捜査におけるデジタル情報収集に対する法的規制

高　村　　紳

第１章　はじめに

現在、我々は様々な情報通信端末を所有するのが一般的なものとなっている。この点、我が国における情報通信端末の利用状況について総務省の調査によると、令和３年の段階で、日本におけるモバイル端末の世帯保有率は96.8％と極めて高い割合を示している(1)。さらに、その中でもスマートフォンの世帯保有率は80％を超え、個人の所有率も70％近くにまで上っている。また、このようにスマートフォンをはじめとした情報通信端末が普及したことによって、日常的なインターネット利用率は80％を超えている（なお、そのうちの約70％がスマートフォンを通じたものであり、パソコンは約50％となっている）。まさに、インターネットを利用するための設備及び端末は我々の生活においてインフラとも呼べる物となった(2)。さらに、

このように情報通信端末が普及するにつれて、事業者・消費者間の電子商取引（以下、B to C-EC）の規模も大幅に拡大しており、国内での市場規模は約19.3兆円にまで上っている。また、他国との越境型 B to C-EC も拡大しており、2020年の段階で日本と米・中との規模は約3400億円とされている(3)。これは、情報通信を通じた商取引の規模を示した数値であるが、このことと先の情報端末の普及率、そしてインターネットの利用状況等を併せて考慮すれば、我々の生活において情報通信がどれほど重要な意義を有することとなっているかはもはや自明のものであると言えよう(4)。

このように、我々の生活において情報通信端末を通じた情報のやり取りが日常的なものとなり、容易に行われるようになった現状は、我々にとって様々な恩恵を与えるものである。また、我々の生活において情報通信端末を通じたインターネット利用が発展することで、いわゆるサイバー空間も公共空間と同等の広がりを有すると解し得る状況となった(5)。しかし、このような情報端末の普及とサイバー空間の拡大は、同時に、いわゆるサイバー犯罪(6)の問題を拡大することにもつながっている。その中でも特に顕著なものが、いわゆるランサムウェアによる被害の拡大である。令和２年度の下半期における被害が21件であったのに対し、令和３年の下半期には85件と１年で４倍以上の被害件数が報告される事態となっている(7)。また、その他のフィッシング詐欺やコンピュータ・電磁的記録対象犯罪も含めた全般的なサイバー犯罪の検挙件数は12275件（暫定値）と、数年前から増加の一途を辿っている(8)。

サイバー空間が我々の実生活との結びつきを強め、それに伴いサイバー犯罪が進展していく現状において、犯罪捜査のあり方もより一層の検討が必要となるものと思われる。ここで重要となるのが、捜査機関による電磁的記録、いわゆるデジタルデータの収集手段である。現行刑事訴訟法においては、基本的に有体物を捜索や差押えの対象としたうえで、法改正により電磁的記録媒体に対する差押え等については別個の規定を設けて対処している。しかし、既に見たようにサイバー空間が公的空間としての広がり

を有していると言える現状において、デジタルデータはより一層の価値を有するようになっているとともに、情報通信技術も日々進歩している状況にある。このような、特にサイバー犯罪をはじめとした情報通信技術を用いたあるいは少なくとも介在させた犯罪の捜査において重要となるデジタルデータを証拠として収集する手法について、本稿は検討を加えるものである。そのために、まずは現行刑事訴訟法におけるデジタルデータの収集に関する法令を確認し、そこにおける問題を指摘する。次に、このような問題についていかなる対応ないし解釈が要求されるかについて、主にアメリカ法の判例や議論を参照し、我が国における捜査機関によるデジタルデータ収集の適正なあり方を論じることとする。

第２章　我が国における捜査機関による デジタルデータ収集の法制

１．現行刑訴法における諸規定について(9)

