Vol.2020-EIP-87 No.10
2020/2/14

犯罪捜査における位置情報の取得とプライバシー

小向太郎[†1]

コンピュータ処理能力の向上とデータ収集可能な情報の増大を背景に，大量のデータがリアルタイムに収集され，蓄積されるようになっている．特に位置情報は，犯罪捜査においても被疑者の特定や追跡などの場面で非常に役に立つ．一方で，こうした情報は本人以外の第三者が保有している場合も多く，本人の知らない間に情報が取得される可能性も高い．本稿では，犯罪捜査機関による位置情報の取得について，我が国における法的位置付けや，欧米における保護の動向を比較し，位置情報に対する捜査のあり方について検討を行う．

Privacy issues in investigation search on location data.

TARO KOMUKAI[†1]

This paper focuses on privacy and data protection for location data that are processed in search for criminal investigations. Location data would be a curse to serious privacy concern because it could be collected, used or disclosed while data subject does not recognize it. The aim of this paper is to compare the relevant discussions about privacy and investigation search on location data in the EU, the U.S. and Japan, and reach a suggestion for appropriate solution.

1. 捜査機関による位置情報の取得

1.1 犯罪捜査と位置情報

多種多様なデータがリアルタイムに収集され，蓄積されるようになっている．こうした情報は犯罪捜査においても被疑者の特定や追跡などの場面で非常に役に立つ．特に位置情報は，対象者の位置情報を活用することで，捜査をさらに精緻かつ有効に行うことができる可能性があり，証拠としての重要性も高い．

現在のところ，利用者の位置情報を最も網羅的に収集し得るのは，携帯電話事業者であろう．携帯電話が電話を受信するためには，携帯電話事業者は自社の契約者の携帯電話端末がどの基地局のエリア内にいるのかを常に把握する必要がある．そうしないと，例えばその端末に電話が掛かってきても，通話を着信させることができない．したがって，携帯電話端末は，電源を切らない限り常に電波を発信して基地局との間で，位置確認をしている．つまり，携帯電話端末の保持者がどの基地局エリアにいるのかという位置情報は，携帯電話事業者が把握可能である．

携帯電話事業者が取得しうる利用者の位置情報には，この「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）」以外にも，実際に「個別の通信を行った基地局の場所」と「GPS 位置情報（ GPS 機能により取得する情報）」がある．

この他にも，IT サービス利用者の所在場所等を確認できる情報としては，写真データにつけられているジオタグ（撮影場所）や，店舗での購入履歴（利用店舗の場所）といったものがある[1].

（図表 1）位置情報の例

種別	利用機器（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	カーナビゲーション・システム，遠隔操作・管理システム	GPS 位置情報，移動履歴
カメラ	監視カメラ，デジタルカメラ	顔認識等による追跡情報，カメラ設置場所，ジオタグ
ID カード等	POS レジ，IC カードリーダ，RFID リーダ，自動改札	購入履歴（利用店舗の場所），通過箇所，交通機関利用経路

†1 日本大学
Nihon University

1.2 プライバシー・個人情報保護

刑事訴訟法 197 条第 1 項は「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」と定めており，強制の処分に当たるものについては，令状等の法定の手続きに従うことが必要になる．

どのような処分が強制の処分になるのかについては見解が分かれているが，①処分をする側の処分手段を基準とする（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を基準とする（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）ものに大別される．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．前者の見解にたてば，捜査機関による位置情報の収集がプライバシーを侵害するのであれば，法定の手続きに基づいて行われなければならない．なお，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」であるという考えを示している[2].

位置情報に関しては，車両に使用者の承諾なく密かに GPS 端末を取り付けて位置情報を把握していたことが，適法な捜査として許容されるかどうかが争われた事例がある．最高裁場所は，このような捜査が，刑訴法上，特別の根拠規定がなければ許容されない強制の処分に当たるとともに，一般的には，現行犯人逮捕等の令状を要しないものとされている処分と同視すべき事情があると認めるのも困難であるから，令状がなければ行うことができない処分と解すべき」という判断を示している．そして，GPS 捜査は，対象車両の使用者の行動を継続的，網羅的に把握することを必然的に伴い，事前の令状呈示が困難であることから，公正担保の手段が仕組みとして確保されている必要があり，これを満たす制度が現行法上存在しないため，GPS 捜査を適法に実施するためには立法的な措置が講じられることが望ましいとしている[3].

