コンピュータ集積情報の捜査とプライバシー

研究代表者　　小　向　太　郎　　日本大学危機管理学部教授

1 はじめに

本研究では、コンピュータ上に大量に蓄積されているデータに対して犯罪捜査が行われる場合における、情報主体（本人）のプライバシーや個人情報の保護に関する問題を検討した。

IoT 等の技術によって収集される膨大な情報は、被疑者等の本人が想定し得ない情報取得、高度な解析による思いがけない情報生成などを生じる可能性がある。例えば、ネットワークサービスの提供事業者に大量の情報が蓄積されている場合に、捜査機関がこうした事業者から任意に情報の提供を受けることで、情報主体の行動が詳細に判明する可能性がある。このような場合には、情報を保有している事業者にとって捜査に協力することに抵抗が少ない場合も多い。また、こうした第三者に対して強制捜査が行われる場合には、被疑者が認識しないうちに情報が収集される可能性がある。しかし、一方で、こうした情報が犯罪捜査にとっても有用であることは疑いがない。

本研究では、まず、急速に収集や集積が進みつつある情報のなかでも、犯罪捜査に非常に有益でありプライシー性も高いと考えられる情報として、対象者の行動や位置に関する情報に着目した。次に、わが国では、「通信の秘密」に当たる情報とそれ以外の情報の差が大きいことを確認した。さらに、海外の議論動向として、特に米国における「第三者法理」に関する判例の変化等について検討した。

そのうえで、日本および米国における動向を踏まえて、蓄積情報に対する捜査に関する課題について、今後のあり方を考察している。

2 集積情報に対する捜査

2-1 行動履歴と犯罪捜査

最近注目を集めている IoT（Internet of Things）やビッグデータ技術において利用されるデータのなかでも、人の行動や位置に関する情報への期待は大きく、具体的な利用分野も幅広い。大規模かつ広範囲に収集される主要な位置情報としては、図表１のようなものがある。

（図表 1）位置情報収集技術の例

端末等種別	ネットワーク接続機器（例）	収集情報（例）
インターネット端末	PC、スマートフォン、タブレット端末、ゲーム機	GPS 位置情報、基地局情報、WiFi アクセスポイント
自動車、重機	カーナビゲーション・システム、自動運転や電気自動車の制御装置、遠隔操作システム	GPS 位置情報、走行情報
カメラ	監視カメラ、デジタルカメラ	顔認識等によるトレース情報、GPS による撮影地情報
ID カード等	POS レジ、IC カードリーダ、RFID リーダ、自動改札	購買場所と登録住所、交通機関の利用経路

出典：小向太郎「ネットワーク接続機器の位置情報に関するプライバシー・個人情報保護制度の動向」情報処理学会研究報告電子化知的財産・社会基盤（EIP） 2016-EIP-74、 2016-11-17

さまざまな機器がネットワークで接続されるようになり、情報が大量に収集処理されることで、従来はあまり意識されなかった POS レジや IC カードリーダによって収集される情報や、監視カメラによって撮影される影像を処理したデータも、位置情報としての意味を持つようになってきている[1]。こうした情報が犯罪捜査にとっても有用であることは疑いがない。

こうした情報の特徴として、個別には意識されにくいものも多いという点を上げることができる。いつどんな情報がとられているか意識されずに、自分についての収集されることが増えており、それをもとにして、さらに情報を生成することも容易になっている。

従来から、写真撮影や通信傍受などの新しい捜査方法の出現にともない、こうした捜査方法が、どのような場合にどのような手続きによって許容されるかということが議論されてきた。しかし、従来の議論は、捜査に協力する者と権利が侵害される者が同一であるか、少なくとも密接な関係にあるような捜査に関する物が多かった。また、情報の利用やそれによって生じる結果も、一般人にとっても十分予測可能なものであった。

