データの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規則（GDPR)」[27]のような包括的な個人情報保護のための連邦法はない。個々の産業や公的機関ごとに、それぞれの分野で個人情報を保護するためのさまざまな法律が存在している。

例えば、FTC 法第５条では、「商取引における不当な競争方法及び商取引に影響を与える不当または欺瞞的な行為または慣行は、ここに違法であると宣言する」と規定されており、FTC（連邦取引委員会：Federal Trade Commission）では、この規定に基づいて消費者のプライバシー規制を行っている。なお、正当な権限のある法執行機関への個人データの提供は、特別な法律によって守秘義務が課せられている場合などを除き、「不当または欺瞞的な行為または慣行」には当たらないと考えられる。

２．３．特別な種類のデータ

公衆電気通信サービスを提供している事業者が保有している通信に関する情報については，SCA（the Stored Communication Act of 1986, 18 U.S.C. §§2701-2712.）が、捜索差押令状や裁判所命令を求める規定を定めている．SCA は、通信に関する情報を、ISP が保有する電子メールの内容（content data）とそれ以外の情報（non content data）に分けている。電子メールの内容のうち保存期間が短いものについては「相当の蓋然性のある根拠（probable cause)」に基づく捜索差押令状を求めているが、それ以外については「信じるに足る合理的な理由（reasonable ground to believe）」によって認められる大陪審命令状、行政命令、裁判所命令等によって開示を求めることができる。これらの命令に際しては、本人への通知が求められるが、通知によって捜査に支障が生じうるなどの問題があると「信じるに足る理由（reason to believe）」がある場合には、この通知を 90 日間延期することができ、政府機関は必要があればさらに 90 日の延期を求めることができる。それ以外の情報のうち、利用者名、住所、電話番号、ネットワークアドレス、契約期間、支払情報、接続時間等の記録については、行政命令や大陪審命令状によってアクセスが可能であり、利用者への通知も求められない。この他、電子メールの宛名や訪問したサイトに関する情報については、令状または裁判所命令が必要である。このように、SCA の制度は非常に複雑であり現状にそぐわないという批判もあるが、捜査機関が第三者である電気通信事業者に情報の提供を求める際に、一定の制約を課している。

医療機関の守秘義務に関しては、アメリカ医師会（American Medical Association）の倫理規範で、医師が患者の個別の同意なしに患者の健康に関する情報を提供できるのは、次の場合に限られるとしている[28]。

---

[27] The European Union, 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.

[28] AMERICAN MEDICAL ASSOCIATION, CODE OF MEDICAL ETHICS: PRIVACY, CONFIDENTIALITY AND MEDICAL RECORDS (June 25, 2019) available at https://www.ama-

・ 治療を行う目的、またはヘルスケア業務のために他の医療従事者に開示する場合。
・ 適切な当局に対する開示で、法律によって開示が要請されている場合
・ 患者が 1)深刻な自傷行為、2)具体的な他者への深刻な加害行為、を行う蓋然性が高いという医者の判断に基づき、脅威を軽減するために他の第三者への提供する場合

これに関連して、やや特殊な事例であるが、州立病院が行った尿検査におけるコカインの陽性結果の警察への報告によって患者が逮捕されたことについて、患者の同意がなければ不合理な捜索になるとした連邦最高裁判所の判決がある[29]。

また、米国でも、捜査機関によって被疑者等から採取した DNA 情報のデータベース化が進められている。現在のところ、医療機関や研究機関が構築した DNA データベースへの捜査機関のアクセスの可否はあまり問題となっていないが、将来的にはルールが必要だという指摘がある[30]。

３．EU

３．１．捜査手続に関する制度

欧州連合基本権憲章[31]では、第 7 条に「私生活および家庭生活の尊重を受ける権利」が定められており、第 52 条第 1 項には、「この憲章で認められている権利及び自由の行使に対する制限は、法律で規定され、かつ、それらの権利及び自由の本質を尊重しなければならない。比例の原則に従い、制限は、必要であり、かつ、連合が認める一般的利益の目的又は他人の権利及び自由を保護する必要性に真に合致する場合に限り、行うことができる」とする規定がある。

