大学院研究年報　第48号　2019年２月

犯罪捜査のための基地局情報の取得

伊　藤　徳　子*

要　　旨

日常生活において重要な役割を担っている携帯電話は，付近の基地局の電波強度を通した端末の位置を通信事業者に常時知らせている．この基地局に係る位置情報は通信事業者によって収集・保管される．こうした過去の所在を示す基地局情報は，特定の事件が発生した地点及び日時と照らし合わせることで，被疑者の犯罪への関与を裏付ける証拠ともなり得る．他方で，基地局情報は，いつ，誰が，どこに，どの程度の時間所在したかといった事項を把握できるため，考慮しなければならないプライヴァシーの問題は非常に大きい．捜査機関が捜査目的で過去の基地局情報を通信事業者から取得するという捜査手法について，当該問題につき議論が進んでいる米国における運用を参照し，我が国における諸問題を検討する．

目　　次

はじめに

我々が携帯電話を使って電話やメール，インターネットをはじめとする電気通信を利用する際，その都度，最も近くに所在する基地局が使用される．また，携帯電話は，異なる基地局エリアに移動しても通信を継続させ，着受信を効率的に行うために常に基地局と通信し，端末の位置情報を常時通信事業者に知らせている[1)]．これらを基地局に係る位置情報（以下，単に「基地局情報」）と呼ぶ．

通信事業者により収集保管された基地局情報を捜査機関が利用することは，対象となった携帯電話所有者の大まかな居場所を特定することを可能にする．加えて，基地局情報は，どの基地局を使用したかという位置的情報だけでなく，いつ使用したかという時的情報をも含む．そのため対象となる携帯電話が，何時何分にＸ地点にいて，○分後にはＹ地点に移動しているということ，あるいは特定の地点にどのくらいの時間滞在したかを知ることができる[2)]．それゆえ，基地局情報は犯罪捜査において，被疑者の足取りを裏付けるのに有用な証拠となり得る[3)]．

類似のものにGPS位置情報がある．我が国においては最判平成29年３月15日で，少なくとも私的財産への取付を伴うGPS捜査が事実上行えなくなった．そのため，GPS捜査につき法整備がなされ

＊　いとう　のりこ　　法学研究科刑事法専攻博士課程後期課程
2018年10月５日　推薦査読審査終了
第１推薦査読者　安井　哲章
第２推薦査読者　中野目善則

るまで，基地局情報の取得がGPS捜査に代替する有力な捜査手法となり得る．しかしながら，基地局情報の取得は捜査機関内部の自主的な規定の下で行われていることもあってか，基地局情報を巡る議論はあまり盛んでない．基地局情報をどのように理解すべきかが問われている．

本稿はこのような関心から，通信事業者が収集保管している利用者の過去の基地局情報を，捜査機関が犯罪捜査の目的で利用する捜査手法について問題提起を行う．被疑者の発見のためにリアルタイムの基地局情報を利用する所在探索について述べるものではない．第１章では，我が国で基地局情報が犯罪捜査においてどのように取扱われているか紹介する．第２章では米国における基地局情報の取扱いを見る．また，最近出されたCarpenter v. United Statesを分析し，先例との関係を整理する．第３章では，米国における法理論法運用を参考に我が国の法解釈を行う．基地局情報の取得について，憲法や刑訴法上の解釈適用上の問題も検討する．第４章では基地局情報の特質やそれに伴う問題点等をまとめる．

Ⅰ　日本における基地局情報の取扱い

１．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

電気通信事業は通信の秘密と直接かかわる事業であって極めて高い公共性を有しており，プライヴァシー保護を要する情報を取り扱うことも想定される．そのため，そこで取り扱われる個人情報につき保護の必要性が高い．また，電気通信役務の高度化・多様化は，大量かつ高度に処理された情報の迅速かつ広範囲な流通・利用を可能とする高度情報通信社会を実現し，国民生活に大きな利便性をもたらしている反面，電気通信役務の提供に伴い取得される個人情報が不適正な取扱いを受けたり，これらの電気通信役務を利用して個人情報が不適正な取扱いを受けることによる被害は小さくない．このようなことに鑑み，『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』はプライヴァシー保護の観点を踏まえた改正が行われている[4)]．

ガイドライン第35条１項は，電気通信事業者が位置情報を取得できる場合を定める．そして同条２項において位置情報の他人への提供が許される場合を定めており，犯罪捜査のため捜査機関に情報を提供する場合がこれに当たる[5)]．本稿は，通信事業者が正当業務行為として基地局情報を収集しログとして保管していることを前提に，捜査機関が犯罪捜査のために当該情報を取得することの適法性を検討する．

ガイドラインによれば，位置情報が個々の通信に関係する場合には，通信の構成要素であるから通信の秘密として保護される．例えば，ある者が携帯電話でメール送信等のインターネット通信を行った際に記録される基地局情報がこれに当たる．この場合，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[6)]．犯罪捜査の文脈においては，被疑者である通信当事者の同意を得ることは考えられず，通常令状によることになる．なお，この場合の令状の形式についてガイドラインは特段の規定をしていないが，実務では検証令状を用いるのが通例となっている[7)]．

これに対し，個々の通信時以外に端末の所持者がエリアを移動するごとに基地局に送られる位置登録情報は個々の通信を成立させる前提として電気通信事業者に機械的に送られる情報に過ぎないことから，通信の秘密には含まれないプライヴァシーとして保護されるべき事項とする．この場合，利用者の同意がある場合又は電気通信役務の提供に係る正当業務行為その他の違法性阻却事由に該当する場合に限り取得することが強く求められる[8)]．これは，犯罪捜査の文脈においては特段の規制を示していないに等しい．さらに，基地局情報に基づく過去の位置探索は，現行刑事訴訟法上，

強制処分としては規定されておらず，またガイドラインも法律とは異なるため，その法的性質の分析に基づいた規律を欠いている．

Ⅱ　米国における基地局情報の取扱い

1．取得方法

米国では証拠の収集方法にいくつかのバリエーションがある．18 U.S.C. §2703（Stored Communications Act: SCA）は，政府機関による利用者の通信又は記録の開示要求について定めている．同条はまず，電話通信・電気通信の内容情報と，内容情報以外のサービスに関する記録に区別する．前者はさらに，情報の保管主体によって区別される．すなわち，通信事業者が保管主体である場合には，保管開始後180日以内は令状によって，保管開始後180日を超えるものは令状，コートオーダー又はサピーナによる．遠隔情報処理事業者が保管主体である場合には，期間の定めなく令状，コートオーダー又はサピーナによる．令状に基づいて行う場合は利用者への通知は不要である．他方，コートオーダー及びサピーナによる場合は，§2705に従って事後通知をする場合を除き，利用者へ事前に通知しなければならないと規定されている．これに対し，内容情報以外のサービスに関する記録は，保管主体及び保存期間の区別をせず，主に令状又はコートオーダーによることになっている．

§2703(b)又は(c)の下で行われる開示のコートオーダーは，管轄裁判所によって発せられ，政府機関によって，要求される電話・電気通信，記録，その他情報の内容が進行中の犯罪捜査に関連があり，かつ重要であると思料すべき合理的な理由（reasonable grounds）の存在を示す特定かつ明白な事実が示された場合でなければ発せられない．