なお，事業者等に蓄積された位置情報は，個人データに該当する場合も多い．我が国の個人情報保護法は，個人データ（電子化または体系化された個人情報）の第三者提供には原則として本人の同意が求められるが，捜査機関への情報提供の多くは，第 23 条第 1 項第 1 号の「法令の基づく場合」として本人の同意なく提供が許される．捜査関係事項照会（刑事訴訟法第 197 条第 2 項）への回答は法律による提供義務に基づくものとして正当化されると理解されている[4].

1.3 通信の秘密との関係

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．総務省のガイドラインでは，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」「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」としている[5].

したがって，電気通信事業者が保有する位置情報を捜査機関が取得するためには，令状その他の違法性阻却事由が必要となり，基本的には強制捜査として行われている．

2. 諸外国における議論

2.1 米国

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）という考え方が支持されてきた．

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

の法理が該当せず，合理的なプライバシーの期待が保護されるという最高裁判所の判断が示され，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，令状の発布に高い蓋然性を要求されるのに比べると，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，これは第三者法理そのものを否定するものではなく，携帯電話の位置情報のような，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については，プライバシーの期待を保護すべきであるという立場である．対象となった情報の特殊性が特に強調されている[6].

なお，米国においても，捜査機関による被疑者に対する GPS 装置の装着が問題となった事例がある．令状が認める期間を超えて GPS 装置を装着したことが修正第 4 条に違反するとされており，当該装着は物理的侵入であることが強調されている[7]

2.2 EU 犯罪捜査指令

EU では一般データ保護規則（GDPR）が 2018 年 5 月に施行されている（Regulation （EU) 2016/679)[8]．GDPR が保護の対象とする個人データは，識別子を参照することで自然人を識別できる情報であり，この識別子の例として「位置情報」が明示されている（第 4 条（1))．したがって，位置情報を含む情報は，個人データとして GDPR の保護を受ける．GDPR は，個人データの処理を行うためには何らかの適法化根拠を求めているが（第 6 条)，捜査機関による捜査については基本的に「（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」などにより正当化される．

犯罪捜査目的の個人データの処理に関しては，犯罪捜査指令（DIRECTIVE（EU）2016/68）[9]が定められている．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．犯罪捜査等の目的のためには，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，次のようなことを求めている[8]

- 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
- 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や，情報保有の制限（保存期限の設定や定期的なレビュー）を求めている．

さらに，本人に対しては次のような情報を提供することが求められる．

- データ処理の目的と手段を決定する所管官庁の名前と具体的な連絡先
- データ処理が行われている理由
- 監督当局に苦情を申し立てる権利および当局の具体的な連絡先
- 個人データへのアクセスや，修正・削除を要求する権利があること，個人データの処理を制限する権利があること

2.3 EU 電子証拠規則案

欧州委員会は，2018 年 4 月に「犯罪捜査における電子的な証拠に対する提出及び保全命令に関する規則（案)」を公表している（COM(2018） 225)[10]．この規則は，犯罪捜査において重要性を増している電子的な証拠について，効果的な捜査を行うとともに，基本的な人権の保護を確保するために検討されているものである．この規則案では，上記の目的のために必要であり目的と均衡のとれる範囲で，発行における同等の国内状況において同じ刑事犯罪に対して同様の措置が利用できる場合に，証拠提出命令（the European Production Order: EPO）の発布を認め，EU 全体で統一的な捜査を可能にすることが提案されている．この手続