基本的人権を侵害する可能性のある調査には、法定の手続きが必要であり、比例原則に合致したものでなければならない。しかし、法執行機関に自発的に提供された場合には、原則として令状は必要とされないと考えられている。例えば、ドイツ連邦刑事訴訟法では、「証拠として関連性があり、人の保管下にあり、自発的に引き渡されていないものの押収」について、裁判所の命令が必要であると規定している（§92（2））[32]。

３．２．個人情報保護制度

2000 年の欧州連合基本権憲第 8 条は、個人データの保護を基本的人権であるとして、「その情報の関係者の承諾か、その他の法定の適法な根拠に基づいて、限定された目的のために、公正に取り扱われなければならない」ことと、「何人も、自分に関して収集されたデータに対してアクセスする権利および情報を訂正する権利を有する」ことが定められている（第 2

---

assn.org/delivering-care/ethics.

[29] Ferguson v. City of Charleston, 532 U.S. 67 (2001). この事例では、検査の実施に治療上の必要が認められるとしても、尿検査自体が警察と共同で策定した方針に基づいて行われており、検査の実施自体も不合理な捜索であるとされている。

[30] MARC L. MILLER et al., CRIMINAL PROCEDURES, 455-456 (6th ed. 2019).

[31] Charter of Fundamental Rights of the European Union, 7 December 2000. 2009 年にリスボン条約が発効したことを受けて、基本権憲章は欧州連合基本条約と同等に位置づけられている。

[32] MICHAEL BOHLANDER, PRINCEPLES OF GERMAN CRIMINAL PROCEDURE 88-89 (2012).

項)。そして、2016 年 4 月には GDPR が採択され、2018 年 5 月 25 日に加盟国への適用が開始されている。

GDPR 第 6 条では、個人データの処理は、同条に規定された正当な理由のうち少なくとも 1 つが適用される場合に限り合法であると規定されており、法執行機関への個人データの提供は、「(c)管理者が服する法的義務を遵守するために取扱いが必要となる場合」に該当する場合が多いと考えられている。

何が「法的義務」に当たるのかは、必ずしも明確にされていないが、単に捜査の正当な権限を有しているということだけでなく、その捜査を行う明確な権限が法律で定められていることが必要だと考えられている[33]。具体的に捜査機関に求められる手続きについては、各構成国の国内法によってかなり違いがあるという指摘もあるが[34]、少なくとも明確かつ具体的な法的義務の規定と、救済手段の確保が求められるものと考えられる[35]。

捜査機関による個人データの処理に関しては、2016 年に、警察・刑事司法当局指令（DIRECTIVE (EU) 2016/68）[36]が採択されている。この指令は、犯罪の抑止、捜査、取調べ、起訴や、刑罰の執行のために法執行機関が行う個人データの処理に関して、人権の保護を図るために定められたものである[37]。

犯罪捜査等の目的のために個人データの保護が制限されることがあることを前提に、法執行機関によって収集される個人データについて、次のような制度を整備するように構成国に求めている[38]。

- 適法かつ公正に処理されること
- 特定された明示的かつ正当な目的のために収集され，これらの目的に沿った処理に限定されること
- 処理目的との関係で，適切かつ関連性があり，過度ではないこと

---

33 ESTELLE DEHON & PETER CAREY, DATA PROTECTION - A PRACTICAL GUIDE TO UK AND EU LAW, 42 (PETER CAREY, et al. eds., 5th ed. 2018).

34 PAUL VOIGT & AXEL VON DEM BUSSCHE, THE EU GENERAL DATA PROTECTION REGULATION (GDPR) A PRACTICAL GUIDE, 107-108 (2017).