ここで問題となるのは，基地局情報が§2703の適用を受けるのかということである．基地局情報が通信の内容に該当するかはさておいても，少なくとも「電気通信サービス又は遠隔情報処理サービスに関する記録（§2703(C)(1)）」に文言上該当することは確かである[9]．そのため，本条の適用を受けるとすれば令状の他にコートオーダーによって取得することが許され，処分を行うために必要な疎明の程度に差が生じる．令状においては「相当理由（probable cause）」が要求されるのに対し，コートオーダーにおいては相当理由よりも程度の低い「合理的な理由（reasonable grounds）」で足りるとされているからである[10]．留意すべきなのは本条と第四修正の関係である．つまり，基地局情報の取得が第四修正上の“search”に該当するならば，第四修正の規定により令状が要求され，令状以外の手段によることは原則として許されない．しかし第四修正上の“search”に該当しないならば，第四修正の射程外となり令状は本来不要である．とはいえ，第四修正の枠外だからといって際限なく行えるとすべきでないものもある．SCAは，そのような一定の事項について，令状手続に準じた手続を踏ませ手厚く保護しようという構成になっている．基地局情報は通信事業者の保管に係る情報であるため，文言上は§2703の規定が適用され得るが，実際に適用できるとするためには，まず第四修正上の“search”該当性を否定することが前提となる．このことは，基地局情報が通信の内容に該当すると考える場合でも，保管開始後180日を超えた基地局情報を取得する場合には令状の他にコートオーダーやサピーナによることが許されるため，より一層妥当する．

2．裁判実務における理解

基地局情報の法的性質を巡り，米国では既に複数の裁判例が存在する[11]．Court of Appealsレベルで初めて基地局情報捜査について扱った*In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. To Disclose Records to Gov't*において，基地局情報はSCAの§2703(d)に基づき取得できること，そして同条の要件として求められる証明の程度は令状で要求される相当理由よりも低いという判断が示された[12]．それを

皮切りに，各地の Court of Appeals で同様の判断がなされ，基地局情報は第四修正上の保護を受けないという裁判実務が集積しつつあった．

このような判断が統一的になされていた中で，ごく最近，合衆国最高裁が初めて基地局情報の法的性質について正面から取り上げた．Carpenter v. United States である[13]．事実の概要は次の通りである．警察官は一連の強盗事件の被疑者として 4 人を逮捕した．その内の 1 人の自白によると，4 か月以上前に，犯行グループは他に 9 件の強盗を行っていた．彼は強盗に加担した15人の共犯者を明らかにし，FBI に彼らの携帯電話番号を教えた．FBI は，自白した被疑者が強盗事件の発生した時間帯に通話していた他の電話番号を割り出すために彼の通話記録を調べた．その情報に依拠して，検察官は，被告人 Carpenter 及びその他の被疑者数名の携帯電話の記録を取得すべく，SCA に基づくコートオーダーを請求した．マジストレイトは，被告人 Carpenter の無線通信事業者に対し一連の強盗事件が発生した 4 か月の間に「Carpenter の携帯電話が受電及び架電した始点と終点の基地局エリア情報」を開示するよう指示する 2 つのコートオーダーを発した．第 1 のオーダーは M 社から152日間の基地局記録を求めるもので，同社は127日間の記録を提供した．第 2 のコートオーダーは S 社に 7 日間の基地局情報を要求するもので，同社は被告人の携帯電話がローミングを利用していた期間を含む 2 日間の記録を提供した．総合すると，政府は 1 万2898，平均して一日101もの，被告人の行動を一覧化する（cataloging）所在地点を取得した．被告人は 6 件の強盗，及び 6 件の銃器携行の被疑事実で起訴された．公判に先立ち，被告人は，通信事業者により提供された基地局データについて証拠排除を申し立てたが退けられた．公判において被告人の共犯者 7 人が彼が犯罪実行の主犯であることを認めた．さらに，FBI 捜査官は基地局データについて専門家証言（expert testimony）を述べた．曰く，携帯電話が無線ネットワークを利用している間，通信事業者は，基地局及び利用された特定のセクターについて日時の記録されたログを取っている．この情報に基づき FBI 捜査官は，4 件の起訴された強盗事件が発生した場所の付近に被告人の携帯電話が所在していたことを示した地図を証拠として提出した．被告人は全ての訴因について有罪判決を受けた．

第 6 巡回区 Court of Appeals は，収集された位置情報について被告人はプライヴァシーの合理的期待を欠くと判示して原判決を認容した．その判断を導くに当たり，被告人が自己の位置情報を通信事業者と共有したということが理由となっている．すなわち，携帯電話利用者は「通信を確立する手段」として携帯電話通信事業者に基地局データを任意に伝達していることを踏まえ，その結果として作成される業務記録は第四修正上の保護を受けられないと結論付けた．

これに対し合衆国最高裁は以下のことを判示した．第 1 に，第四修正の目的に照らし，基地局情報を通じて捕捉されるような移動記録について，人はプライヴァシーの正当な期待を有する．第 2 に，Stored Communications Act（SCA）に基づき発せられたコートオーダーに従って被告人の携帯電話の通信事業者から取得された過去 7 日間の基地局情報は，“search”によって得られたものである．第 3 に，政府が過去127日間の基地局情報にアクセスしたことは，被告人の有するプライヴァシーの合理的期待を侵害する．第 4 に，政府が携帯電話の通信事業者から基地局情報を取得しようとする場合には原則として，事前に相当理由に支えられた“search”令状の発付を受けなければならない．

Roberts 首席裁判官執筆の法廷意見は，基地局情報の取得が“search”に当たるかどうかの判断の前提として，基地局情報に「第三者法理」の発想が及ぶか否かを検討しているため，第三者法理について概観する．

(1) 第三者法理

合衆国最高裁は長きに渡り，危険負担（assumption of risk）という分析を用いて，ある者が保護された利益を有しているという主張を退けてきた．これとよく関係する法理が第三者法理である．すなわち，第三者に対して任意に，物，情報又は空間を提供する者は，その行為によって相手方である第三者が，警察官に情報を開示し又は物を提出しあるいは捜索又は差押えを許すかもしれない危険を想定し負担しているため，第四修正上の保護が失われるとする[14]．第三者法理は United States v. Miller において明確にされ，Smith v. Maryland において確立されたと理解されている．

(a) United States v. Miller

1972年12月18日，情報提供者の内報を受けて，ジョージア州ハウストン郡からの保安官代理（deputy sheriff）が被告人の共謀者とされている者２人の乗るトラックを停止させた．そのトラックには蒸留装置や原料が積まれていた．1973年１月９日，ジョージア州カスリーンで被告人の借用する倉庫から出火した際，消防士と保安係官（sheriff department officials）が違法な蒸留設備，ウィスキー及び関連器具を発見した．２週間後，米国財務省アルコール・タバコ・火器局（Treasury Department's Alcohol, Tobacco and Firearms Bureau）の係官は，被告人が口座を有する銀行２社の頭取に対してサピーナを呈示した．当該サピーナは，両銀行の頭取に対し，「預金額，小切手，貸付金等，被告人名義の口座に関する全ての記録」の提出を求めるものであった．銀行側は従業員に，入手可能な記録の作成と，係官が望んだ文書の写しの提供を命じた．A銀行において係官は，関連する口座のマイクロフィルム記録を閲覧し，預金伝票１枚及び小切手１，２枚の写しの提供を受けた．B銀行においては，さらにマイクロフィルムの記録を閲覧し，被告人の口座記録の写しを入手した．これらの中には，一切の小切手，預金伝票，２枚の資産報告書，３枚の月次報告書が含まれていた．被告人は，銀行が保持する記録は，銀行が限られた目的のために利用できる個人に関する記録の写しに過ぎず，そこにはプライヴァシーの合理的期待があるということを理由に，これらの記録について第四修正上の利益を有すると主張した．そこで，当該記録の法的性質が問題となった．

Miller において合衆国最高裁は次のように述べた．「銀行預金者は，個人に関する事項を他人に教える際，相手方がその情報を政府にリークし得る危険を負う[15]．第四修正は，第三者に提供され，提供された者によって政府にリークされた情報の入手を禁じてはいないと当裁判所は繰り返し判示してきた．たとえ，限られた目的のためにのみ使用され，相手方たる第三者が裏切らないという信頼を前提として情報が提供された場合であっても，この理は変わらない[16]．」このような理解に基づいて第四修正上の権利の侵害はないと判示した．

