論　説

「リバース・ロケーション令状」と令状主義

指　宿　　信

1、はじめに

本論文は、最近米国で登場した「リバース・ロケーション令状」と呼ばれる令状方式、すなわち被疑者が存在したと考えられる特定エリアに所在した移動体端末情報を網羅的に収集し、それを母集団としながら被疑者を絞り込む手法について紹介、検討を加えると共に、こうしたデータ収集を出発点とする捜査手法に対する規制のあり方について考究することを目的としている。

このリバース・ロケーション令状は「ジオフェンス令状」とも呼ばれている。それはジオフェンス（geofence）と呼ばれる技術が利用されているためである。ジオフェンスとは一定の場所、エリアに滞在するクライアントを識別して情報を交換するための情報技術で既に産業界や様々な経済活動で広く利用されている[1)]。

例えば、職場に出勤した際にこれまでであればタイムレコーダーと呼ばれる機械に自分のタイムカードを差し込んで、出勤時刻や退出時刻を記録する。ジオフェンス技術を使えば、対象となっているクライアントが設定され

1)　ジオフェンス技術に関する一般的な解説としてたとえば以下参照。「GPS を活用したジオンフェンス機能とは？」Cariot　https://www.cariot.jp/blog/2021/09/30/geofence/

ている空間、すなわち職場、に滞在した時間が全て自動的に記録されタイムレコーダーは不要になる。また、クライアントがチェーン店の会員になっている場合、チェーン店に接近するとスマートフォンのプログラムが作動してその日の特売品やサービスを自動的に知らせるような仕組みにも使われている。

このように、今日ではクライアントの位置情報を把握することで様々なサービスが可能になっている。そこで、特定のエリアに滞在する位置情報を蓄積・記録しておくことができれば、ある時刻、特定の場所に所在した端末情報を収集して犯人を突き止めることが可能になる。

この仕組みがリバースロケーション、すなわち、犯行時刻と考えられる時間帯に犯罪現場やその周辺に滞在した端末を潜在的な被疑者と想定し、位置情報が取得された端末の所有者を割り出し、遡って被疑者を絞り込もうという発想へと繋がった。

こんにち、ほとんどのスマホ利用者の位置情報を網羅的に蓄積・記録しているのは、Google 社である。スマホ利用者が Google のサービスを利用していれば端末の位置情報は Google 社に記録・蓄積される。Google 社から位置情報記録を強制的に取得するための令状がリバースロケーション令状、通称「ジオフェンス令状」なのである[2)]。

このジオフェンス令状はまだ日本では使われた痕跡がない。現在、この技術を用いていることが判明しているのは米国である。

この令状が使われた最近の例を紹介しよう。2021 年 1 月 6 日に数百人の暴徒がワシントン DC の国会議事堂に乱入した事件は世界を驚かせたが、この事件の実行犯を特定するためにジオフェンス令状が用いられた。多数の暴徒が一定の時刻に国会議事堂にいたが、その暴徒を特定するためにジオフェンス令状が使われたのだ[3)]。

2） この問題に関する邦語での最初期の記事として、拙稿「スマホ位置情報『一網打尽』捜査　ジオフェンス令状の正体」世界 2022 年 1 月号（岩波書店）52 頁参照。

3） “How a Secret Google Geofence Warrant Helped Catch the Capital Riot Mob”, WIRED, Sep. 30, 2021.

この事件の暴徒がスマートフォンなどの移動体端末を利用していてGoogleのサービスを利用していれば、位置情報記録を入手することが容易にできる。そこでFBIは、この位置情報に基づいてアカウント情報を取得し、個人の特定をおこない、300人以上を逮捕したとされている。

そうした被疑者の一人について起訴状に添付された資料には、同人の位置情報がGoogle社の位置情報サーバで確認されたことが記載されていた。多くの暴徒が議事堂内で撮影した動画や写真をSNSにアップしていたため、FBIは、位置情報で特定された個人情報と投稿された映像で被疑者の同一性を確認することができた。

これまでの捜査であれば、監視カメラの映像をもとに被疑者を特定する作業が繰り返されていただろう。しかし、監視カメラの映像があったとしても本人特定は簡単ではない。ところが、Google社の位置情報サーバに記録が残ってさえいれば、Googleのアカウントを経由して個人特定まで可能だ。

こんにち世界的にはアンドロイド携帯がスマホ市場の7割を占める。このアンドロイド携帯は自動的にGoogle社に位置情報を取得されている。それ以外のスマートフォン、例えばiPhoneであってもGoogle社のサービスを利用していれば、当然位置情報を取得される。現在、スマートフォンアプリで最も利用されているのはG-mail、Google map、そしてGoogle searchである。つまり、アンドロイド系であれiPhoneであれ、ほとんどのスマートフォン利用者はGoogle社にその位置情報を残さなければネットの利用は不可能な状態にあると言っても過言ではない。