35 2020 年 7 月 16 日に欧州連合司法裁判所が欧米プライバシーシールドには十分性が認められないと判断したいわゆる Schrems II 決定(Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems, CJEU Case C-311/18)では、米国の FISA（外国諜報監視法： The Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. §§ 1801-11, 1821-29, 1841-46, 1861-62, 1871.）に基づく監視プログラムが、最低限の救済手段を欠き、比例原則違反にもなるとしている。

36 European Union (2016) Directive 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.

37 小向太郎「犯罪捜査における位置情報の取得とプライバシー」情報処理学会研究報告電子化知的財産・社会基盤（EIP） 2020-EIP-87、2020-02-14。

38 EU, Protecting personal data when being used by police and criminal justice authorities (from 2018), available at https://eur-lex.europa.eu.

- 必要な範囲で正確かつ最新に保たれること
- 処理の目的に必要な期間を超えて個人の識別を可能にする形式で保持されないこと
- 無権限または違法な処理がされないための保護も含め，適切な安全管理がされていること

また，法執行機関が処理する異なるカテゴリーの情報（①相当な根拠を持って犯罪者と判断できる者、②有罪判決を受けた刑事犯、③犯罪被害者、④証人になりうる者など犯罪の関係者）を、それぞれ明確に区別すること（６-7 条）や、情報保有の制限（保存期限の設定や定期的なレビュー）について（5 条）も規定がある。

法執行機関は、本人に対して情報提供（処理を行う機関に関する情報、データ処理の目的とその法的根拠、監督機関と苦情申立方法、データへのアクセス方法等）をしなければならず（13 条）、本人がこういった情報にアクセスする権利も保障されている（14 条）。ただし、情報提供やアクセスの権利については、捜査上の必要性や公共の安全等のために制限される場合がある。データ処理の実施に関する記録の作成も求められる（24 条）。

さらに、構成国には、この分野のデータ処理に関する監督機関を設置し、適切な権限を付与することも求められている(45-49 条)。

３．３．特別な種類の情報の保護

GDPR は、いわゆるセンシティブ情報に関して、「特別な種類の個人データ（第 9 条）」として、特別の規定を置いている。対象となるのは、人種、民族的、政治的思想、宗教、信条、労働組合への参加が分かってしまうような個人データの処理、および、遺伝データ、自然人を一意に識別するバイオメトリックデータ、健康に関するデータ、性生活又は性的指向に関する個人データの処理である。これらの個人データの処理は原則として禁止され、本人の同意に基づいて処理が許容される場合でも、より厳格な、明示的な同意（explicit consent）が求められている。明示的な同意がなくても取扱いが許されるのは、法律上の義務を遵守するためや、公共の利益において若しくは管理者に与えられた公的な権限の行使において行われる職務の遂行のために、特に規定が設けられている場合に限られる（第２項(b)～(j)号）。

通常の個人データよりも強いセーフガードが求められていると考えられており、比例性、データの最小化、データの安全性などへの配慮が必要とされる[39]。警察・刑事司法当局指令では、特別な種類の個人データは、厳格な必要性と本人の権利と自由のための救済手段があり、EU 法または構成国法に基づいて認められる場合、データ主体又は他の自然人の生命に関する利益を保護するために取扱いが必要となる場合、本人によって明らかに公表されているデータに関する処理である場合、に限定している（10 条）。

電気通信に関わる情報については、e プライバシー指令(個人データの保護および電子通

[39] LUCA TOSONI, THE EU GENERAL DATA PROTECTION REGULATION (GDPR): A COMMENTARY 381 (CHRISTOPHER KUNER et al. eds., 2020).

信分野のプライバシー保護に関する欧州議会および理事会の指令[40])が、「EU 域内の公衆通信網における公的に利用可能な電子通信サービスの提供に関連して行われる個人データの処理」であり、基本的に EU 域内の電気通信サービスを対象とする規定を定めている[41]。電気通信サービスとしては、例えば、データ収集やユーザ識別の機能がある端末を利用するものが想定されている（第 3 条）。ただし、犯罪捜査に関しては、GDPR と同様に管理者が対象とする法的義務を遵守するために必要な場合は適用が除外されると考えられている[42]。ただし、通信傍受や通信履歴に関して捜査を行う場合には、各国で捜査に関する特別な令状を要求するなどの規制が設けられている。