しかし、IoT 等の技術によって収集される膨大な情報は、被疑者等の本人が想定し得ない情報取得、高度な解析による思いがけない情報生成などを生じる可能性がある。例えば、ネットワークサービスの提供事業者に大量の情報が蓄積されている場合に、捜査機関がこうした事業者から任意に情報の提供を受けることで、情報主体の行動が詳細に判明する可能性がある。このような場合には、情報を保有している事業者にとって捜査に協力することに抵抗が少ない場合も多い。また、強制捜査であっても、第三者を対象とする捜査が行われる場合には、被疑者が認識しないうちに情報が収集される可能性がある。

2-2 任意捜査と強制捜査

犯罪捜査には任意捜査と強制捜査があるが、できるだけ任意捜査によって行うことが望ましいと考えられている。これは、捜査機関による強制的な捜査は、人権を制約するものであるため、できるだけ強制によらず自発的な協力によって、捜査の目的を達成することが望ましいからである。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」は、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（強制処分法的主義）とともに、任意捜査を原則とする考え方を示すものとされている。

どのような捜査方法が強制の処分となるのかについては、見解が分かれている。まず、強制の処分となるかどうかを判断する基準を、①処分をする側の処分手段とする（有形力の行使または、法的な義務付けがある場合を強制の処分とする）ものと、②被処分者の利益侵害の有無とする（法益の侵害、または一定の重要な利益の侵害がある場合を強制の処分とする）ものがある。そして、②被処分者の利益侵害の有無を基準とする見解には、プライバシー侵害を含む法益全般の侵害をふくむとするものと、特に重要な利益が侵害される場合に限られるとするものがある。

写真撮影や通信傍受などの新しい捜査方法は、必ずしも有形力の行使や法的な義務による強制にあたらないとも考えられるため、法定の手続によらなければ行うことのできない強制処分に当たるかどうかが議論されてきた。ただし、基本的にこれらの捜査方法では、捜査対象者と権利が侵害される者が同一であるか、少なくとも密接な関係にある。

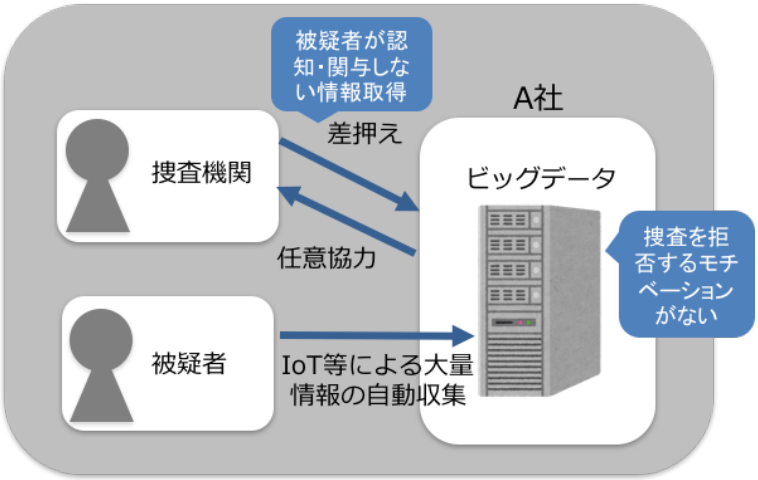
2-3 第三者の保有する情報に対する捜査

現在では、個人に関する情報をさまざまな機関が保有している。それらの機関にとっては、捜査機関の要請を拒否して本人のプライバシーを守ることに、それほど強いモチベーションがない。

従来から、「地取り」「張り込み」「聞き込み」「尾行」などの方法は、任意捜査として比較的広く行われてきた。一方で、盗聴、盗撮、住居への侵入等は問題があると理解されてきた。しかし、ビッグデータの発展によって、個人に関する膨大な情報が蓄積されるようになると、本人のまったく手の届かないところで、本人の情報が捜査機関に入手されるようになる。特に、いわゆるセンシティブ情報について、このような情報が任意開示されることにまったく歯止めがないのでは、強制処分法定主義の趣旨を損なうことになりかねない[2]。もちろん、捜査対象が第三者であっても、プライバシーや個人情報保護の観点から、任意協力を拒絶することはある。しかし、こうした対応が法的に担保されるのは、何らかの守秘義務（通信の秘密、秘密漏示罪等）が対象者に課せられる場合に限られる。