(b) Smith v. Maryland

強盗事件の被害者が警察官に，犯人の特徴及び犯行現場付近で目撃した車両について供述した．その事件以降，被害者の自宅に，強盗犯を自称する者から脅迫的な電話がかかってくるようになった．別日に被害者宅付近において被害者の供述に一致する男が，犯行現場で目撃された車両を運転しているのを警察官が発見し，当該車両のナンバーを調べたところ，被告人名義で登録されたものであることが判明した．

電話会社は警察官の要求に基づき，被告人の自宅から架電された電話番号を記録するために事務所にペン・レジスタを設置した．この際，警察官は，令状もコートオーダーも得ていない．ペン・レジスタの設置により，被告人宅から被害者宅に架電された事実が判明した．当該事実及びその他の証拠に基づき，被告人宅を捜索すべき場所とする捜索令状が発付され，令状執行の結果，種々の証拠が押収された．

強盗の被疑事実で起訴された被告人は公判に先立ち，ペン・レジスタを設置する前に令状が発付

されていないことを理由に，ペン・レジスタによって得られた証拠全てについて排除申立てを行った．公判裁判所は被告人の証拠排除申立てを退け，無令状でのペン・レジスタの設置は合衆国憲法第四修正に違反しないと判示し，被告人に有罪判決を下した．連邦控訴裁判所も原判決を支持した．

これに対し合衆国最高裁は次のように判示した．「一定の形態をとる，政府主導の電子的監視が第四修正上の“search”に当たるかどうかを検討するにあたり，Katz v. United States が指標となる．政府の行為によって何らかのプライヴァシーが侵害され得るが，第四修正の適否は，その侵害されたプライヴァシーについての期待が『もっとも（justifiable）』，『合理的（reasonable）』あるいは『正当（legitimate）』であるかどうかによって決まる．この問いには，*Katz* の補足意見で Harlan 裁判官が適切に述べたように，本来，２つの別個の観点が含まれている．第一に，対象者が行動により，プライヴァシーの現実の（主観的な）期待を表示していたかどうか．すなわち，*Katz* の多数意見の言葉を借りて言えば，その者が，内密に保とうと努めていることが示されていたかどうかである．第二は，そのプライヴァシーの主観的な期待は，社会が合理的だと認める期待かどうか．すなわち *Katz* の多数意見の言葉を借りて言えば，客観的に見て，その者の主観的な期待が個別の事案の状況下で正当化されるかどうかである．本件で問題となっている捜査機関の行為は，ペン・レジスタの設置及び使用である．被告人は，政府が被告人の有するプライヴァシーの正当な期待を侵害したという主張をしている．しかし，*Katz* で用いられた聴取機器は会話の内容を取得するものであったのに対し，ペン・レジスタは，架電された電話番号がわかるだけで，会話の内容はおろか実際に電話が繋がったかどうかさえ知ることができない．ペン・レジスタにはこのような限定的な機能しかないことを踏まえると，ペン・レジスタの設置及び使用が“search”に当たるという被告人の主張は，彼が自分の電話から架電した番号について，プライヴァシーの正当な期待を有していたかどうかにかかっているが，何人も，架電した番号について，何らかのプライヴァシーの現実的な期待を有しているとは思われない．また，たとえ被告人が，架電した電話番号が内密に保たれるだろうという主観的期待を有していたとしても，この期待は『社会が合理的だと認める期待』ではない．当裁判所は，第三者に対し任意に情報を提供した場合，その者は提供した情報について，プライヴァシーの正当な期待を有しないと一貫して判断してきた[17]．内密な情報を任意に第三者に教える者は，その相手方が教えられた情報を政府に伝えるかもしれない危険を負う．第四修正は，第三者に晒され，その第三者により政府官憲に伝えられた情報を入手することは禁じていない．たとえ，限定された目的にしか使用されないという考えに基づいて，また，情報を渡す相手方たる第三者が裏切らないだろうという信頼に基づいて，情報が提供されたのだとしても．この理論から，本件被告人はプライヴァシーの正当な期待を主張することができない．」このような理解に基づいて，ペン・レジスタの設置及び使用は“search”に当たらず，令状は不要であると判示された．

（2） *Carpenter* の分析

Carpenter において Roberts 首席裁判官執筆の法廷意見は，基地局情報の取得が“search”に当たるかどうかの判断の前提として，基地局情報に「第三者法理」の発想が及ぶか否かを検討しているが，その分析は２つのテーマで構成されている．第１に取得される情報の質について，第２に任意の提供（voluntary exposure）という行為についてである．

まず第１のテーマについて見る．*Smith* は，第三者法理を確立した判例だと理解されるが，*Smith* の判示から読み取ることのできる第三者法理の正当化根拠の１つは，取得される情報が限定されているということである．*Smith* は *Katz* と同様に「電

話」に関する事案であったところ，ペン・レジスタを使用する捜査手法について *Katz* をそのまま適用することを否定した．*Katz* において用いられた機器は通話の一方当事者の音声を聴き取るものであり，一方話者の音声から会話の内容を網羅的に捕捉することが可能であるが，*Smith* で用いられたペン・レジスタは架電された電話番号を記録するものであり，ペン・レジスタによっては会話の内容はおろか実際に架電が果たされたかどうかさえ知ることができない．*Smith* が *Katz* において定式化されたプライヴァシーの期待を否定したのは，ペン・レジスタがこのような「限定された機能」しか持っていないことを理由としている[18]．機能は取得され得る情報に直結する．*Katz* と *Smith* とでは取得可能な情報の質及び量に大きな違いがあり，ペン・レジスタによって取得できる情報は限られた種類のものであるということが *Smith* の判断の要とも言える．*Smith* はペン・レジスタによって把握される情報が「限られている」ことに依拠した上で，*Miller* で示された第三者法理を確認したものである．そのため，第三者法理の正当化根拠の一部は，取得される情報が限られていることに求められる．言い換えれば，把握される情報が限られていなければ，第三者に対する任意の提供という行為があってもプライヴァシーの問題が生じ得る．

では，基地局情報によって取得され得る情報はどうか．基地局情報の取得によって，携帯電話の電波が通信した記録を通して人の過去の移動状況を把握し得る．この事象がプライヴァシーとの関係でどのように位置付けられるかを分析するために，*Carpenter* の法廷意見は United States v. Jones を参照している[19]．*Jones* は，被疑者使用車両に秘かに GPS 端末を取り付け，その移動を把握する捜査手法が第四修正上の“search”に当たるとされた事案である[20]．*Jones* において Scalia 裁判官執筆の法廷意見は，車両という私的財産に端末を取り付けるという行為に着目し，端的にトレスパス法理に基づいて“search”と構成したが，Alito 裁判官と Sotomayor 裁判官の各補足意見は，GPS 捜査によって侵害されるプライヴァシーの期待という観点からの分析を試みている．*Jones* の法廷意見も，トレスパスなく，電子信号を発信するだけという事案においてはプライヴァシー・テストに依拠することを認めているが[21]，少なくとも従来のトレスパス法理によって判断できる事案であったためプライヴァシーとの関係では主として補足意見が参照される．

Carpenter の法廷意見は，携帯電話の位置情報について，GPS による車両の追跡と同様に詳細（detailed）かつ網羅的（encyclopedic）であると性質付け，人の過去の移動状況が把握され得る基地局情報の取得は，その大部分において，*Jones* で検討された GPS による監視と質的に共通する旨述べる[22]．このような理解を前提とすれば，基地局記録は，人の移動についての詳細かつ包括的な記録であって，「限られた情報」の取得である *Smith* とは質的に異なる[23]．第三者法理にはその客観的側面として情報の質による適用の限界があり，基地局情報の取得は第三者法理の適用範囲の外に位置する捜査手法であると整理される．