DNA データベースに関しては、例えばドイツでは、いわゆるバイオバンクに個人が提供した検体等を利用して捜査機関が遺伝子分析を行うことを禁止する規定がある[43]。また、ドイツには、捜査機関がデータベースを使って不特定多数から容疑者をあぶり出す捜査手法（ドラグネット捜査）について、特別な令状を求める規定がある[44]。ドイツ連邦刑事訴訟法は、「裁判所または検察官は、他のより限定的な捜査方法では十分な結果が得られない場合に限り、補完的措置としてドラグネット捜査を命じることができる」と定めている。この命令によって、既存のデータセットと多数の人物の照合を行い、容疑者を見つけ出し、無関係の人物を除外するための追加資料を入手することが可能である（98 条 a）。この対象となる犯罪は、組織犯罪や、その他の薬物、武器、通貨法制、国家安全保障、公共の危険の惹起、生命身体、性的自律、個人の自由を脅かす重大犯罪等に限定される（98 条 a）。また、対象データは、データを保管している主体から、通常、捜査に関連するデータとして特定され、その他の保存データから分離された形式で、検察に提出されなければならない。このような分離が難しい場合には、データセット全体を提供することが許されるが、特定されていないデータの利用は禁止されている（98 条 a(3)）。裁判官ではなく検察官がこの命令を行った場合には、3 営業日以内に裁判所の確認を得る必要があり、これを得られない場合には失効す

---

40 Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications).

41 e プライバシー指令は、GDPR の成立を踏まえて、ネットワーク上の新たな問題に対応するために、規則に改正することが検討されている。そして、現在公表されている e プライバシー規則案では、GDPR で EU 市民等の情報が扱われる場合に広く適用を広げたことも踏まえて、対象サービスと適用範囲が拡大されている（小向太郎・石井夏生利『概説 GDPR 世界を揺るがす個人情報保護制度（NTT 出版、2019 年）68-73 頁参照）。

42 IAN WALDEN, COMPUTER CRIMES AND DIGITAL INVESTIGATIONS 275 (2nd ed. 2016).

43 BOHLANDER, *supra* note 32, at 87 (2012).

44 ドラッグネット捜査が最も早く成功した例としては、1979 年にドイツ赤軍のテロリストに対して行われた事件がある。この事件では、法執行当局が、現金でアパートを購入した人のリスト（約 18,000 人）を検索して、フランクフルトに潜伏しているテロリストを探すために、各種法的記録（奨学金、土地登記、火災保険、健康保険など）に記載されている実名を除外して、偽名を使ったテロリストを探し出した。有効な捜索方法として認識されているが、プライバシーを懸念する声も多く、連邦法や州法では令状を求める制度が設けられている。MW Hentschel and NF Pötzl (1986), *Die Position der RAF hat sich verbessert*, Der Spiegel August 9, available at https://www.spiegel.de/spiegel/print/d-13519259.html.

る（98 条 b(1)）。

４．検討

以上のように、第三者が保有するデータについて捜査が行われる場合に本人の権利を保護するためには、3 つの制度的なアプローチがある。

第一に、捜査手続に関する制度では、捜査が令状等の法定手続に従って行われることを要求するのが基本である。基本的人権の保障と犯罪捜査の必要性のバランスをとるために、捜査の目的や目的について裁判官による審査が行われ、裁判官が発布した令状が捜査対象者に提示される。これによって、刑事手続きによる権利侵害の抑制と、透明性の確保が図られている。しかし、捜査対象者が自主的に捜査機関に協力すれば、令状などの法的手続きを経ることなく情報が取得される可能性がある。捜査対象者が第三者である場合には、特別な守秘義務を課されているのでなければ、捜査協力を拒否するインセンティブは低い。また、自分の情報が取得されていることを本人が知らない場合には、権利侵害を主張することができない。このような問題を解消するために、例えば、アメリカ法律家協会「犯罪捜査機関の第三者保有記録へのアクセスに関する基準」では、私事性の高い情報に対する捜査が行われる場合には、本人に通知されることが望ましいと提言している。ただし、捜査手続に関する制度としてこのような仕組みを導入する場合には、適正な運用が行われているかどうかのチェックをどのように行うかが問題になるであろう。