なお、位置情報に関連するものとしては、GPS 装置の無断装着の可否が裁判で争われ、最高裁判所において現行法に基づく強制捜査は困難であるとして新たな立法を求める判断がされている[3]。この判決では GPS 捜査の問題点として「情報の蓄積」が指摘されていることが注目されるが、「物理的侵入」も重要な要素として考慮されており、第三者が保有する個人情報に対する捜査の歯止めとなる規範が提示されているとは言い難い面がある。

（図表 2）集積情報の取得・解析とプライバシー・個人情報保護に関する問題の例



3 行動履歴と守秘義務

3-1 行動履歴と個人情報保護

行動履歴や位置情報のなかには単独では個人情報に該当しないものもあるが、個人に関連して収集されることも多い。わが国の個人情報法保護法においては、「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」や「個人識別符号」が含まれている場合や、そうした情報と「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」場合には、個人情報となる（個人情報保護法 2 条 1 項）。個人情報取扱事業者が個人情報を取扱うにあたっては、利用できる目的をできる限り特定し（第 15 条）、公表等することと（第 18 条）その目的の範囲で利用すること（第 16 条）が求められる。そして、個人情報を収集した事業者が、その事業者内で利用する場合には、特に本人の同意等は求められていない。

これは、「個人情報の有用性を過度に減殺しないために、利用方法、利用目的自体を規制するのではなく、利用目的の通知または公表を契機とする本人等からの苦情等を通じて、個人情報の適正な利用を確保することを基本方針」としたためであるとされる。不適正な取得や（第 17 条第 1 項）、他の法令に抵触する利用は許されないが、利用目的の範囲についての制約は少なく、情報の収集と収集した事業者の内部利用に関して自由度が高い制度である。

しかし、事後的に当初の目的と「相当の関連性を有すると合理的に認められる範囲を超えて（第 15 条第 2 項）」利用目的を変更するのであれば本人の同意が必要となる（第 16 条第 2 項）。また、個人データの第三者提供にも、原則として本人の事前同意が必要である。ただし、法令に基づく場合や緊急性等がある場合（第 23 条第 1 項）、オプトアウト（第 23 条第 2 項）、委託先への提供（第 23 条第 4 項第 1 号）、事業承継（第 23 条第 4 項第 2 号）、共同利用（第 23 条第 4 項第 3 号）には、本人の同意がなくとも、第三者提供が例外として許容される。

3-2 行動履歴と通信の秘密

憲法第 21 条第 2 項は「検閲は、これをしてはならない。通信の秘密は、これを侵してはならない」と定め、通信の秘密を基本的人権のひとつとして保障している。電気通信事業法（4 条、179 条）、電波法（109 条、109 条の 2）、有線電気通信法（9 条、14 条）にもそれぞれ通信の秘密に関する規定がある。例えば、インターネット上でやり取りされる情報は、何らかの形で電気通信事業者が媒介することが多いため、電気通信事業法との関係が特に問題となる。

わが国の電気通信事業法は、「電気通信事業者の取扱中に係る通信の秘密」を侵すことを禁じており（4 条）、

通信の秘密を侵した者に対して刑事罰を科している（第 179 条)。通信の秘密として保護される情報としては、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 。

我が国の電気通信事業者は一般に、通信の秘密に対する任意捜査には応じておらず、通信の秘密に該当する情報の提供を捜査機関が求める場合には、令状（傍受令状または捜索差押え令状等）によることが必要であると考えられている。