大量の被疑者がいる事件や、被疑者不詳の事件ではこのジオフェンス令状が大いに頼りにされることがわかるだろう。

2、ジオフェンス令状に関する手続と利用実績

続いて、ジオフェンス令状の発付までのプロセスを紹介する。

法執行機関は、被疑者が直ちに判明しない場合、ジオフェンス令状を裁判所に請求して、これを使ってGoogle社に対して同社の位置情報サーバに記録された特定エリアに特定時間に滞在したアカウント情報を提出させる。

Google 社はこの命令を受けるとまずジオフェンス令状に従うかどうかの判断をおこなう。従うと決めた場合（裁判所に対して異議申し立てを行なうことも理論上はあり得る）、令状に記載されたエリア所在の端末情報を提供する。その後、法執行機関がこの端末リストからユーザ情報の開示を要求する。たとえてみると、犯行現場に残された指紋情報から指紋所有者をリストアップし、そこから被疑者を絞り込むというプロセスに似ていよう。もちろん、米国でも日本でも指紋情報の登録義務はない。しかし、Google 社への位置情報の提供も義務ではないものの、スマートフォンを利用し、Google のアプリを使えば自動的に位置情報は Google 社に記録される。結局、全国民指紋情報登録制度と同様の効果をもたらす。

2020 年 5 月に、Black Lives Matter (BLM)（黒人の命が問題だ）運動の最中、抗議行動がエスカレートし暴徒化した事件に関して、ミネアポリス警察署が取得したジオフェンス令状をみると、被処分者はカリフォルニア州に本社のある Google 社で、請求人の警察官の氏名は黒塗りになっている。特定の日時に特定のエリアに所在した、GPS 発信装置、Wifi 発信装置、ブルートゥース接続機器そして携帯の位置情報とその履歴を提出するよう求めている。

一方、ジオフェンス令状の利用状況については全く情報が公開されていなかった。2020 年 8 月にこの令状方式の存在がメディアによって伝えられプライバシー侵害の批判が強まったのを受けて、Google 社がようやく利用実績を開示した[4)]。開示された資料によれば、2018 年第一・四半期に同令状の利用が始まっており、2020 年には毎週 200 件のペースで全米の法執行機関から令状を受け取って位置情報データベースに記録された該当端末に関する情報を提供している。利用の多いのはカリフォルニア州、テキサス州、フロリダ州の順で、95％を州の法執行機関が占めている。

3、ジオフェンス令状の法的問題点

ジオフェンス令状については、当初から様々な法的問題が指摘されてきた。

4） https://www.documentcloud.org/documents/21046081-google-geofence-warrants

まず、「令状」として情報を強制的に取得するには通常予定されているはずの被疑者が特定されていないことが問題だとされている。もちろん、通常事件でも被疑者不詳というケースもある。しかし、その場合でも差押え取得対象は特定されている。そうでなければ「一般令状（general warrant）」として違法となる。ジオフェンス令状は、データを大量にかき集めるための令状だからこの一般令状に当たるという批判があった。この点、後に検討したい。

また、位置情報が取得される被処分者に対して事前告知がない。Google社は場合によって法執行機関からアカウント情報の提供を求められていることを情報主体に告知することがある。しかし、少なくとも最初の特定エリアに滞留していた位置情報を取得する段階では告知はない。この問題は、事前に同意の上で第三者に提供されているデータを法執行機関が情報主体に告知することなく取得しても問題はない、という考え方―第三者法理―と関係する。この点についても後に検討する。

重要な問題として、捜査機関が設定したエリアに偶然滞在していただけの無実の人を誤認逮捕してしまう危険性も見逃せない。多くの人が滞留する場所であれば多くの無関係な人の位置情報も収集される。実際に、米国ではすでにジオフェンス令状が使われたケースで無実であることが判明した事案が出てている[5)]。

例えば、フロリダ州で誤認逮捕されたザッカリー・マッコイ氏のケースが分かりやすい。ある日、マッコイ氏はGoogle社から一通の警告状を受け取った。それは警察が同社に対して強盗容疑で同氏の個人情報を開示するよう要求していることを告知する内容だった。警察は位置情報で同氏が強盗事件の被害者宅である犯罪現場にいたことを明らかにできると考えたのだ。

マッコイ氏は事件のあった日に1時間に三度、自転車で被害者の家の前を通っていた。同氏は自転車の走行を記録するアプリを自身のスマートフォンで利用していたため、このアプリがGoogle社に彼の位置情報を送っていた

5） “Google tracked his bike ride past a burglarized home. That made him a suspect.” By Jon Schuppe, NBC News March 7, 2020.