まず、デジタルデータを捜査機関が収集する場合に適用され得る刑事訴訟法上の諸規定について確認をし、そこにおける問題点を見ていきたい。

デジタルデータについては次のような特徴を挙げることができる。すなわち、①情報記録媒体には事件との関連性の有無に関わらず大量の情報が含まれ得ること、②ディスプレイに表示するなどしなければ可読性がなく、内容を精査することができない、③アクセス権限があれば情報の改変、消去が有体物に比較して容易に行い得ること、である(10)。このような特徴は、従来の有体物に対する捜索、差押えと同様の解釈や規定では対処しきれない面があるため、現行法においては新たな諸規定が制定されるなどしてきた。そのうち、捜査機関が被処分者のデジタルデータを収集する場合に適用され得る代表的なものとして、刑事訴訟法222条１項に基づき準用される110条の２、218条１項前段、218条２項が挙げられる(11)。これらは、平成23年の刑事訴訟法改正によって導入された、電磁的記録媒体

に対する差押え等に関する規定である。それぞれ、110条の２が電磁的記録媒体に対する代替的執行方法について、218条１項前段が記録命令付き差押えについて、218条２項がリモートアクセスについて規定している。

電磁的記録媒体に対する代替的執行方法は、コンピュータ等の記録媒体を差押えるのに代えて、捜査に必要とされる対象情報を他の記録媒体等に複写、印刷、移転[12]した上で差押えるものである。この方法によれば、本来差押えの対象となっていたコンピュータ等の記録媒体に代えて、必要とする情報のみを他の記録媒体に移して取得することができるため、関連しない情報をも同時に取得するという問題を回避することが期待されている。比例原則の観点から、プライバシーをはじめとする諸利益に対してより侵害の程度の低いこのような手法が優先されるべきであると考えられる。しかし、この代替的執行方法は、法文上、本来の差押えの執行方法に常に優先するものではなく、現場の捜査官の判断に委ねられるものであると考えられている[13]。したがって、捜査によって大量の無関連情報が取得される危険性は完全に回避されていない。

次に、記録命令付き差押えであるが、これは、電磁的記録媒体（主にサーバ等）の差押えに代えて、目的とする情報を他の記録媒体に複写、又は印刷させるようプロバイダ等のデータ管理者に命じ、当該記録媒体を差押える処分をいう。これにより、データが記録されている基となっている電磁的記録媒体を差押えることで生じる不利益をデータ管理者が避けることができるようになるとともに、大量の関連しない情報の取得を回避することが期待されている。しかし、記録を命じられるのは、「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」と規定されており、したがって、データを作成した捜査対象者（サーバ等の利用者）ではなく、プロバイダ等のデータ管理者が第一義的な対象となっている。これにより、本来プライバシー等の利益を有する捜査対象者に対する令状呈示等がなされずに、不知の状態でデータが収集されるという問題が生じ得る[14]。

続いて、いわゆるリモートアクセスであるが、これは、差押えの対象となる電磁的記録媒体等によって作成されたデータであって、電気通信回線によって接続されているサーバ等に保存されているものを、当該電磁的記録媒体に複写した上で差押えることをいう。近年では、メールやその他デジタルデータをコンピュータの記録容量ではなく、クラウド等に保存することが広く行われているため(15)、リモートアクセスの有する意義は大きいと思われる。しかし、このリモートアクセスについては、データサーバ等にアクセスするためのパスワード等が判明していなかったため、一旦記録媒体を差押えたうえで、改めて検証令状を得て解析し目的とする情報を取得する、ということは許されていない（法文上は、「複写した上」となっているため、記録媒体の差押えに先立って行われることが要求される）(16)。この点、近年の電磁的記録媒体には強いプロテクトがかけられていることなどから、捜査の現状に適合しない面が既に生じていることが指摘し得る(17)。

以上、まずは現行刑事訴訟法において、特に平成23年の法改正によって導入されたデジタルデータの収集に関する規定を概観してきた。これらの規定の個別の問題については既に指摘した通りであるが、さらに次のような全般的問題点を指摘し得る。

まず、いずれの規定においても、電磁的記録媒体という「有体物」の差押えを前提としている点である。本来、捜索や差押えといった強制処分は、具体的な物の収集に向けられたものであり、これを拡張する形で導入されたのが平成23年改正による諸規定である。したがって、従来の有体物に対する捜索・差押えの理解を前提とする以上このような規定になるのは避けられないものとなる。しかし、「データそのもの」の収集が重視されるとともに、他国では記録媒体の差押えを伴わないデータ収集も可能となっている。その代表的なものとして、ドイツにおけるオンライン捜索（Online-Durchsuchung）が挙げられるであろう。これは、「捜査機関が、被疑者が不知の間、技術手段、特に、その使用する情報技術システム