インターネット上で情報発信を行っている者に関する情報（発信者情報）については、従来の考え方が通信の内容だけでなくその構成要素まで含めて通信の秘密として保護すべきとしていることを重視すれば、たとえ通信の内容が周知のものであっても、独立して通信の秘密保護の対象となると考えられる。なお、公衆無線 LAN でやりとりされる情報も、当然通信の秘密になる。諸外国の公衆無線 LAN では、提供事業者がセキュリティ上の理由からモニタリングを行っているものも多いが、我が国では通信の秘密に該当するため、通信の伝送に必要と認められる範囲でのみ情報を取得するのが一般的である。

したがって、電気通信事業者が管理するサーバやルータのアクセスログの提出を捜査機関が求める場合には、捜索差押令状が必要である。しかし、例えば、対象となるメールサーバがユーザによって運用されていて電気通信事業者の管理下にない場合には、当該サーバに蔵置された情報は「電気通信事業者の取扱中に係る通信の秘密」ではないと考えられる。また、任意捜査に応じて情報を提供したとしても、通信の秘密侵害罪に問われる可能性は低いであろう。同様の違いは、web サーバや無線 LAN のアクセスログについても生じることになる。

さらに、携帯電話に関する位置情報には、通信の秘密との関係が問題となる。携帯電話事業者が取得しうる位置情報は、「個別の通信を行った基地局の位置情報」「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)」「GPS 位置情報（ GPS 機能により取得する情報)」の 3 種類がある。

このうち「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。さらに、総務省のガイドラインでは「位置登録情報」「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」として、利用者の同意取得等を求めている。そして以前は、捜査機関が令状に基づいて強制捜査する場合であっても「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」ため、「画面表示や移動体端末の鳴動等の方法により、当該位置情報が取得されていることを利用者が知ることができる」ようにすることを求めている[4]。つまり、被疑者等に「捜査機関があなたを探しています」と伝えてから、捜査機関に位置情報を渡すということになる。他の国と比べても、かなり厳格な利用者保護がとられていた。ただし、この被疑者等に通知を行うことを求める規定は、現在では削除されている。

このように従来から、「通信の秘密」に関わる情報は厚く保護され、捜査機関との関係でもきちんとした手続きに基づいて提供がなされてきた。位置情報はすべてが通信の秘密に当たるわけではないが、このような保護の考え方を踏襲している。

3-3　その他の守秘義務

職務の性格から秘密の保持が必要であると考えられる職業については、法律上の守秘義務が課せられている場合がある。例えば、刑法 134 条（秘密漏示罪）は、「医師、薬剤師、医薬品販売業者、助産師、弁護士、弁護人、公証人又はこれらの職にあった者が、正当な理由がないのに、その業務上取り扱ったことについて知り得た人の秘密を漏らしたときは、6 月以下の懲役又は 10 万円以下の罰金に処する（1 項)」「宗教、祈祷若しくは祭祀の職にある者、又はこれらの職にあった者が、正当な理由がないのに、その業務上取り扱ったことについて知り得た人の秘密を漏らしたときも、前項と同様とする（2 項)」と定めており、これ以外にも各種の事業法において守秘義務が課せられているものがある。

法律上の守秘義務を課された者は、正当な理由なく、職務上知り得た秘密を漏らした場合には、処罰の対象となる。ただし、任意捜査への協力が正当な理由になりうるかどうかは明確な基準が示されているとは言えず、一般に通信の秘密ほど厳密な運用がされていないと考えられている。

4 欧米の動向と今後の課題

4-1 行動履歴と個人情報保護

EU の GDPR（一般データ保護規則）において個人データの取扱いが適法とされるのは、次のいずれかを満たす場合に限られる。

(a) データ主体が、一つ又は複数の特定の目的のための自己の個人データの取扱いに関し、同意を与えた場合。
(b) データ主体が契約当事者となっている契約の履行のために取扱いが必要となる場合、又は、契約締結の前に、データ主体の要求に際して手段を講ずるために取扱いが必要となる場合。
(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。
(d) 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。
(e) 公共の利益において、又は、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取扱いが必要となる場合。
(f) 管理者によって、又は、第三者によって求められる正当な利益の目的のために取扱いが必要となる場合。ただし、その利益よりも、個人データの保護を求めるデータ主体の利益並びに基本的な権利及び自由のほうが優先する場合、特に、そのデータ主体が子どもである場合を除く[5]。