のだ。マッコイ氏から相談を受けた弁護士は、警察が犯行現場近くに所在した位置情報リストを同社から受け取っていたことを突き止めた。同氏は、自身が犯罪と無関係で、同社が警察にそれ以上の情報を提供することを止めさせるため、弁護費用として７千ドル（およそ 100 万円）を費やさなければならなかったという。

４、ジオフェンス令状をめぐる法的状況

続いて、そうした様々な問題のあるジオフェンス令状が米国でどのように議論されているのか、裁判例や学説を検証してみよう。

まず、第一に、ジオフェンス令状が請求された令状請求裁判所の判断を紹介し、第二に、まだ少ないながら公刊物に現れている学説を紹介する。最後に、ジオフェンス令状を用いて得られた位置情報を証拠として起訴された事案において、弁護側が同令状を憲法違反であると主張し違法収集証拠として位置情報を排除するよう争った事案を紹介する。

４－１　令状裁判官の判断

2020 年 7 月 8 日北イリノイ地区連邦地裁の David Weismann 判事は、以下の事案で令状請求を却下する判断を示した[6)]。

事案はある調剤会社からの窃盗罪事件だ。捜査機関は３件のジオフェンス令状を請求した。１件目の令状では、取得対象とされたエリアは盗難場所から 100m 四方、時間帯は盗難のあった日の午後の早い時間帯で 45 分間だった。２件目と３件目の令状では、対象エリアは犯人が盗品を密売するために発送したとされる場所の 100m 四方で、時間帯は二日間それぞれ 45 分間だった。

これらの令状の取得対象エリアは複数階層の商業ビルで、いくつかの医療機関も入居していて多くの無関係な人が滞在する場所である。

判事は、第一に請求された令状が広範に過ぎること、第二に差し押さえる

6）　WL 5491763 (N.D. Ill. July 8, 2020).

べきもの（items）が特定、表記されていないということを指摘した。そして、捜査機関がジオフェンス令状の地理的範囲を限定し、3 件の令状で得られた位置情報のリストにあった端末についての付加的な情報を求める際の携帯電話番号［の数］を限定していれば、こうした広範性や特定性の問題を解決できたはずだと述べている。

結論として判事は、令状は捜索範囲と差し押さえるもの（items）の特定性の双方に関して広範に過ぎ、修正第 4 条の先例法（jurisprudence）に適合しないとして、政府側による令状請求を却下した。

反対に、令状を発付したケースを紹介したい。

2020 年 10 月 29 日北イリノイ地区連邦裁判所 Mary K. McClelland 判事は放火事件捜査においてジオフェンス令状が請求され、これを発付した際に次のような理由を記している [7)]。

すなわち、捜索にあたって求められる「相当性」要件は、特定の場所や物と犯罪を結びつける終局的な証拠（の存在）まで要求していないので、捜索令状の発付に当たって、裁判所は犯罪の性質やその方法によって証拠が発見されるであろう場所について合理的な推論を働かせることが認められている、という。

判事は、本件における放火現場とその付近に所在していた携帯電話の位置情報を取得する捜索令状において、［修正 4 条が要求する］特定性の要請は充足されていると考えた。なぜなら、捜査機関は、十分に限定された時間帯、すなわちおよそ 15 分から 30 分で、個別に限定したジオフェンス・ゾーンの線引きをしており、取得対象エリアを放火場所やその付近の通りに絞り、住居や商業ビルを除外することによって無関係な個人の位置情報を大量に獲得する可能性を最小化していた、とする。

7） Matter of Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation, 497 F. Supp. 3d 345 (N.D. Ill. Oct. 29, 2020).

４－２　学説の状況と立法対応

現在までのところジオフェンス令状を主題とした法学論文は、米国主要ロージャーナルでも３本しか確認できない。いずれも裁判所に規律を委ねるのではなく、濫用を抑止するため予防的な立法上の手当てを求めている[8)]。例えば、「リバースロケーション令状はわれわれの生活を安全にすると同時に、政府による監視の蔓延に繋がる」ので、今後も警察がジオフェンス令状を使用するなら、消費者や市民の修正第４条の権利を守るため、更なる保護が必要であり、「連邦および州の立法府は、令状請求にあたり相当の理由を満足させるかどうかを判事が判断することを容易にするよう新たな法律を制定すべき」という。

しかしながら、当の連邦、州の立法府の対応は活発ではない。唯一、ニューヨーク州議会で 2020 年４月に法案が提出されたにとどまっている[9)]。

４－３　違法収集証拠排除申し立て

次に、ジオフェンス令状で取得された位置情報が被告人の犯行の情況証拠として証拠調べ請求され、それに対して弁護側が違法収集証拠であるとして排除を申し立てたケースを紹介する。

事案はバージニア州リッチモンドで 2019 年 5 月 20 日に発生した強盗事件である。警察は、ジオフェンス令状で犯行場所の銀行の 150 メートル圏内の犯行前後１時間の滞在端末を要求した。

令状の第一段階で Google 社は 19 個のアカウントを警察に提供した。そのうちの１個のアカウントは同時刻に銀行内に所在していたことがわかっている。強盗事件を目撃していた証人の証言によりそのアカウントの持ち主が犯人であるとされた。第二段階で警察は 19 個のうち匿名化されていた９個の

8）　Mohit Rathi, “Rethinking Reverse Location Search Warrants”, 111 Journal of Criminal Law and Criminology 805 (2021), Note, “Geofence Warrants and the Fourth Amendment”, 134 Harvard Law Review 2508 (2021), Haley Amster & Brett Diehl, “Against Geofences”, 74 Stanford Law Review 384 (2022).