(informationstechnises System) にインストールされたプログラム（スパイウェア）により、そこに蔵置されているすべてのデータを収集・保全(erheben) すること」と定義される[18]。ドイツ刑訴法100条ｂ以下に規定されており、スパイウェアを通じた直接的なデジタルデータ取得を認めるものである。この手段によれば、プロバイダ等のデータ管理者を介さずに、捜査の対象となる者の有するデータを取得することが可能となる。このような手法に対して、現行法の解釈では対応しきれない。また、アメリカにおいては近年、いわゆるジオフロント令状（またはリバース・ロケーション令状）やキーワード令状が問題とされつつある。これは、特定地域・特定時間に滞留した携帯端末のアカウントを特定し得るプロバイダ等（特に Google が想定されている）に対して位置情報やキーワード検索の態様について開示、取得を求めるものである[19]。このような手法について、我が国では総務省による「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」等においてプロバイダ等の対応が規定されてはいるが、ジオフェンス令状は特定の個人のみならず特定の範囲、時間における位置情報等を包括的に取得するなど、従来の議論とは異なる問題点も生じ得る。この点についても、新たな対応が必要となるであろう。

次に問題となるのが、取得したデータの取り扱いである。すなわち、収集したデジタルデータは一定期間捜査機関において保存されることとなるが、これを他の事件等の捜査に用いることを規制する規定がないことが問題となる。いわゆる取得後の規制の問題である[20]。これまでの捜査に対する法的規制は、主に情報の取得の段階を主な規制の対象としたものであり、その後の利用については十分な関心が払われてこなかった[21]。情報通信技術の発展によって、大量の情報を取得するに際してのコストや容易性といった「障壁」が低下しつつあること[22]、ビッグデータ等の利用、解析によって個人の生活状況等の網羅的把握が可能となり得ること、情報の有する価値それ自体が重視されている現状等を鑑みた場合、取得した情報の利用に関して詳細な規定を設けることが必要であると思われる。この

点において重要となるのが、情報プライバシー権[23]、または自己情報決定権の視点である。被処分者の情報取得とその利用を規制するにあたって、権利解釈から論じ、必要なアーキテクチャ等の在り方を論じることは重要な意義を有すると言える。

このように、具体的な規定において捜査機関によるデジタルデータの収集に対する十分な規制が及んでいないと考えられるが、これに対しては、刑訴法または憲法解釈によってこの間隙を埋めることができるかが問題となる。この点について、次に諸判例を見ていきたい。

2．判例におけるデジタルデータ収集に対する法的対応

情報全般に対する捜査の適法性についてはさまざまな判例の集積が見られるが、その中でも特に、電磁的記録媒体やそこに増置されているデジタルデータの収集に関して重要な意義を有するものとして挙げることができるのが、平成10年最高裁決定[24]及び、下級審判例ではあるが、平成30年９月11日大阪高裁判決[25]であろう。前者はパソコン及びフロッピーディスクの包括的差押えについて、その場で情報を確認していたのでは記録された情報を損壊される恐れがあるとして、適法と解した事例である。後者は、この平成10年最高裁決定の射程が及ぶとしつつ、「電磁的記録に係る記録媒体の差押えにおける差押えの対象は、記録媒体に保存されている個々の電磁的記録ではなく、記録媒体そのものであるから、保存されている情報の中に被疑事実と関連性のある情報が含まれている以上、他に被疑事実と関連性のない情報が保存されていたとしても、当該記録媒体と被疑事実との関連性が否定されるものではない」として、サーバに対するリモートアクセスの上、内容を精査せずにデータを電磁的記録媒体に複写し無関連の情報も含めて包括的に差し押さえた行為につき適法と判断した事例である[26]。これらの判例において共通しているのが、記録媒体の差押えを通じた包括的な情報の収集を許容している、というものである。この点、大阪高裁判決において判示されているように、対象となる情報につい