次に第 2 のテーマについて見る．United States v. Miller では電話会社に伝達された架電番号記録についてプライヴァシーの期待が否定された[24]．そこでは，被告人が銀行という第三者に対し，自己に関する情報を「任意に提供」したことが根拠とされ，第三者に任意に提供した情報については第四修正上の保護が及ばないとする第三者法理が示された．また，Smith v. Maryland も *Miller* を確認しつつ，同時に第 1 のテーマのところで述べたように，取得される情報による第三者法理の適用の限定を示唆した．第三者法理は，捜査官ないし協力者がその身分を秘して被疑者に接近し，情報を聞き出す捜査手法（シークレット・エージェント法理）に由来する[25]．その背後には危険負担の発想が支えとして存在する[26]．すなわち，第三者

に任意に情報を提供する者は，相手方によってその情報が捜査機関にリークされ得る危険を負担していると考えられる．任意に提供するという行為は，個人に関する情報を内密に保っておこうとする意思（プライヴァシーの期待）が減少していることを体現する行為として位置付けられる．

Carpenter の法廷意見は，基地局情報の場合，利用者には第三者法理を適用する前提としての危険の負担を欠くと考えている．法廷意見も指摘するように，携帯電話の電源さえ入れていれば基地局情報は自動的に収集され，利用者による何らかの積極的な行為は不要であることから，位置情報についてプライヴァシーの期待が減少していることを示す何らかの行為がない[27]．そして，仮に，携帯電話の契約又は使用自体が，プライヴァシーの期待の減少を示す行為であると捉えても，携帯電話は現代社会において生活する上で必要不可欠な存在であって，位置情報を収集させないためにネットワーク接続を切っておくという方法も現実的ではなく，結果として基地局情報の収集を許す以外の選択肢がないため，「任意に」提供されているとも言い難いのである[28]．

適法な逮捕に伴う捜索により発見された携帯電話について，その内部のデータまで無令状で調べることが許されるかという問題を扱った Riley v. California[29] は，「プライヴァシーの期待が縮減しているという事実は，第四修正の射程から完全に外れるということを意味するものではない」と述べている[30]．*Riley* は逮捕に伴う無令状捜索の事案ではあるが，この部分の説示は，プライヴァシーが縮減する一局面として逮捕を例にとったものである．*Carpenter* の法廷意見が *Riley* の上記説示を引用した上で，第三者法理の正当化根拠について，プライヴァシーが縮減していることにも基づくと述べていることは，本件法廷意見は「プライヴァシーに関する問題が十分に深刻である場合には，プライヴァシーの期待が縮減していてもなお令状を必要とする」ことが本件においても妥当することを示唆するものである[31]．そうすると，携帯電話の基地局に係る位置情報について，プライヴァシーの期待が縮減していることを前提としても，なおプライヴァシーの問題が深刻であれば第四修正によって保護される．では基地局情報の取得に関わるプライヴァシーの問題はいかほどであるか．この点，第 1 のテーマに関連して述べた通り，基地局情報によって把握される位置情報は詳細かつ網羅的であって GPS による追跡と同様である．しかし，法廷意見の分析はそれだけにとどまらず，以下のように述べる．「携帯電話の基地局記録には，*Jones* で検討した GPS による車両の監視よりも大きなプライヴァシーの問題がある．車と異なり携帯電話は，所有者の移動をほぼ正確に追跡する．車両を使わない日はあっても，携帯電話は常に所持している．携帯電話は，その所有者と共に，公道だけでなく，個人の邸宅，医院，政党本部，その他の場所について行く．」法廷意見は，このような携帯電話特有の性質に照らし，「携帯電話の所在を追跡する場合，まるで携帯電話利用者の足首に監視装置を装着するように，限りなく完全に近い監視が行われる」ことを指摘した[32]．

このような理解を踏まえると，基地局情報の取得に関わるプライヴァシーの問題は著しいものである．*Carpenter* の法廷意見が「*Smith* や *Miller* で問題となったような限られた種類の個人情報と，通信事業者によって普段から収集されている位置情報の『年代記』とも言える膨大な記録とでは，雲泥の差がある」と述べるほど，基地局情報に関するプライヴァシーの問題は深刻なのである．そうすると，携帯電話利用者は携帯電話の契約又は利用という行為によって，基地局を通じて把握される位置情報についてのプライヴァシーの期待が縮減しているとしても，なおプライヴァシーの問題は深刻である．したがって，そのような基地局情報は第四修正による保護が及び，これを取得するためには令状の発付を受けなければならないと結論付けられるのである．

Ⅲ　日本法への示唆

1．強制処分該当性

⑴　判断枠組み

こうした米国での法運用を踏まえて，我が国における憲法，刑訴法の法解釈という観点から基地局情報の取扱いを捉え直してみたい．刑事訴訟法197条２項は「捜査については，公務所又は公私の団体に照会して必要な事項の報告を求めることができる」と規定している．基地局情報は，同条に基づく任意処分である開示要求の中で取得することが許されるか．我が国の法律上，捜査機関が通信事業者から基地局情報を取得することはどのような法的性質を持つか．

平成29年３月15日判決は，捜査機関が無令状で被疑者使用車両にGPS装置を取り付け，その動静を監視した捜査手法につき強制処分に当たる旨判示したが，そこでは昭和51年決定に沿って強制処分該当性の判断が行われている．すなわち，我が国の最高裁は，問題となっている捜査手法が，「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」か否かを強制処分該当性の基準にしている[33]．そうすると，基地局情報の取得という捜査手法の法的性質を検討する上でも同様の観点からの分析が必要となる．

⑵　処分の対象者

強制処分該当性を検討するに当たり，処分の対象者を明らかにする必要がある．捜査機関が通信事業者に記録を開示させるという点を捉えて，通信事業者を対象とした処分だと理解するならば，通信事業者は通信の秘密と直接かかわる事業であることから，業務上知り得た利用者個人に関する情報を外部へ提供することには否定的であると思われ，個人の意思を制圧する処分だと構成することになる．しかし，処分の対象者を通信事業者と構成すると，処分による被侵害利益がはっきりしない．むしろ基地局情報捜査によって暴かれるのは，捜査機関がまさに求めている，捜査対象となっている携帯電話利用者の位置情報であることに鑑み，実質的には携帯電話利用者を対象とする処分として構成すべきであろう．

⑶　基地局情報の特徴

通信事業者の収集・保管に係る基地局情報は，携帯電話利用者の過去の時々刻々の位置情報であり，捜査のためこの情報を取得する捜査手法は，利用者の過去の時々刻々の所在を検索し，把握すべく行われるものである．その性質上，公道上におけるものだけでなく，個人のプライヴァシーが強く保護されるべき場所や空間に関わるものも含めて，対象となっている携帯電話端末ひいては利用者本人の所在と移動状況を網羅的に把握することが可能である．基地局情報は「特定の携帯電話が単なる過去の一時点として特定の基地局と通信した」ことを示すに過ぎないものではなく，通信を経由して，誰が，いつ，どこに所在していて，どのような移動をしたかを示す行動を網羅する記録となり得る．このような情報はプライヴァシーの中でも特に保護の必要性が高く重要な権利利益である．

公道上の移動については，「通常，人が他人から容ぼう等を観察されること自体は受忍せざるを得ない場所におけるもの」として正当な理由による撮影等が許容される．これは，公道上を移動するという行為が，公の目から逃れようという期待（プライヴァシー）の縮減を反映していることに加えて，正当な理由による捜査機関の利益が増大していることから正当化されると理解できる[34]．しかし，これを基地局情報について見ると，プライヴァシーの縮減を示す事情を見出すことができない．対象者は携帯電話の電源を入れているだけであって，この行為の性質は公道上においても住居内においても変わらない．したがって，携帯電話の基地局情報を通じて対象者の過去の所在及び移動状況を把握することにつき，公道上の所在及び移動