9）　Reverse Location Search Prohibition Act, Assembly Bill A84A 2021-2022 Legislative Session. https://www.nysenate.gov/legislation/bills/2021/A84

アカウントの開示を要求した。裁判所は 150 メートル圏内にいたアカウントの犯行時刻後の対象圏外における位置追跡を許容した。この記録を使って警察はアカウント保持者の住居を特定し、被疑者の詳細な情報を入手した。第三段階で警察は、Google 社に３個のアカウントの契約者情報の開示を要請し、氏名、住所、電子メールアドレスを入手して起訴に至った。

2022 年 3 月 3 日、ヴァージニア東地区連邦裁判所の Hannah Lauck 判事は、本件ジオフェンス令状は修正４条に違反する、と判断した[10)]。ただし、捜査によって得られた情報は証拠として許容されるとした。その根拠は、伝統的な排除法則に関わる例外則のひとつである「善意の例外（good faith exception）」である。つまり、ジオフェンス令状を請求した捜査官には憲法違反をしているという認識がなかったから、違法ではあるけれども排除は相当ではない、というのである。

結局、判事が証拠排除の申し立てを却下した以上、いかなる範囲で令状によって求められるプライバシーの合理的期待を被告人が侵害されたかどうかについて、判断が示されなかった。その一方で判事は、ジオフェンス令状のような技術発展に現在の修正４条の保護原理が大幅に遅れを取っていると警告を発している。立法府の動きを促していると言っていいだろう。

５、分析と検討

最後に、ジオフェンス令状の法的妥当性について米国での議論を紹介するとともに４点にわたって検討を加えていきたい。第一に、ジオフェンス令状が「一般令状」にあたり違憲違法であるという指摘について、第二に、いわゆる「第三者法理」について、第三に、ジオフェンス令状が持っている「地引網的」性格について、そして第四に、ジオフェンス令状の執行に関わる問題について、である。

10） United States v. Chatrie, No. 19-cr-00130, 2022 WL 628905.

５－１　「一般令状」批判の妥当性

合衆国憲法修正４条は「不合理な捜索及び逮捕押収に対し、身体、住居、書類及び所有物の安全を保障される人民の権利は、これを侵害してはならない。 令状はすべて、宣誓又は確約によって支持される相当の理由に基づいていない限り、また捜索する場所及び逮捕押収する人又は物が明示されていない限り、これを発してはならない」と定めている。日本国憲法３５条のルーツであることはいうまでもない。令状発付にあたって裁判官は同条後段にある“相当な理由（probable cause）”と、捜索される場所や逮捕押収の対象となる人や物の“特定性（particularity）”が満たされているかどうかを確認しなければならない。

同条は、かつて植民地時代に法執行機関が押収すべき場所や物を特定しない「一般令状」が用いられたことへの反省から生まれたものだ。こうした一般令状を禁じるため、裁判官にゲートキーパを期待して令状発付に際して二つの要件―相当の理由と特定性―を設けたと解されている[11)]。

前述したように、ジオフェンス令状はこの“一般令状”のように捜査機関が不特定情報をただ探索しているだけではないかと疑問視されている。すなわち、一定時刻の特定エリアで位置情報サービスを受けたアカウントをリスト化するよう命じることは、先に説明した位置履歴のオプトイン方式を前提にした場合には必ず犯人がそのリストの中に含まれるという「相当の理由」を説明できないからだ。また、特定の被疑者の情報を開示させるのではなく犯人の可能性のあるアカウントを提示させているのは、捜索押収に当たって対象の「特定性」を欠いているとも批判されている。

さて、一般令状について米国法学ではこれまで次のように定義されてきた。例えば著名なブラック法律辞典は、一般令状について「場所や人物の特定性を欠いた捜索押収の広い権限を法執行官に与える令状。押収されるべき物や捜索される場所について十分に特定性を欠いた捜索・逮捕令状」と定義する

11）　修正４条について詳しくは、ジョシュア・ドレスラー他（指宿信監訳）『アメリカ捜査法』（レクシスネクシス・ジャパン、2014）第４章以下参照。

(Black Law Dictionary 11th Ed.)[12]（傍点筆者）。

ジオフェンス令状の請求を却下した令状裁判官の判断も「特定性」を問題としているから、やはり請求時点で捜査機関が「地引網的に」情報を取得するという同令状の性質が問題の根本に在ることは間違いないだろう。