では，電子的証拠が下記のような 4 つのカテゴリーに分けられている．

（図表 2）電子証拠規則案における情報種別

加入者情報	a）名前，生年月日，住所，請求・支払情報，電話番号，電子メールアドレスなどの加入者や顧客の識別情報．(b) サービスのタイプとその利用期間（技術情報と関連技術や使用インターフェースを示す情報，利用可能なサービスに関する情報を含む)．ただし，利用者が設定したり利用者の要求によって設定されたりするパスワードその他の認証手段は除外される．
アクセス情報	利用者のサービスへのアクセス開始と終了に関連するデータをいう．利用者を識別するためだけに厳格に必要なものであって，利用日時，サービスへのログイン・ログオフ，ISP によって割り当てられる IP アドレス，利用インターフェースを識別するための情報，ユーザ ID などがこれに当たる．この情報には，e プライバシー規則における電気通信メタデータが含まれる．
トランザクション情報	サービスプロバイダーが提供するサービスの提供に関連する情報であって，そのサービスに関する背景や追加情報を提供するために使われるものであって，サービスプロバイダの情報システムによって生成または処理されるものをいう．例えば，情報のソース，メッセージをやり取りするための宛先その他の情報，端末の所在地，日時，時間，サイズ，ルート，フォーマット，利用されているプロトコルや圧縮技術などであり，これらの情報のうちアクセスデータに該当しないものをいう．この情報には，e プライバシー規則における電気通信メタデータが含まれる．
コンテンツ情報	加入者情報，アクセス情報，トランザクション情報以外の，テキスト，音声，ビデオ，画像，音響などの保存されているデジタル情報

「加入者情報」と「アクセス情報」は全ての犯罪について，「トランザクション情報」と「コンテンツ情報」は，3 年以上の拘留の対象となる犯罪か，金融犯罪，性的虐待，サイバー攻撃，テロリズムに関する一定の犯罪に情報システムが関与している場合に限り，欧州提出命令（EPO）の発布ができることになっている．位置情報に関して言うと，通信の必要のためだけに取得される位置情報は「アクセス情報」に，それ以外の位置情報は「トランザクション情報」に該当すると考えられる．

3. 位置情報取得に関する課題

3.1 第三者が保有する情報

現在では，個人に関する情報が，さまざまな企業や団体に保有されている．捜査機関が捜査協力を依頼してきた場合に，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は，その企業や団体にとってあまり重要に感じられない可能性がある．個人情報保護法上も，捜査協力が目的であれば，本人の同意なく個人データの第三者提供が許容されると考えられている．

従来から，任意捜査として広く行われてきた「聞き込み」は，捜査対象者以外の第三者に情報提供を求めるものである．捜査機関に対する市民の自発的な協力は，むしろ望ましいことと考えられてきた．これに対して，捜査機関による盗聴，盗撮，住居への侵入等は問題があると理解されてきた．任意捜査として許容されるかどうかを考える際には，暗黙の了解として物理的侵入の程度が考慮されてきたといってよい[9]．

しかし，データ利用の拡大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．物理的侵入の有無があるもの以外については捜査機関と情報保有者の判断に委ねて，本人が情報を取得された事自体さえ知ることができないとすれば，プライバシーや個人情報保護の観点から問題となりうる[10]．

3.2 対象情報と法的保護

情報保有者が捜査機関への任意協力を求められた場面で，制度的に提供に歯止めをかけるものとしては，通信の秘密の保護や秘密漏示罪などの規定がある．位置情報に関して言えば，日本では，携帯電話事業者に関する位置情報に関しては厳格な配慮が求められているが，他の分野では状況に応じて任意捜査への協力も行われる場合がある．我が国で通信の秘密が厳格に保護される電気通信事業とは「有線，無線その他の電磁的方式により，符号，音響又は影像を送り，伝え，又は受けること」

（電気通信事業法第 2 条第 1 号）であり，これを行うための電気的設備を用いて他人の通信を媒介し，その他電気通信設備を他人の通信の用に供する役務（サービス）を，「他人の需要に応ずるために提供する事業」(4 号）が電気通信事業であると定義されており，一般に次のようなサービスが該当すると考えられている[11].