状況なのか否かということは一切意味を持たない．それゆえ，基地局情報を通じて把握される所在及び移動状況は，それについてのプライヴァシーの期待が縮減しておらず，公道上のものか否かに拘わらず総じて，憲法35条の保障する住居，書類及び所持品に準ずる重要な権利利益である．そして，このような情報について通信事業者から取得する捜査手法は，公権力による私的領域への侵入を伴うものと言える．

既に述べたように，対象者は携帯電話の電源を入れておくだけで基地局に係る位置情報が収集・保管されているため，当該基地局情報が捜査機関に取得されていることについての認識がない．人は通常，誰が，いつ，どこに所在していて，どのような移動をしたかを示す行動を網羅する記録が捜査機関に取得されることに対して強い拒否感を持っており，捜査機関による基地局情報の取得が合理的に推認される個人の意思に反することは明らかである．合理的に推認される個人の意思に反することも昭和51年決定にいう意思の制圧に当たることが平成29年判決で明確にされているため，捜査機関が通信事業者から基地局情報を取得する捜査手法は，個人の意思を制圧し，重要な権利利益に制約を加える手段であり強制処分に当たる[35]．

2．憲法21条2項との関係

基地局情報は憲法21条2項により保障される通信の秘密との関係が問題となる点でGPS捜査とは性質が異なる[36]．我が国では，通信の内容は通信の秘密として保護される[37]．現行のガイドラインの下では，通信の秘密として保護される位置情報と，通信の秘密には含まれないプライヴァシーとして保護されるべき位置情報とでは，通信事業者が捜査機関に提供するのに令状を要するか否かという点で，保護の程度にも取得の手続にも違いがあることは既に述べた通りである．しかしながら，この区別による手続的差異が適切であるかどうかは甚だ疑問である．ガイドラインの解説において認められているように，通信の内容に該当しない事項であっても，ある人がどこに所在するかということはプライヴァシーの中でも特に保護の必要性が高い．そして，基地局に係る位置情報は通信とも密接に関係する事項であるから，強く保護しなければならない．他方，個々の通信時に収集される基地局情報と，個々の通信時以外に自動的に収集される基地局情報では，当事者が通信の認識を有しているか否かの違いに過ぎず，手続や保護の程度に違いを及ぼすほどの実質的な差異はない．通信の秘密に含まれないプライヴァシーとして保護されるべき基地局情報も，個々の通信を成立させる前提として収集されるのであれば，憲法上保障された個々の通信と密接に関連するものであり，少なくとも通信の秘密に準ずる権利利益として取り扱うべきである[38]．したがって，基地局情報捜査は，通信の秘密ないし通信の秘密に準ずる権利利益の侵害を伴う捜査手法と言える．

憲法35条は条文上，令状による権利制約のある場合を想定しているのに対し，通信の秘密を保障する憲法21条2項には権利制約を想定した文言がない．しかし，通信の秘密も絶対無制約の権利ではなく，憲法12条及び13条が規定するように公共の福祉という観点から一定の制約を課すことが許される．では，憲法21条2項により保護される通信の秘密にも，憲法35条の令状要件が及ぶのか．憲法21条2項の手続的保障の問題として，憲法21条2項と35条の関係が問われることになる．

憲法13条は広くプライヴァシーという権利利益を保障しているが，そこに含有されるプライヴァシーの中でも保護すべき程度は様々である．そこで，特に強い保護を与えるべき一定の類型を抽出し別途明文で規定したものが，憲法21条や33条，35条等であると理解できる．憲法21条2項の規定がプライヴァシー権を実体的に保障するものであるのに対し，憲法35条は憲法31条に基づく適正手続の保障をさらに特化させたものとして令状主義という手続的保障を求める[39]．憲法35条は「住居，

書類及び所持品」と列挙しているように，有体物を念頭に置いた立法がなされている．しかし今や，有体物でない通信も憲法35条の令状要件の規律を受けていることから，有体物でなくても，憲法35条の列挙する住居，書類及び所持品に準ずる重要な権利利益については同条の令状要件の規律が及ぶと理解して良い[40]．そもそも，憲法が制定された当時，憲法35条と憲法21条は相互に補完し合う権利であったと理解できる．つまり，憲法35条が「住居，書類及び所持品」という個人の私生活の物理的な側面を保障し，憲法21条２項が手紙や電話等通信の秘密という個人の私生活の非物理的な側面を保障する構造になっていたと考えられる．そうであれば，テクノロジーの発達による社会の変化に伴い，プライヴァシーとの関係でこれらの規定が理解されるようになった現代においては，憲法21条２項の保障する通信の秘密は憲法35条の解釈に包摂され，令状要件の規律が及ぶことになる．

３．令状主義との関係

基地局情報捜査が強制処分に該当するとの前提の下，通信の秘密又は通信の秘密に準ずる権利利益の制約について令状要件の規律が及ぶと理解すると，これを行うためには令状を取得しなければならないが，どの種の令状を取得する必要があるのか．これは換言すれば，基地局情報の取得が「いかなる類型の」強制処分に該当するかという問題であり，処分の性質に基づいた分析が求められる．我が国において捜査機関による基地局情報の「取得」について考える際，捜査対象者に関する一定期間のログを通信事業者内のコンピュータに表示させて，これを捜査機関が直接確認する方法と，文書又は他の記録媒体に複写した形式で通信事業者から取得する方法とが考えられる．米国において“search”の文脈で検討されるものでも，我が国においては捜索と検証とで異なる令状形式が要求されているため，取得がどのような態様で行われるかは令状主義との関係で重要である．

(1) 検 証 令 状

第１に，検証令状に基づくことが考えられる．これは，通信事業者のシステム端末を操作し，情報を表示させた画面を視認することにより，過去の一定期間に対象の携帯電話から発信された電波を受信した基地局の位置や基地局からの方角，距離等のデータから，被疑者が使用する携帯電話の位置情報を，五官の作用により認識する点で検証に当たると理解する[41]．平成29年判決においてGPS捜査が検証では捉えきれない性質を有するとされたのはGPS捜査に伴う端末の「取付」という行為が検証の枠から出るためであったと理解すれば，取付行為を伴わない基地局情報捜査は検証として捉える余地が残されている．

また，リアルタイムで追跡できるGPS捜査は，「GPS端末を取り付けた対象車両の所在の検索を通じて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うものであって，GPS端末を取り付けるべき車両及び罪名を特定しただけでは被疑事実と関係のない使用者の行動の過剰な把握を抑制することができず，裁判官による令状請求の審査を要することとされている趣旨を満たすことができないおそれがある」ことが，令状発付の可能性との関係で指摘されていた[42]．しかし，通信事業者から過去の基地局情報を取得する捜査は，捜査中の被疑事実に関連して被疑者の所在を確認したい日時を特定することで，限定的に基地局情報を取得することができ，個人の行動の過剰な把握をある程度抑制することは可能であると考えられる．

さらに，平成29年判決では事前の令状呈示と同程度に手続の公正を担保する手段がGPS捜査においては仕組みとして確保されていないことが指摘されていた．しかし，通信事業者からの基地局情報の取得という捜査手法においては，通信事業者に対して令状を事前呈示することが可能であり，個人の位置情報について過剰な把握を抑制するために通信事業者に立ち合いを求めることも可能で