適法化根拠は、個人データの取扱いに先立ち、情報とその利用目的ごとに決定しておく必要がある。そして、適法化根拠にどれを選ぶかによって、データ主体がどのようなコントロールを行使できるかが変わってくる。まず、どのような根拠で適法化した場合であっても、「アクセスの権利」、「訂正および消去の権利」、「取扱いの制限の権利」などの権利が、データ主体に認められる。そして例えば、データ主体の同意を根拠とした場合（第(a)項）は、データ主体はいつでも何の負担もなく同意を撤回することができる。また、公共の利益・公的権限の遂行（第(e)項）や正当な利益（第(f)項）が根拠となっている場合には、異議申し立てをすることができる。

また、GDPR は、「同意の条件」を厳格に定めている（第 7 条）。個人データが同意を根拠として扱われる場合には、管理者が証明責任を負うこと（第 1 項）、書面で示される利用規約によって同意内容が示される場合には他の事項と区別しデータ主体が理解しやすい態様で同意を要請すること（第 2 項）、データ主体が同意をいつでも撤回できること（第 3 項）、同意の任意性を判断する際に契約履行に同意を条件づけているか否かを十分考慮すること（第 4 項）が求められる。さらに、管理者は本人に対して、情報収集の事実や本人が管理者にアクセスするために必要な情報等を、知らせることが義務付けられている（第 13 条）。

特に、有効な同意であると認められるためには、①自由な同意、②特定された同意、③事前説明を受けた同意、④不明瞭ではない表示による同意、⑤明らかに肯定的な行為による同意、でなければならない（前文第(32)項）。

一方、米国では、連邦取引委員会（FTC: Federal Trade Commission）が、消費者プライバシーを所轄しており、2012 年３月に「急変する時代の消費者プライバシー保護[6]」という報告書を取りまとめている。この報告書が提示するフレームワークでは、本人意思の反映を重視しており、プライバシー・バイ・デザイン、シンプルで分かりやすい消費者の選択、透明性を重要な要素としてあげている。さらに、消費者が自分のデータに関する決定を行うような状況では選択の機会が与えられるべきであり、（１）データが収集される際に示された方法と大きく異なる方法で利用される場合と、（２）ある目的のためにセンシティブ情報を収集する場合には、積極的な同意の表明を得るべきである」としている。そして、「子供に関するデータ、金融情報と健康情報、社会保障番号、および一定の位置情報は、少なくともセンシティブ・データ」として扱うという考えが示されている（47 頁、注 214）。ただし、これらは事業者に対するベストプライティスを示したものであり、執行の指針を直接示したものではない。

FTC 法 5 条は「商業活動に関わる不公正な競争手段と、商業活動に関わる不公正または欺瞞的な行為または慣行は、違法であることがここに宣言される（15 U.S.C. § 45(a)(1).）」と規定しており、FTC はこの規定に基づく法執行も、積極的に行っている。実際に対象となっているのは、自社のプライバシー・ポリシーや利用規約で個人情報の利用を拒否できるかのように記述しているにもかかわらず、対応を十分にしていなかったことなどが、欺瞞的とされているケースが多い[7]。