加入電話，ISDN，中継電話，国際電話，公衆電話，FAX，電報，携帯電話， PHS，移動端末データ通信，データ伝送(フレームリレー・ATM 交換等)，IP 電話， ISP，FTTH・DSL・CATV・FWA・公衆無線 LAN アクセス，インターネット 関連サービス(電子メール，インスタント・メッセンジャー，IX 等)，広域イーサネット， IP-VPN，専用役務，無線呼出し 等

米国では，第三者が保有する情報に対する捜査は任意で行いうることが多いが，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，捜索差押令状や裁判所命令を求める規定がある（the Stored Communications Act: 18 U.S.C. §§2701-2712 (2012)）．そして，前述の通り，特に携帯電話会社が保有する位置情報については，より厳格な要件で発布される捜索差押令状が必要であるという裁判所の判断が示されている．

EU の電子証拠規則案では，サービス・プロバイダ（電気通信事業者，ISP，SNS 等の事業者）が保有する情報を，「加入者情報」「アクセス情報」「トランザクション情報」「コンテンツ情報」に分類し，「トランザクション情報」と「コンテンツ情報」については，より厳格な手続きを定めている．個別の通信の伝送に直接必要とされない位置情報については，「トランザクション情報」になる．

3.3 今後の課題

従来から，電気通信事業者の取扱う情報は，他の分野と比べて特に厳格な保護が求められてきた．通信の秘密に代表されるセンシティブなものが多く，どの国でも特別な規制が課せられていることが多い．しかし，現在，インターネット上で利用者に関する情報を利用しているのは電気通信事業者だけではなく，例えばプラットフォーム事業者を始めとして様々な事業者が，顧客に関する大量の情報を収集・利用している．位置情報についても，現在のところ携帯電話事業者が保有する情報の重要性が高いのは間違いがないが，今後さまざまな形で蓄積や利用が進んでいくことは疑いがない．

そして，本人以外の第三者が保有している情報については，情報の保有者が，本人の人権に配慮することを過度に期待することはできない．こうした情報について，どのような保護を確保すべきかが問題となる．第三者が保有する情報が犯罪捜査の対象となる場合に，過度な情報の利用を抑止するアプローチとしては，①法定の手続きに基づく強制処分として位置づけ令状等の手続きを求める（捜査機関の義務），②特定の情報について守秘義務を課して捜査機関への任意協力を禁止する（情報保有者の義務），といった方法が，考えられてきた．こうした制度の対象の拡大については，当然議論すべきである．

しかし，その前提として，第三者が保有する情報については，本人の知らないうちに情報が利用される可能性があるという問題がある．EU 犯罪捜査指令が重視している透明性の確保と本人に対する情報提供に関する制度は，米国や日本ではほとんど考慮されていない．今後は，本人への一定の情報提供に関する制度の検討が，より重要になると考えられる．

謝辞

本研究は，科学研究費補助金・基盤研究(C)(課題番号: 18K01393)による研究費を得て実施した．

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] 最三小決昭和 51 年 3 月 16 日刑集 30 巻 2 号 187 頁.
[3] 最判平成 29 年 3 月 15 日刑集 71 巻 3 号 13 頁.
[4] 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）.
[5] 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）114-115 頁.
[6] Carpenter v. United States, 138 S. Ct. 2206.
[7] United States v. Jones, 565 U.S. (2012).
[8] 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.
[9] 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
[10] Proposal for a Regulation f the European Parliament and of the Council on European Production and Preservation

Orders for electronic evidence in criminal matters, 17.4.2018, COM(2018) 225 final, 2018/0108(COD).
[8] EU, Protecting personal data when being used by police and criminal justice authorities (from 2018), https://eur-lex.europa.eu.
[9] 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.
[10] 小向太郎「クラウド上のデータを対象とする犯罪捜査に関する法的課題」情報処理学会研究報告電子化知的財産・社会基盤（EIP） 2018-EIP-79，2018-02-16.
[11] 総務省「電気通信事業参入マニアル［追補版］-届出等の要否に関する考え方及び事例-」（平成 17 年 8 月 18 日）.