ある．そうすると，適正手続の保障という観点からも許容し得るように思われる．

しかしながら，捜査機関が基地局情報記録を通信事業者内のシステム装置で直接確認する捜査手法を検証として理解することにはいくつかの問題点が残されている．検証とは，「直接自己の感覚作用により場所や人，物についてその存在及び状態などを強制的に認識し，証拠資料を得ること[43]」，「物の占有を取得できないとき又は裁判のときまでこれを保持しておくことができないとき，その物を見てその状態を記録・保全する手続[44]」とも説明されるように，検証という処分の実質は，場所・物・人の存在，位置，性質等について「直接」感知することにある．判例では，エックス線による撮影や通信傍受が検証に当たるとされたが，これらは装置の利用が目や耳に直接代替するものであると理解できる．すなわち，エックス線装置を利用することで，写された影を直接「見る」，傍受装置を利用することで，電話回線での会話内容を直接「聴取する」ことができるのである．このような理解に基づくと，基地局情報の確認により対象者の所在を直接感知できるか．基地局情報は，①いつ，②どの基地局の，③どの向きのアンテナが，④どの携帯電話番号（又はID番号であるISMIやESN）の，⑤どんな通信種類（通話か電子メールか等）を中継したか，など」のログである[45]．そのような過去のログを確認しても，対象者の所在や移動状況等を直接感知できるものではない．したがってこのような捜査手法を検証として位置付けることは困難であると結論付けざるを得ない．

また，基地局情報の取得を検証と位置付けると，処分の対象者は当該情報を収集・保管する通信事業者になり，令状は通信事業者に対し呈示される．しかし既に述べた通り，位置情報の把握によって実質的に侵害されるのは，被疑者のプライヴァシー，すなわち憲法21条２項に保障される権利及び憲法35条により保障される権利である．通信傍受について扱った最高裁判例において反対意見を述べた元原利文裁判官は，通信傍受が「情報の押収という側面を有する」から，「違法な傍受が行われたときは，処分対象者に対し原状回復のための不服申立ての途が保障されていなければならない」が，「検証については，『押収に関する裁判又は処分』として準抗告の対象とすること（同法429条１項，430条１項，２項）も認められていない」ことを指摘する[46]．通信傍受及び基地局情報の取得を「情報の押収」と理解するかは別として，基地局情報の取得を検証として位置付けることは，不服申立ての余地がない点で適正手続きの保障が十分でないため許容し得ない．

また，捜査機関が基地局情報記録を通信事業者内のコンピュータに表示させて直接確認するという方法をとる場合ではなく，基地局情報記録を文書等の形式で通信事業者から物理的に取得する場合も検証として理解することができない．なぜなら，通信事業者が通常の業務として利用者の基地局情報を取得した時点では，捜査機関による「強制処分」は行われていない．それどころか，「捜査」さえ行われていない．そうすると，捜査機関が基地局に関する情報を「通信事業者から文書の形式で取得する行為」だけが問題となるところ，いわば「提出」に近い態様であるこの行為を，五官の作用を通じて場所・物・人の存在，位置，性質等を把握する処分である検証に位置付けることは困難だからである．したがって，捜査機関が通信事業者の保管に係る基地局情報を取得する捜査手法は，検証令状によって行うことができない．

⑵　捜索差押え令状

第２に捜索差押え令状に基づくことが考えられる．これは，捜査機関が基地局に関する情報を「通信事業者から文書等の形式で取得する行為」をカバーするものである．すなわち，通信事業者の保管に係る捜査に必要な基地局情報を用紙等に印刷し，この占有を強制的に取得する点を差押えとして理解する．そして，差押えの前提として，取得したい被疑事実と関連する基地局情報を通信事業

者のコンピュータにつき探索する点で，差し押さえるべき物を一定の場所につき探索する処分である捜索として理解する．

ところで，電子計算機や，かつて主流であったフロッピーディスクなど有体物たる記録媒体の中に，被疑事実と関連性を有する情報が蔵置されている蓋然性が認められる場合には，証拠物として記録媒体（電磁的記録物）自体を差し押さえることが従来可能である．しかし，多くの場合，証拠として意味を持つのは，無形の電子情報・電磁的記録であり，それが納められている記録媒体それ自体ではない[47]．また，コンピュータ・ネットワークが高度に発展し，クラウドコンピューティングなど，遠隔のコンピュータの記録媒体に電磁的記録を保管し，あるいは必要の都度これをダウンロードするなどといった利用がかなり一般化していることから，従来の，有体物としての記録媒体そのものを差し押さえるという方法だけでは捜査の目的を十分に達成できないおそれが生じている[48]．そこで，情報化社会の進展に適切に対応するため，刑訴法218条２項は「差し押さえるべき物が電子計算機であるときは，当該電子計算機に電気通信回線で接続している記録媒体であって，当該電子計算機で作成若しくは変更をした電磁的記録又は当該電子計算機で変更若しくは消去をすることができることとされている電磁的記録を保管するために使用されていると認めるに足りる状況にあるものから，その電磁的記録を当該電子計算機又は他の記録媒体に複写した上，当該電子計算機又は当該他の記録媒体を差し押さえることができる」と規定した．この規定により，従来の記録媒体自体の差押えに加えて，差し押さえるべき物がコンピュータである場合に，当該コンピュータで作成・変更（又は変更・消去できる）電磁的記録を保管するために使用されていると認められるものから，当該コンピュータを操作して，必要な電磁的記録をそのコンピュータ又は他の記録媒体に複写した上で，当該コンピュータ又は当該他の記録媒体を差し押さえることが認められた．例えば，コンピュータで処理すべきファイルを保管するために使用されているリモート・ストレージ・サービスの記録媒体等が想定される[49]．通信事業者の収集・保管に係る基地局情報は膨大であるため，その保管のためには，通信事業者のコンピュータに接続されたサーバーやストレージ・サービスが利用されていると考えられる．したがって通信事業者のコンピュータを差し押さえるべき物とする場合，基地局情報が当該コンピュータに接続されたサーバーやストレージ・サービス内に保管されていれば，法218条２項に基づき，当該コンピュータを操作して，必要な基地局情報をCDロムやUSB，用紙等他の記録媒体に複写又は印刷した上で，当該他の記録媒体を差し押さえることで基地局情報の取得が可能であると解する．

この場合に219条２項は「（差押え）令状に，差し押さえるべき電子計算機に電気通信回線で接続している記録媒体であって，その電磁的記録を複写すべきものの範囲を記載しなければならない」と規定している．差押えの対象を特定・明示すべきであるという令状主義の要請を満たすのがこの規定の趣旨であるため，令状を執行する捜査機関が対象物該当性を判断でき（捜査機関による恣意的判断を防止し得），被処分者が受忍範囲を判断できる程度に，具体的に記載しなければならない[50]．通信事業者のコンピュータに接続されたサーバーやストレージ・サービスには，被疑者以外の，犯罪とは無関係な者の基地局情報も当然に記録されているため「基地局情報」といった形式を記載しても，令状主義の要請を満たすことができない．また，取得しようとする基地局情報が被疑事実との関係でどのような内容を証明する証拠となるのか，換言すれば証拠として差し押さえる必要性の問題として，被疑者についての基地局情報の中でも，被疑事実とは無関係なものも多くある．例えば，基地局情報により証明しようとする事実が「同一グループによる犯行と思われる一連の事件の発

生時に被疑者が現場付近に所在していたこと」という場合に，事件の発生していない日時の位置情報や，事件現場から遠く離れた基地局の情報は被疑事実との関連性を有しない．そのため「被疑者の所有に係る携帯電話の基地局情報」といった記載でも令状主義の要請を満たすことができない．コンピュータに接続されたサーバーやストレージ・サービス内に保管されている基地局情報の中でも，被疑事実と関連性を有すると思料される時間的場所的範囲をできる限り特定して記載する必要がある．

基地局情報は無形の電磁的記録であり，通信事業者のコンピュータがその記録媒体に当たる．差し押さえられる記録媒体が大型のコンピュータである場合などは，差押えによって業務に著しい支障をきたし得るほか，事件と無関係な第三者の情報が含まれていたりするため，コンピュータ自体を差し押さえなくとも，その中の電磁的記録を取得することで証拠収集の目的を達することができるのであれば，そのような取得を可能にすることが合理的である[51]．そこで，コンピュータ自体の差押えに代替する執行方法として，捜査機関は自ら，又は通信事業者をして，差し押さえるべき基地局情報をCDロムやUSB等の他の記録媒体に複写，又は用紙に印刷することができると解することができる（刑訴法222条1項，110条の2）．これは差押え令状の執行に代わる処分であるため，この処分を行うためには差押え令状によることになる．