4-2 行動履歴と通信の秘密

諸外国の動向をみると、EU では、「個人データの保護および電子通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（電子通信プライバシー指令） 」が 2002 年に採択され、2006 年および 2009 年に改正されている。この指令において位置情報は「電気通信網または電子通信サービスにおいて処理される情報であり、公衆電気通信サービスのユーザ端末機器の地理的な位置を示す情報」と定義され、匿名化されている場合か、(通信サービス以外の) 付加価値サービスの提供のために必要な範囲及び期間に関して、利用者が同意をしている場合に限って、処理することができるとされている。サービス提供者は、位置情報の種類、利用目的、処理期間、データの第三者提供の有無について、同意取得に先立って、利用者・加入者に知らせなければならない（第９条第１項)。また、同意が得られている場合には、利用者・加入者に対して、シンプルな手段によって無料で、当該ネットワークへの接続や電子通信の伝送が行われるたびに、これらの情報の処理をいつでも拒否することを常に可能にしておかなければならない（第２項)。付加価値サービスを提供するための権限を付与された者は、当該付加価値サービスの提供目的に必要なものに限られている場合に、限定されなければならない（第３項)。電子通信プライバシー指令は、GDPR の成立をうけた改正が検討されており、適用対象を電子メールやオンラインメッセージング・サービスに拡大している。現在提案されている規則案が成立すると、WhatsApp、Facebook Messenger、Skype、Gmail、iMessage、Viber のような新しい電子通信サービスの提供事業者についても、適用される可能性がある。

米国の連邦通信法は、「顧客情報のプライバシー」に関する規定を定めており、「全ての電気通信事業者は、他の電気通信事業者（電気通信事業者が提供する通信サービスを再販売する電気通信事業者を含む)、機器製造事業者、および顧客に関連する情報であって、これらの者に帰属する情報の秘密を、保護する義務を負う（47 U.S. C. § 222(a))」とされている。特に、電気通信サービス提供を提供するために取得した CPNI（顧客に帰属するネットワーク情報）は、「(A) そのような情報が生成された電気通信サービス、(B) そのような電気通信サービスの提供に必要であるか、提供の過程で利用されるサービス（電話帳の発行を含む)、のいずれかを提供するためである場合」にのみ利用することができる（47 U.S. C. § 222(c))。ただし、個々の顧客の識別子および特性が当該データから除去した顧客統計情報（「顧客統計情報」とは、「サービスまたは顧客のグループまたは属性に関する集合体のデータであり、個々の顧客の識別子および特性が当該データから除去されているもの」をいう（47 U.S. C. § 222 (h)(2).)）は、これらの目的以外にも利用、開示、またはアクセス可能にすることができる。なお、顧客からの要望にも続いて開示する場合も、「顧客からの明示的な書面による要求」が必要である。

特に、商用携帯電話や IP 音声電話の位置情報を利用するための同意については、事前かつ明確に表明される必要があるとしている（47 U.S. C. § 222(f)). また、商用携帯電話の位置情報については、公共の安全や緊急事態のための必要な場合に利用できることが、例外規定として明示されている（47 U.S. C. § 222(d))。

（図表３）行動履歴の取扱いに関する比較

	個人情報取扱事業者	ネットワーク事業者	備考
EU	本人の同意または正当化事由（法定の利用、公共の利益、適法な利益等）同意の撤回等を保障	サービス提供や課金等のために必要がなくなった場合の匿名化または消去の義務	e プライバシー規則案(適用対象を電子メールやオンラインメッセージング・サービスに拡大)
米国	不公正または欺瞞的な行為または慣行の禁止	法に基づく要請または顧客の同意	FTC レポート(位置情報全般に同意取得を推奨)
日本	利用目的の通知・公表、適正取得、本人同意なき第三者提供の原則禁止等	本人の同意または正当化事由（正当業務行為、緊急避難等）	スマホアプリ事業者に対するガイドライン（同意取得等の推奨)

なお、米国では従来、本人が第三者に提供した情報については、プライバシーを期待することができない

とする「第三者法理」の考え方が取られていたとされ、携帯電話会社の保有する利用者の位置情報に関しても、緩やかな要件で発布される裁判所命令による取得が許されるとされてきた。しかし、 Carpenter v. United States 事件に関する連邦最高裁判所の判決[8]では、このような情報に対してもプライバシーの期待を持ちうるとして、令状による強制捜査によらなければならないという判断が示されている。