5－2 「第三者法理」適用の是非について

反対に、ジオフェンス令状の適法性、合憲性の根拠はなにか。法執行機関は、いわゆる「第三者法理」を持ち出す[13]。すなわち、スマートフォン利用者が事前に Google 社による位置情報の収集に同意しているのであるから、収集した第三者から適法な手続を踏まえて情報を取得することには問題がない、というのである。スマートフォンを利用する被処分者が第三者に提供した情報にはプライバシーの合理的期待はなく、ジオフェンス令状に基づく特定エリアに滞留したクライアントの情報収集は適法だとする。

この第三者法理の前提となっているのは、建前として利用者において位置情報の取得がオプトイン方式となっていることだ。Google 社も同社による位置情報収集は完全に利用者の意思に基づいて行われていると主張してきた。例えば、先に米国でジオフェンス令状に基づいて得られた位置情報が違法収集証拠として争われた Chatrie 事件で訴外第三者として Google 社は意見書で次のように述べている。

> Google 社の位置履歴記録は利用者自身によってコントロールされており、Google 社側は利用者の判断に従ってその情報を蔵置しているに過ぎない（例えば、オプトインするかオプトアウトするか、また、当該記録を保存するか、編集するか、消去するか）。

12）「一般令状というのは、イングランドで治安妨害の疑いのある出版物を探し出すために用いられたものである。捜索令状に基づいて、一つの小さな理由から家屋に押し入り、治安妨害的な中傷罪での起訴に備えて書籍や書類を捜索することを（実質はくまなく荒らしまわることを）王の官吏に許容するものであった」同書 74 頁。

13） 第三者法理について、たとえば髙村紳「プライバシー侵害を伴う捜査の許容される限界：「第三者法理」の検討を通じて」法学研究論集第 48 号（2017 年）143 頁を参照。

また、ジオフェンス令状が対象とする位置履歴についても、Google 社は次のように利用者の任意の意思によって蓄積されているだけだと主張している。

> Google 社は利用者が自身のアカウントの設定上で自身の位置記録をオプトインしない限り、（かつ、自身のモバイル端末を適切に設定して Google アカウントへのログインしない限り）保存されないのである

しかしながら、Google 社のこの主張については重大な疑義が明らかになっている。例えば、AP 通信は Google 社が位置情報機能をオフにした利用者を実際には追跡していると報じている[14]。豪州では、豪州競争・消費者委員会（Competition and Consumer Commission、ACCC）が提起した訴訟において、Google が位置情報の設定を二重にすることで消費者を欺いていたとする連邦裁判所の判決が出されている[15]。その際、裁判所は、「Google アカウントを作成した際、Google は『位置履歴』の設定は Google アカウントだけの設定であり、それにより Google が消費者の位置に関する個人を同定できるデータを収集し保持、利用するという、間違った表現をしている」と指摘していることは見逃せない。

米国アリゾナ州で起こされた消費者訴訟でも、当局は Google 社の個人情報収集について、「Google は位置情報などの設定項目をユーザーにわかりやすく配置したアンドロイド携帯をテストしたものの、多くのユーザーが位置

14） “AP Exclusive: Google tracks your movements, like it or not” (August, 14, 2018) https://apnews.com/article/north-america-science-technology-business-ap-top-news-828aefab64d4411bac257a07c1af0ecb　記事では、Google 社が位置情報マーカーを保存するのを止めるには、利用者は「ウェブとアプリのアクティビティ」という名前の設定をオフにしなければならない。この設定は初期設定ではオンになっており、設定の説明文には位置情報に関する記述がない、と指摘している。

15） https://www.accc.gov.au/media-release/google-misled-consumers-about-the-collection-and-use-of-location-data

情報の共有をオフにしてしまうことがわかり、Google はこれを“問題”と考え、意図的に設定項目を設定メニューの奥深くに配置し、操作に不慣れなユーザーが到達できないようにしたことを示す内部文書が発見された」と非難している。しかも Google 社が、「携帯電話メーカーに対し位置情報の設定がわかりやすすぎるとして、簡単に目に触れない場所へ埋め込むよう“周到に圧力をかけた”」というのである[16)]。

2022 年 1 月には、ワシントン DC、テキサス、インディアナ、ワシントン州の各司法省が Google 社を消費者保護法違反の疑いで提訴した。豪州のケースと同様、各州当局は、「Google は位置情報のプライバシーを保護できるよう設定機能を置いているが、実際は情報を収集して消費者を欺いている」というのである。ワシントン DC から Google 社に対して起こされた訴状には、データ収集について「（ユーザー側が）選択を可能にする能力を侵食するような偽装的な方法を用いている」と非難されているところである[17)]。