なお，差押えの要件として，差押えの必要性が要求されるところ，これには，差押えという手段による必要性も含まれる．そのため，後述する記録命令付差押えで足りることが明らかな場合には，電磁的記録媒体の差押えは必要性がなく，令状審査する裁判官は請求を却下することができる[52]．したがって捜査機関は，差押え令状の請求を行うにあたり，記録命令付差押えによることが不都合である事情を疎明資料に付すことが望ましいと思われる．

(3) 記録命令付差押え

差押えは捜査機関が直接的に行う処分であるところ，記録媒体そのものの差押えによると，捜査機関では電磁的記録が記録されている記録媒体を特定することが困難である場合や電磁的記録が複数の記録媒体に分散して保管されている場合には，捜査の目的が十分に達成できないおそれがある[53]．

電磁的記録に関連して，平成23年の刑事訴訟法改正により記録命令付差押えという処分が新たに創設された．記録命令付差押えは刑訴法99条の2の規定により，「電磁的記録を保管する者その他電磁的記録を利用する権限を有する者に命じて必要な電磁的記録を記録媒体に記録させ，又は印刷させた上，当該記録媒体を差し押さえること」と定義される．同条は裁判所による記録命令付差押えを規定しているが，法218条1項が「検察官，検察事務官又は司法警察職員は，犯罪の捜査をするについて必要があるときは，裁判官の発する令状により，差押え，記録命令付差押え，捜索又は検証をすることができる」と規定していることから，捜査段階においても，裁判所による当該令状の発付を受けることで記録命令付差押えの処分を行うことが可能である[54]．この処分は，命令の相手方に記録又は印刷する義務を負わせる新たな強制処分であるが，その性質は，一種の提出命令と解される[55]．ただし，米国における文書提出命令（subpoena duces tecum）と異なり，従わない場合の罰則規定が設けられていないことから，記録命令付差押えは通信事業者等が捜査に協力的であって，直ちに差押えという直接強制によらなくても目的を達することができる場合を想定したものと考えられる[56]．

基地局情報の取得について考える場合，通信事業者のコンピュータそのものを差し押さえ又はそれに代わり他の媒体に複写した上で差し押さえるとしても，膨大な量の基地局に関するログの中から捜査の目的に必要な情報だけを特定することは，

捜査機関にとっては困難と言える．現代のコンピューティング・システムは極めて複雑であり，その操作には種々の専門的知識等が必要である[57]．捜査に必要な基地局情報を取得するにあたっては，セキュリティを解除したり，コンピュータを操作して基地局情報を表示させたり，基地局情報の中から被疑者の携帯電話に紐づくものだけを特定して抽出するといった行為が必要であり，また表示されるログを読み取ることが必然的に伴うため，専門的知識を有する通信事業者をして捜査に必要な基地局情報を特定させることが最も効率的であり，侵害性が弱い方法と言える．さらに，特定した情報を他の記録媒体に記録させるための操作も通信事業者に行わせる方が効率的かつ侵害性が弱い[58]．また，これらの行為を捜査機関自らではなく第三者である通信事業者に行わせることにより，利用者一般のプライヴァシー保護にも資すると思われる．以上のことから，現行刑事訴訟法において基地局情報の取得は記録命令付差押えとして行い得る．

4．記録命令付差押えによることの課題

刑訴法430条1項は，「検察官又は検察事務官のした押収若しくは押収物の還付に関する処分」について準抗告を認めている．記録命令付差押えは，記録命令処分と差押え処分をまとめたものであるため，同条に言う押収に関する処分の対象となり，被処分者は準抗告を申し立てることができる．しかしながら，記録命令付差押え令状執行の相手方としての被処分者は，基地局情報を提出する通信事業者である．しかしながら，取得される情報が被疑者の位置情報であることから，実質的に権利利益の侵害を受けるのは被疑者である．その上，被疑者は必ずしも自己の過去の基地局情報が捜査機関に取得されていることについて認識し得るわけではない．そうすると，被疑者が実質的な被処分者であるにもかかわらず，準抗告を申し立てられないことになる．第三者を介することで準抗告の権利が画餅に帰すことになりかねない．したがって，一定期間の後に被疑者に対し基地局情報の取得を事後通知する等，何らかの法的な措置を講ずる必要があり，さらに第三者に情報を提出させる場合に実質的な被処分者である被疑者にも準抗告の申立適格を認める必要がある．

さらに，基地局情報の取得に違法があった場合，被疑者は証拠排除の申立適格を有するかという点も問題となる．証拠排除申立適格を巡り，学説では，第三者の権利利益の侵害という意味で違法手続きが行われた場合には，被告人自身には違法を主張して排除を求める適格がないと説明される[59]．しかし，この説明は，第三者宅の違法捜査や証人の自己負罪拒否特権の侵害等，被疑者のプライヴァシーとは直接関わりのない場合を想定したものである[60]．基地局情報の記録命令付差押えを行う場合も，被疑者に対する公判との関係では通信事業者は第三者であって，上記の場合と同様と言える．しかしながら，基地局情報の取得によって実質的に侵害されるのは被疑者のプライヴァシーそのものである．この事実を踏まえると，被疑者に証拠排除の申立適格を認めるべきと思われる．

Ⅳ　おわりに

携帯電話は常時基地局と交信し通信事業者に端末の位置を知らせており，通信事業者はこの情報を収集し保管している．携帯電話が犯罪に利用されたと思しき場合，捜査機関は当該携帯電話を証拠として用いる．しかしながら，犯罪に利用されたかに関係なく，被疑者が特定の犯罪に関与したことを立証する証拠の一部として過去の基地局情報を取得することがある．基地局情報により，犯罪の発生時刻に犯罪現場付近に被疑者の携帯電話があったということが把握できるからである．このことが示すように，基地局情報によって把握できるのは単なる過去の一時点の携帯電話端末の位置ではなく，端末所有者の所在である．しかも基地局情報は時刻と紐づけて記録されている．した

がって，特定の携帯電話についての基地局情報を辿れば，網羅的な行動及び移動状況を把握することが可能なのである．加えて，GPS端末による場合には，端末を起動させた以降の情報しか取得できず，取付以前の過去の行動を確認することができない．

類似のGPS装置に目を向ければ基地局情報の特質がより明らかになる．最高裁の事案で行われたように，車両にGPSを取り付けても，車両を使用しない場合には行動を把握することができない．また，車両は米国の事案でそうであったように，他者に貸し出され，他者の目的のために使用されることもある．さらに，車両によって立ち入ることができるのは，公道又は私道ないし駐車場等施設である．他方，携帯電話は所有者が移動する時には通常「携帯」されるため，車両のように使わないからといって置いて行くようなものではない．また，携帯電話には膨大かつ種々の個人情報が含まれているため，所有者以外の者に貸されることもない．そして，携帯電話はポケットや鞄に入たまま自宅やホテル，病院等，場所を問わず所有者に追従する[61]．さらに，基地局情報は通信事業者によって自動的に収集された後，一定期間保管される．このように，基地局情報によって把握できる情報はGPSによって把握できる情報よりも，より精確かつ詳細に個人の行動や生活のパターンを明らかにする[62]．

このような基地局情報の取得は，現行法上は裁判官による令状発付を受けて記録命令付差押えによることが可能である．しかしながら，上記のような基地局情報の性質を踏まえると，実質的な被処分者と言える被疑者のプライヴァシー保護は十分とは言えない．また，少なくともGPS端末の取付を伴う捜査は現行法上許されないが，取得方法は違えども，基地局情報も精確な位置情報の把握という点でGPSによって得られる情報と同様（あるいはそれ以上）のものが得られるのであるから，基地局情報についても法整備されることが望ましい．その際は，被疑者が実質的な被処分者であることを決して忘れてはならない．

1） 中嶋信生＝有田武美『携帯電話はなぜつながるのか』27頁（日経BP社，2007年）．

2） Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 Md. L. Rev. 681, 702 (2011); Justin Hill, *Digital Technology and Analog Law: Cellular Location Data, the Third-Party Doctrine, and the Law's Need to Evolve*, 51 U. Rich. L. Rev. 773, 785 (2017).