第二に、個人情報保護制度においては、通常、利用目的の明確化と透明性が求められている。ただし、正当な権限のある捜査機関に対して捜査のために個人情報を提供することは、例外として認められることが多い。犯罪捜査においては、個人情報の保護がある程度制約されざるを得ない。捜査の必要性を考慮したうえで個人情報の保護を図るために、両者のバランスを目指す制度としては、EU 警察・刑事司法当局指令が注目される。特に透明性の確保（情報公開、記録の保存等）や、独立の監督機関に関する規定は重要であると考えられる。また、犯罪捜査のために利用される個人情報には、被疑者、犯人、犯罪被害者、その他の利害関係者など、性質の異なるカテゴリーのデータが含まれている。これらの区別を明確にすることも重要であろう。

第三に、特別な種類の情報については、第三者に守秘義務を課して捜査機関から提供を求められた場合でも、法定手続きに基づいて対応することが求められている。こうした制度のなかには、令状に厳格な要件を求めるもの（通信傍受制度、ドイツのドラッグネット捜査等）や、本人に対する通知を義務付けているもの（米国 SCA 等）もある。

表１．各アプローチの比較

	捜査手続に関する制度	特殊な種類の情報に対する保護	個人情報保護制度
対象データ	プライバシーが懸念される情報	通信の秘密、医療情報、DNA情報等	個人情報

捜査の制限	令状、裁判所命令等（異議申立、補償等）	令状、裁判所命令等（特別な要件の加重）	利用目的の限定、提供に関する記録等
透明性	－	（本人への通知義務）	情報公開、本人によるアクセス
問題点	透明性・本人関与の欠如	対象が限定的	適用除外

（出典）筆者作成

当然のことであるが、これらのアプローチは、それぞれに目的や効果が異なる。第三者が保有するデータに対する捜査において、本人の権利保護と捜査の必要性とのバランスを図っていくためには、これら 3 つのアプローチのそれぞれについて、必要な制度を整備することが必要である。

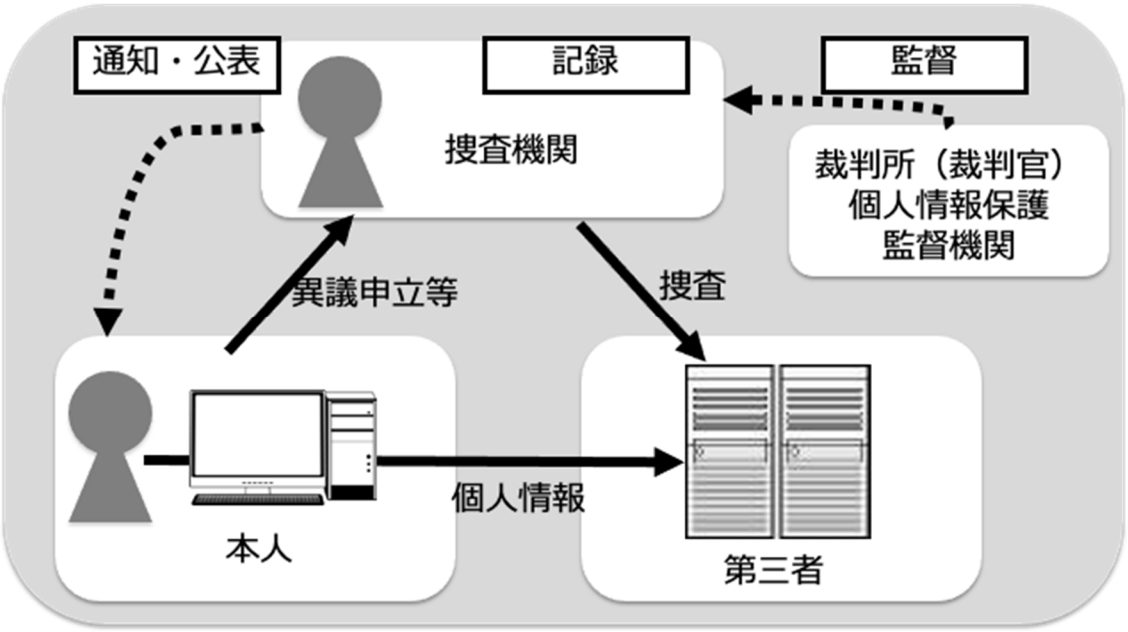
日本ではこの問題に関する包括的な議論がほとんどなされていない。特に、①捜査機関による情報取得の透明性、②本人の保護や救済の仕組み、③通信の秘密以外の特別な種類の情報に対する保護、については検討が必要である。