こうなると、Google 社がいう“スマートフォン利用者の同意に基づく位置情報・位置履歴の収集、記録”という実態が怪しくなってこよう。「第三者法理」を適用しようにもその事実的基礎が存在せず、ひいては、ジオフェンス令状を正当化するための前提が崩れることになっている。

５－３　「地引網的捜査」の適法性

先にも触れたように、米国ではジオフェンス令状を批判する際に「地引網的捜査」（dragnet investigation）という表現が使われる。この「地引網的捜査」という言葉は、元々は「警察による犯人逮捕の一方法。一定の地域に大量の警察官を投入してターゲットの犯人を発見することを目的とする」（Collins Dictionary）手法を指していた。ジオフェンス令状の場合、特定地域に網を

16）“Google cannot escape location privacy lawsuit in Arizona, judge rules”, by Paresh Dave, Jan 25, 2022 Reuters. 最終的に、2022 年 10 月に Google 社がアリゾナ州に 8500 万ドル（約 100 億円）の賠償金を支払うことで和解したと公表されている。”Google to pay Arizon $85M in privacy suit that alleged ‘deceptive’ location tracking”, Oct 5, 2022 USA Today.

17）“Google Sued By Washington, D.C. Over Alleged Location Tracking Deception”, by Derek Saul, Forbes, Jan 24, 2022.

かけて情報を引っ張る様子が思い浮かんだことからこのような非難が向けられたものと想像される。

地引網的な捜索行為や犯人逮捕行為を直ちに違法と断ずることはできない。実際、ある種の情報が犯人の特定に繋がるとして大規模な情報収集を行なって、そこから遡って（リバース）絞り込んでいく手法はこれまでも日本で行われたことがある。それが、1995 年に起きた地下鉄サリン事件の捜査で用いられた、国会図書館利用者記録の差押えである。日本の警察は、オウム真理教による地下鉄サリン事件の捜査のため、犯人がサリン製造に関する文献を国会図書館で閲覧した可能性があると考え、被疑者不祥で国会図書館の利用者記録 14 ヶ月分（利用申込書 53 万人分、資料請求票 75 万件、複写申込書 30 万件）を押収した[18]。その記録から犯人逮捕に結びつく情報が得られたのかどうかは定かではないが[19]、かかる令状についての合憲適法性が日本の裁判所で検討されることはなかった。

そこで、日米両国で実施された包括的な差押えから被疑者に関連する情報を取得する「地引網的捜査」手法の検討のため、米国議会議事堂襲撃事件で使われたジオフェンス令状と、日本の地下鉄サリン事件捜査のため国会図書館の利用者記録の入手のために使われた捜索差押令状とを比較してみたい。

まず収集対象だが、位置情報と図書館利用記録という、いずれもプライバシー情報に含まれるデータだ。しかも、図書館利用記録の方が思想信条の自由と直接結びついている点でより法益侵害が大きいと考えられよう。取得の範囲については、ジオフェンス令状では位置情報の取得にあたって対象地域の特定や時刻の特定などが行われるのに対して、図書館利用記録は 14 カ月間に及ぶ全利用者の記録が取得された。図書館の利用記録は利用者の思想信

18）「国会図書館でサリン書閲覧調査　資料 53 万人分押収」朝日新聞 1995 年 4 月 19 日夕刊記事。4 月 6 日、警視庁によって押収された資料は２トントラックで搬出され、6 月 22 日に、利用申込書３枚、資料複写申込書７枚以外が全て国会図書館に還付された。JLA 図書館の自由に関する調査委員会関東地区小委員会「図書館利用記録の押収 ―『地下鉄サリン事件』捜査に関する事例」図書館雑誌 1995 年 10 月号 808~810 頁参照。

19）1995 年 5 月 29 日付読売新聞は押収された複写申込書に教団化学班キャップの名前があったと伝える。

地引網的捜査の比較

米国連邦議会議事堂襲撃事件

項目	データ
発生日時	2021年1月6日　ワシントンDC
被疑事実	不法侵入、窃盗、器物損壊、暴行、傷害致死、治安妨害、致死性武器使用、
逮捕者数	700人以上、350人以上身元不明
被害状況	死亡5人、負傷者140人以上
利用令状	上記発生日の午後２時から３時の携帯端末のリストを求めるジオフェンス令状
押収データ数	最低でも45人分
法的判断	進行中

地下鉄サリン事件

項目	データ
発生日時	1995年3月20日　東京都内
被疑事実	殺人、殺人幇助、殺人未遂、傷害他
逮捕者数	40人（18人起訴、死刑10人・無期5人）
被害状況	死亡12人、負傷者6,300人
利用令状	捜索差押令状
押収物	国会図書館１４ヶ月の全利用申込書53万人分・資料請求票75万件・複写申込書30万件（4月6日押収、6月22日利用申込書3通、複写申込書7通を除いて全て還付
法的判断	刑事裁判（判決文）で言及なし