3） Christian Bennardo, *The Fourth Amendment, CSLI Tracking, and the Mosaic Theory*, 85 Fordham L. Rev. 2385, 2387 (2017).

4） 「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」6頁．

5） 本項は犯罪捜査の目的ではなく電気通信役務提供の目的で通常の業務過程で取得，保管された記録に対するものである．そのため，捜査機関の要請によって位置情報をこれから取得しようとする場合には2項ではなく同条4項による．

6） 「正当業務行為」とは，電気通信役務を提供する観点から，業務の目的が正当であり，当該目的を達成するための行為の必要性及び手段の相当性が認められる行為をいう．例えば，携帯電話で通信を行うために基地局等において位置登録情報等の位置情報を取得する行為がこれに該当する．ガイドライン解説112-113頁．

7） 石渡聖名雄「逃走中の被疑者の所在把握等のため，通信事業者内設置の装置から将来の携帯電話の位置情報を探索するために同装置の検証令状を発付する際留意すべき事項」髙麗邦彦＝芹澤政治編『令状に関する理論と実務II』別冊判例タイムズ35号144頁（2013）．

8） 前掲註4）．

9） *See* In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. To Disclose Records to Gov't, 620 F.3d 304, at 307-308 (3d Cir. 2010).

10） *Id.* at 313.

11） *See* In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. To Disclose

Records to Gov't, 620 F.3d 304 (3d Cir. 2010); In re Application of the U.S. for Historical Cell Site Data, 724 F.3d 600 (5th Cir. 2013); U.S. v. Davis, 785 F.3d 498 (11th Cir. 2015); U.S. v. Carpenter, 819 F.3d 880 (6th Cir.2016); U.S. v. Graham, 824 F.3d 421 (4th Cir. 2016); U.S. v. Thompson, 866 F.3d 1149 (10th Cir. 2017).

12) *Supra* note 9, at 313.

13) Carpenter v. United States, ___ S.Ct. ___ (2018). 2018WL3073916. 脱稿後，校正の段階で，緑大輔「携帯電話会社基地局に蓄積された被疑者の位置情報履歴を捜査機関が無令状で取得した行為が違憲と判断された事例―― Carpenter v. United States, 138 S. Ct. 2006 (2018)」判例時報2379号128頁；尾崎愛美＝亀井源太郎「基地局位置情報取得捜査と令状の要否―― Carpenter v.United States 判決を契機として――」情報法制研究 4 号15頁 に接した.

14) Thomas K. Clancy, THE FOURTH AMENDMENT: ITS HISTORY AND INTERPRETATION 121 (2013).

15) United States v. White, 401 U.S. 745, 751-752, 91 S.Ct. 1122, 1125-1126, 28 L.Ed.2d 453, 458-459 (1971).

16) *White*, *Id.*; Hoffa v. United States, 385 U.S. 293 (1966); Lopez v. United States, 373 U.S. 427 (1963).

17) *E.g.*, United States v. Miller, 425 U.S. 435, at 442-444 (1976); Couch v. United States, 409 U.S. 322, at 335-336 (1973); *White*, *supra* note 14, at 752; *Hoffa*, *Id.* at 302; *Lopez, Id.*

18) Smith v. Maryland, 442 U.S. 735, at 741-742.

19) *Carpenter, supra* note 13, at ___.

20) United States v. Jones, 565 U.S. 400, 132 S.Ct. 945 (2012).

21) *Id.* at 411.

22) *Carpenter*, *supra* note 13, at ___.

23) *Id.*; Michael T.E. Kalis, *Ill Suited to the Digital Age: Fourth Amendment Exceptions and Cell Site Location Information Surveillance*, 13 PITT. J. TECH. L. & POL'Y 1, 11 (2013).

24) *Miller*, *supra* note 17, at 443.

25) *See* Katz v. United States, 389 U.S. 347, at 351. Rebecca Lipman, *The Third Party Exception: Reshaping an Imperfect Doctrine for the Digital Age*, 8 HARV. L. & POL'Y REV. 471, 473 (2014).

26) *See* Lewis v. United States, 385 U.S. 206, at 210; United States v. Lee, 274 U.S. 559, at 563.

27) *See* Hill, *supra* note 2, at 819.

28) *See Carpenter*, *supra* note 13, at ___. 州最高裁レベルでも同旨のことが指摘されていた．*See* State of New Jersey v. Earls, 214 N.J. 564, at 584 (N.J. 2013). *See supra* note 3, at 2403. 海野敦史『通信の自由と通信の秘密――ネットワーク社会における再構成』260頁（尚学社，2018年）.

29) Riley v. California, 573 U.S. ___ (2014).

30) *Id.* at ___.

31) *Id.* at ___.

32) *Carpenter*, *supra* note 13, at ___.

33) 最決昭和51年 3 月16日刑集30巻 2 号187頁.

34) 最決平成20年 4 月15日が「受忍」と表現しているのは，このような発想が前提としてあるように思われる．刑集62巻 5 号1398頁.

35) 最判平成29年 3 月15日刑集71巻 3 号13頁.

36) 小向太郎『情報法入門［第 4 版］』49頁（NTT 出版，2018年）.

37) 同上39頁.

38) 松井茂記ほか『インターネット法』285頁（有斐閣，2015年），小向・前掲註34）39-40頁.

39) 井上正仁『捜査手段としての通信・会話の傍受』12頁（有斐閣，1997年）.

40) 実際に，無形である通信による会話の取得について令状要件を課す通信傍受法が存在する．同上14頁.

41) 大野正博「携帯電話による位置認識システムの活用とプライヴァシー」朝日法学論集39号77頁，110-128頁（2010年），石渡・前掲註 7 ）.

42) 前掲註35）.

43) 池田修＝前田雅英『刑事訴訟法講義［第 4 版］』192頁（東京大学出版会，2012年）.

44) 小林充『刑事訴訟法第 5 版』109頁（立花書房，2015年）.

45) 大橋充直「携荷電話の捜査実務（導入編）」捜査研究677号66頁（東京法令出版，2007年）.

46) 最決平成11年12月16日刑集53巻 9 号1327頁（元原利文裁判官の反対意見）．田宮裕『刑事訴訟法［新版］』499-500頁（有斐閣，1996年）.

47) 小林・前掲註44）105頁.

48) 池田＝前田・前掲註43）181-182頁.

49) 同上182頁.

50) 同上183頁，中園江里人「電磁的記録媒体の差押

え」近畿大学法科大学院論集14号65頁，73頁.

51） 小林・前掲註44）105頁.

52） 中園・前掲註50）75-76頁.

53） 池田＝前田・前掲註43）183頁.

54） 同上183-184頁.

55） 同上184頁.

56） 小林・前掲註44）106頁.

57） 池田＝前田・前掲註43）184頁.

58） 同上・註11参照.

59） 田宮・前掲註46）406-407頁.

60） 同上.

61） David Oscar Markus & Nathan Freed Wessler, *That '70s Show: Why the 11th Circuit was Wrong to Rely on Cases from the 1970s to Decide a Cell-Phone Tracking Case*, 70 U. MIAMI L. REV. 1179, 1203（2016）.

62） Freiwald, *supra* note 2, at 734.