まず、「①捜査機関による情報取得の透明性」については、個人情報保護制度において、個人情報の取得や利用に関する記録の保存、情報公開や本人への通知を捜査機関に対しても義務付けることが考えられる。ただし、捜査上の必要性等の理由で情報公開や本人への通知が制限する規定も必要であろう。

次に、「②本人の保護や救済の仕組み」については、個人情報保護に関する監督機関が関与する制度が望ましい。現在、個人情報保護制度について、行政機関、独立行政法人等に係る法制と民間部門に係る法制との一元化が検討されており、所管を個人情報保護委員会に一元化することが提案されている[45]。現在のところ、行政機関に対する監督権限について限定的な考え方が示されているが、将来的には、犯罪捜査機関による個人情報の取扱も含めて、独立専門の監督機関が関与する制度を整備すべきであろう。

[45] 個人情報保護制度の見直しに関する検討会「個人情報保護制度の見直しに向けた中間整理案」（令和 2 年 8 月）35-40 頁。

図 2. 透明化のためのスキーム（イメージ）



（出典）筆者作成

また、「③通信の秘密以外の特別な種類の保護」に関しては、日本では通信の秘密については、捜査機関への提供がかなり慎重に行われており、ルールも明確化されている。しかし、その他の分野では、守秘義務の対象になっていない場合や、運用が必ずしも明確でない場合がある。特に DNA 情報などの技術の発展によって重要性と危険性が増大する分野については、できるだけルールを明確化しておくことが望ましい。

５．おわりに

犯罪捜査における捜査対象者の権利の保障は、強制処分法定主義や令状主義の考え方によって図られてきた。しかし、これらが有効に機能するためには、それに対する異議申立がありうることが前提になる。強制処分は、強制されなければ対象者が協力を拒否するから強制処分なのであり、自分が保有する情報について強い利害関係を持たない第三者に対して情報の提供が求められる場合には、十分に機能しない可能性がある。

現在では、情報技術の発達で膨大な量の情報が収集・保存されるようになったことにより、第三者が保有している情報に対する本人の利害が、以前とは比べ物にならないほど大きくなっている。そもそも、個人情報保護制度はこのような状況から発展してきたものであり、透明性や本人の関与が求められるようになった理由もここにある。

一方で、犯罪捜査の世界では、地道な情報収集は捜査の基本である。どのような情報を捜査機関が持っているのかを全て被疑者に知られてしまっては困る。捜査機関の側からすれば、個人情報を保有する第三者に捜査協力を依頼することは、「張り込み」や「聞き込み」等の伝統的な捜査の延長線上にあるものであろう。情報の本人の人権に配慮して抑制したり、本人にして情報を取得していることを知らせたりすることを、捜査機関の自主的な取組

として求めることは、難しい面がある。また、犯罪捜査が過度に抑制され、社会の安全が損なわれることが望ましくないのは言うまでもない。

これらのバランスを、犯罪捜査手続きに関する制度だけで実現することは難しい。個人情報保護制度や特別な情報に対する法的保護とあわせて、相互補完的な制度を検討していくことが必要である。