条に関わる情報で多くの無実の人の思想信条に関するデータが大量に取得されたことはより深刻といえる。

捜索の必要性や相当性についてみても、位置情報の場合は犯人が所在した蓋然性は高いのに対して、図書館利用記録の場合、該当情報が存在する蓋然性は必ずしも高いとはいえず、無関係情報が大量に含まれていることは明らかだ。やはりジオフェンス令状に比しても侵害の程度が大きいと言わざるを得ない。議事堂襲撃事件の場合は議会職員や議員などを除外すれば容易に侵入者を特定することが可能だから、関係のない無実者の情報を取得する危険性も低い。

こうして、日米の地引網的捜査の先例との比較という限りにおいては、議事堂襲撃事件使われたジオフェンス令状の違法性の程度は比較的低いと評価されることになるだろう。

５－４　執行上の問題点

とはいえ、ジオフェンス令状の執行にあたっては見逃せない問題点がいくつかあるのも事実だ。順に検討しよう。

当然の前提となるが、ジオフェンス令状で得られるデータの正確性の問題がある。さらにいえば、スマートフォンの電源をオフにしている滞留者についてGoogle社は位置情報を取得できないから、捜査機関の入手することの

できるデータについて不十分性は否めない。Google 社の位置情報を集約するデータベースはセンサーボルトと呼ばれるサーバだが、その位置情報データがどこまで正確か、という問題も残っている。

また、ジオフェンス令状を用いて犯人を特定できたケースが一体どのくらいあるのかも不明である。Google 社は令状請求件数については公開に踏み切ったものの、そのうち何件で捜査機関が犯人検挙に至ったかというデータは開示されていない。いわゆる「ヒット率」が分からず、その点で効率性や有効性が検証されていないのが現状である。誤認逮捕まで現実に発生していることに照らすと、効率性や有効性の検証が今後不可欠であろう。

そこで、ジオフェンス令状を立法化するには、通常の捜索差押令状とは区別した上で、通信傍受令状に倣って、第三者機関による監査や査察などのチェックを盛り込んだ立法が必要だと思われる[20]。捜査機関が収集したジオフェンス関連データについても、無関係であることがわかった Google クライアント情報を破棄することを義務付けることなど、司法的な判断に委ねるだけでは不十分な点をカバーする立法が望ましいだろう。

6、おわりに

ジオフェンス令状をめぐっては、合衆国最高裁判所の判決が出ていないのはおろか、未だ州最高裁、中間上訴裁判所などでも判断が示されたことがない。今後のアメリカ法の動向には目が離せないところだ。

筆者の基本的なスタンスは、米国の学説と同様、ジオフェンス令状の実施については新たな立法が必要というものだ。

本稿の最後に、ジオフェンス令状問題の検討から引き出すことのできる刑事訴訟法学上の示唆として、次の二つの点を指摘しておきたい。

第一は、日本で最近刑事訴訟法学説の中で有力に唱えられるようになってきた、「事後規制論」への転換についてである[21]。若い世代の刑訴法学者を

20）　その方法については、拙監修『GPS 捜査とプライバシー保護』（現代人文社、2018）参照。

中心に次のような考え方が提唱されている。すなわち、監視型捜査が発展し、捜索押収されるデータの収集が大規模化していく現代では、従来の令状主義では十分に捜査機関を規律できないため、事前規制型の令状主義ではなく、捜査終了後に第三者機関が捜査の成果物をチェックする事後規制型の手続に転換することがより所期の目的（捜査権の統制と市民の自由の保護）を達成できる、とする考え方だ。

この考え方は、GPS 発信装置を用いた位置情報収集のような非定型的な捜査の登場によって、開始前には収集されるべきデータについて十分にその特定性を満たすことができないことから、現実的な必要が感じられるようになったと考えられる。

しかしながら、米国州レベルのみならず欧州各国でも GPS 捜査については各種の事前規制を用意して、取得データの範囲を限定しようと試みているし（次表参照）、直ちに事前規制が有効でないという理由にはなり得ない。