4-3 今後の課題

研究を通じて、特に我が国においては、「通信の秘密」に当たる情報とそれ以外の情報の差が大きいことを、あらためて確認した。わが国では、携帯電話事業者が取扱う位置情報は、通信の秘密に準じた取扱がされており、犯罪捜査の対象として捜査が行われる場合でも、強制捜査として令状が必要であると考えられている。しかし、通信の秘密に該当する情報以外にも、現在では個人に関する情報が膨大にコンピュータ上に蓄積されている。これらの情報の多くは、本人が認識しないうちに捜査機関に取得され、その内容が探査解析される可能性が大きくなっている。電気通信事業者が取扱う情報とその他の情報の間のプライバシー・ギャップは、犯罪捜査の分野でより顕著に現れているといえる。

一方で、米国の Carpenter v. United States 事件をみると、わが国における通信の秘密に当たる情報について、米国の犯罪捜査ではあまり厳格に保護されていなかった実態もうかがえる。本件に関する連邦最高裁判所の判断は、特定のカテゴリーに限定されず、第三者が保有する個人情報について捜査機関からのプライバシーが保護される広い射程をもちうるものである。この判断は、合衆国憲法修正 4 条（不合理な捜索、押収、抑留の禁止）に基づくものであるが、このような考え方の対象や範囲をどこまで広げるのかが問題となる[9]。一方で、こうした問題において、実際の保護のレベルは、裁判所命令や令状の運用実態に左右される。こうした内外の運用実態の比較についても、今後の課題としたい。

ビッグデータとして膨大な量の情報が集積利用されると、捜査に利用できる情報も当然に増大していく。社会の安全と治安を維持するためには、こうした情報を犯罪捜査に役立てていくとも必要である。一般論としては、有形力を伴う調査に比べて人権侵害の程度が比較的軽微で、侵害感が少ないこともありうる。

しかし、そもそも強制処分法定主義は、人権を制約する強制処分の乱用を防ぎ透明性を高めるためのものである。そして、個人情報の収集によって侵害を受ける可能性が高いのは、当該情報の本人である。今後、さまざまな情報がいたるところに保存されることによって、本人以外の者に対して捜査機関が情報の提供を求めることは増えることが確実である。

個人情報を保有する第三者を対象とした捜査が制限されるのは、実質的に強制処分に当たると評価される場合（米国：第 4 修正、日本：憲法 35 条）と、特別の立法がある場合（通信の秘密、各種守秘義務等）に限られる。コンピュータの利用が社会隅々まで浸透している現状を考えると、コンピュータ処理される情報に対する犯罪捜査を全て強制捜査として令状を要請するのは現実的でなく、むしろ形骸化を招きかねない。プライバシー保護の観点から保護の必要な場面を具体的に限定して議論することが望まれる。

【参考文献】

[1] 小向太郎「ネットワーク接続機器の位置情報に関するプライバシー・個人情報保護制度の動向」情報処理学会研究報告電子化知的財産・社会基盤（EIP） 2016-EIP-74、 2016-11-17。

[2] 小向太郎「ビッグデータと捜査機関との情報共有」山本達彦他編『入門・安全と情報』（成文堂、2015）。

[3] 最大判平成 29 年 3 月 15 日刑集 71 巻 3 号 13 頁判タ 1437 号 78 頁。

[4] 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の解説」46 頁。

[5] 個人情報保護委員会「一般データ保護規則の条文（仮日本語訳）」 https://www.ppc.go.jp/enforcement/cooperation/cooperation/GDPR/。

[6] FTC, Protecting Consumer Privacy in an Era of Rapid Change (2012).

[7] 小向太郎「米国 FTC の消費者プライバシーに関する法執行の動向」堀部政男編『情報通信法制の論点分析』商事法務(2015)151-162 頁.

[8] Carpenter v. United States, 585 U.S. (2018).

[9] 稲谷龍彦『刑事手続におけるプライバシー保護』（弘文堂、2017 年）263-269 頁。