本研究は、日本学術振興会科学研究費（JP18K01393）の助成を受けて行った。

参考文献

1. Richard A. *Posner, Privacy, Surveillance, and Law*, 75 U. CHI L. REV. 245 (2008).
2. 小向太郎「ビッグデータと捜査機関との情報共有」山本達彦・横大道総・大林啓吾・新井誠編『入門・安全と情報』（成文堂、2015 年）。
3. 共同通信社会部取材班「丸裸にされる私生活　企業の個人情報と検察・警察」世界 921 号 (2019)。
4. 個人情報保護委員会「日 EU 間・日英間のデータ越境移転について」、https://www.ppc.go.jp/enforcement/cooperation/cooperation/sougoninshou/
5. 宇賀克也『個人情報保護法の逐条解説』（有斐閣，第 6 版，2018 年）。
6. 一般財団法人情報法制研究所「捜査関係事項照会問題」研究タスクフォース「捜査関係事項照会対応ガイドライン（案）への意見募集（2020 年 3 月 17 日）」https://jilis.org/proposal/pages/2020-03-17.html
7. 多賀谷一照他編著『電気通信事業法逐条解説』(財団法人電気通信振興会、2008 年)
8. 総務省「電気通信事業における個人情報保護に関するガイドライン（平成 29 年総務省告示第 152 号。最終改正平成 29 年総務省告示第 297 号）の解説」（平成 29 年 9 月（平成 31 年 1 月更新)。
9. 米村滋人『医事法講義』（日本評論社、2016 年)。
10. 警察庁『平成 24 年警察白書』（ぎょうせい、2012 年)。
11. 警察庁『令和元年警察白書』（日経印刷、2019 年)。
12. JOSHUA DRESSELER et al., UNDERSTANDING CRIMINAL PROCEDURE (7th ed. 2017).
13. Andrew E. Taslitz and Stephen E. Henderson, *Reforming the Grand Jury to Protect Privacy in Third Party Records*, 64 AM U L REV 195 (2014).
14. Michael C. Pollack, *Taking Data*, 86 U. CHI. L. REV. 77 (2019).
15. 稲谷龍彦『刑事手続におけるプライバシー保護　熟議による適正手続の実現を目指して』（弘文堂、2017 年）217-222 頁。
16. AMERICAN BAR ASSOCIATION, LAW ENFORCEMENT ACCESS TO THIRD PARTY RECORDS STANDARDS (3rd. ed. 2013) available at https://www.americanbar.org/groups/criminal_justice/standards/law_enforcement_access/

17. AMERICAN MEDICAL ASSOCIATION, CODE OF MEDICAL ETHICS: PRIVACY, CONFIDENTIALITY AND MEDICAL RECORDS (June 25, 2019) available at https://www.ama-assn.org/delivering-care/ethics.
18. MARC L. MILLER et al., CRIMINAL PROCEDURES (6th ed. 2019).
19. MICHAEL BOHLANDER, PRINCEPLES OF GERMAN CRIMINAL PROCEDURE (2012).
20. ESTELLE DEHON & PETER CAREY, DATA PROTECTION - A PRACTICAL GUIDE TO UK AND EU LAW (PETER CAREY, et al. eds., 5th ed. 2018).
21. P PAUL VOIGT & AXEL VON DEM BUSSCHE, THE EU GENERAL DATA PROTECTION REGULATION (GDPR) A PRACTICAL GUIDE (2017).
22. LUCA TOSONI, THE EU GENERAL DATA PROTECTION REGULATION (GDPR): A COMMENTARY (CHRISTOPHER KUNER et al. eds., 2020).
23. 小向太郎「犯罪捜査における位置情報の取得とプライバシー」情報処理学会研究報告電子化知的財産・社会基盤（EIP） 2020-EIP-87、2020-02-14。
24. 小向太郎・石井夏生利『概説 GDPR 世界を揺るがす個人情報保護制度（NTT 出版、2019 年）。
25. IAN WALDEN, COMPUTER CRIMES AND DIGITAL INVESTIGATIONS (2nd ed. 2016).
26. MW Hentschel and NF Pötzl (1986), *Die Position der RAF hat sich verbessert*, Der Spiegel August 9, available at https://www.spiegel.de/spiegel/print/d-13519259.html.
27. 個人情報保護制度の見直しに関する検討会「個人情報保護制度の見直しに向けた中間整理案」（令和２年８月）。