また、先にみた米国の学説の中で有力な立法論でもいずれも事前規制を念頭に置いていた。米国の刑事訴訟法学説を見渡しても、司法による統制の可

位置情報取得捜査の立法比較

	米国（メイン州）	イギリス	ドイツ	フランス	豪州(NSW州)
事前・事後の規制	事前（令状審査）事後（本人告知）	事前（警視以上の許可）	事前（長期の場合、令状審査）事後（本人告知）	事前（令状審査）	事前（令状審査）事後（オンブズマン査察）
対象犯罪・保護利益等	制限なし	国家安全保障、犯罪抑止、国家経済利益、安全、公衆衛生、脱税等	重大な犯罪	生命・身体犯については３年以上の罪、それ以外は５年以上の罪	制限なし
実施要件	相当の理由	必要性、相当性	犯罪の重大性、補充性	必要性	犯罪の蓋然性、必要性、相当の理由
実施期間	１０日間	3ヶ月（通常・書面申請）72時間（緊急・口頭申請）	短期監視（最大２日）長期監視（３月）	検察官許可（１５日間）裁判官許可（一ヶ月）特殊事案で４ヶ月	９０日以内
被処分者へ告知	３日以内（90日以内の延長可）	—	あり	—	—
異議申し立て	—	審判所(Tribunal)による審査	—	あり	—
記録媒体の保存	—	終了後３年間保存	あり	あり	あり
記録媒体の破棄廃棄	—	あり	あり	あり	あり
記録保管状況に対する査察	—	あり	—	—	あり
捜査実施報告義務	あり（裁判所。裁判所は議会に）	あり	—	あり	あり
記録の秘匿化	—	あり	—	あり	あり
情報流用	—	—	他事件利用可	—	禁止

21） 事後規制論について、たとえば「〈小特集〉強制・任意・プライヴァシー：『監視捜査』をめぐる憲法学と刑訴法学の対話」法律時報 87 巻 5 号（2015）58 頁以下参照。

能性に対する疑問は見受けらない。

今後、事後規制を導入するとして具体的にいかなる主体がいかなる手続で関与するかを明らかにしていく必要があるだろう。令状主義が果たしてきた捜査権統制と市民の自由の保護という役割を、事後規制がどのように代替できるかという検討が必要だ。事後規制論者は、先行例としてオーストラリアが監視捜査についてオンブズマンによる監査を実施しているのを参考に、具体的な手続や制度を提示しておくべきだろう。

参照されるべき例としては、米国メイン州やドイツで監視捜査実施後に対象となった本人告知が義務付けられていることが挙げられる。日本の通信傍受法でも同様である。告知の仕組みがあれば取得対象者自身が監視捜査の正当性を争う機会を設けることができ、事後規制が実質化することに繋がるだろう。

第二は、Google 社のような巨大企業が保有している個人データ（ジオフェンス令状の場合は位置情報・位置履歴）を法執行機関が収集し、それを犯人特定や公判での立証に用いることの問題だ。これは、巨大プラットフォーマが法執行機関の「エージェント」と化してそれがビジネス化していること、利用者のプライバシーが圧倒的なプラットフォーマによって侵食されていることに関わる [22)]。

この巨大企業の保有する個人情報を捜査機関が入手する方法としては、日本の捜査実務で大量に利用されている「捜査関係事項照会」という手続がある。この照会手続は、令状なしに私企業に対して収集している顧客の個人情報を捜査機関に提供させるために用いられる任意処分だ。最近、個人情報保護の観点から問題視されている [23)]。個人情報を顧客から収集するにあたり企業側は必ず約款上犯罪捜査の場合に免責を明記している。ただ、この「照会」

22） この点はショシャナ・ズボフ・野中香方子訳『監視資本主義 ― 人類の未来を賭けた闘い』（東洋経済新報社 , 2021）など参照。

23） 共同通信社社会部取材「丸裸にされる私生活企業の個人情報と検察・警察」世界 2019 年 6 月号。

手続の場合は裁判所が令状発付手続で関与することがない。もっぱら捜査機関が直接企業に提供・開示を要求している。

「照会」手続には告知聴聞手続きが用意されていないし、保秘条項が置かれて企業が顧客に通知することを禁じているのが一般的で、顧客は自身の個人情報が捜査機関に収集されたことを知りうる術がない。

犯罪と無関係であった場合であっても、収集された個人情報がどのように保管利用廃棄されるのかも定めがない。日本は 2019 年に GDPR の十分性認定を受けているが、この「照会」手続だけをみても公的機関である捜査機関の個人情報収集に大きな問題が横たわっていることは否定できない[24)]。

本稿が取り扱ったジオフェンス令状のように、IT 利用が犯罪捜査において活用され、効率的で有効な捜査に結びつく反面で、伝統的な原理原則が掘り崩されたり、無関係の市民のプライバシーが知らないうちに侵食されたりしている実態について、刑事訴訟法学者はもっと注意を払う必要があることを最後に強調しておきたい[25)]。

（了）

本稿は 2022 年 11 月 2 日に韓国・成均館大学校で行った講演原稿を論文調に改め、注を附したものである。

（いぶすき・まこと＝本学教授）

24） この問題については、拙稿「講演録―データ駆動型捜査時代の規律方法 ～令状主義との決別？」情報法制レポート第２号（2022）。

25） 筆者による IT を用いた犯罪捜査の問題についてその他の技術については、拙著『電脳空間と刑事手続』（成文堂、2022）を参照。また、連載「刑事手続における IT 利用の光と陰」刑弁 OASYS　URL: https://www.keiben-oasis.com/ 第 10 回以降参照。