ては関連性が要求されるところ、差押えの対象となる有体物たる媒体を介することで関連性が推測されるとしている点に問題を見出すことができる。すなわち、パソコンをはじめとする電磁的記録媒体は、そのほとんどが共通の規格によって構成されている以上、それ自体の個性と意義に乏しいものであり、しかも、複数人が管理している場合があるために、捜査対象者のみならず第三者の情報や無関連の情報を大量に取得し得る、というものである(27)。令状請求の段階において情報の特定が困難であることに加え、無関連の情報を大量に取得することが可能である以上、平成10年最高裁決定を前提とした平成30年大阪高裁判決のような理解は支持し得ないものと思われる。

また、情報収集について有体物に対する処分を前提とした理解は、他の最高裁判例においても見出すことができる。それが、いわゆるGPS捜査に対する平成29年最高裁大法廷判決(28)である。本件において最高裁は、GPS端末を取り付けた上で被疑者の位置情報を取得する監視型捜査の適法性を判断するにあたって、動静の継続的、網羅的把握が可能となることで被疑事実と関係のない位置情報を取得し得る点についても言及しているが、より本質的な点は、そのような監視を可能とするGPS端末という機器の取付によって、憲法35条における「住居、書類、財産」に準じた「私的領域」への侵入が構成されるものと解していることにある。位置情報というデータの収集それ自体ではなく、むしろ現実の空間における「侵入」に依拠する判断からは、やはり有体物性を前提とする理解が根付いているものと考えられるとともに、情報プライバシー権への考慮を欠いているものと思われる。そして、そのような有体物性を前提とする理解によっては、無制限に広がり得る情報取得を規制することは極めて困難である。

このように、刑事訴訟法における規定においても、判例の解釈においても、データ収集に対する規制には重大な欠陥があるものと解さざるを得ない。それでは、今後どのようにこの点を乗り越えるべきか。次章では、この問題についてアメリカ法を参照することで若干の検討の素材としたい。

第３章　アメリカにおけるデジタルデータ収集をめぐる議論

１．合衆国連邦最高裁における見解

（１）全般的な理解

まず、個別の諸判例の意義について見ていく前に、前提となる規定及び諸法理について確認をしていく。

アメリカにおいて、捜査機関による被疑者への捜査行為が適法とされるか否かは、主に合衆国憲法修正第４条における「合理的な（reasonable）」捜索（search）、押収（seizure）に当たるか否か、という観点から論じられる(29)。この合理性について、特に重要となるのが、Katz 事件判決(30)において示された「プライバシーの合理的期待（reasonable expectation of privacy）」法理である。このプライバシーの合理的期待法理というのは、社会的に正当とされる（客観的期待）プライバシーの期待を被疑者等が有しているとされる場合（主観的期待）に、捜査機関がその期待に反する捜査行為を行った場合、当該捜査は合衆国憲法修正第４条における「不合理な（unreasonable）」な捜索、押収である、とするものである(31)。このプライバシーの合理的期待法理は、それまで取られていた財産的アプローチ(32)からの転換と評し得るものであり、具体的な物理的侵入の有無によらずに捜査活動の適法性を判断できるようになったため、特に新たな科学技術等を用いて行われる捜査についてより直接的な判断を下せるようになった(33)。

他方で、このプライバシーの合理的期待法理には修正法理もまた存在する。その中でも特に重要なものが、いわゆる「第三者法理（third-party doctrine）」である。これは、政府による情報収集において、情報を保有している主体が自ら、対象となっている情報を通信事業者(34)や銀行(35)といった第三者に移したと言える場合、当該情報に対するプライバシーの期待は失われるとするものである(36)。プライバシーの合理的期待という法理

が抽象的な基準であることは否めず、それに対して一定の制約をかけるものである。したがって、例えば、基地局に送信された携帯電話の位置情報については、この第三者法理の適用が検討され得ることとなる(37)。

このような理解を前提とした上で、次に情報やデータの取得が問題とされた連邦最高裁の事例とその意義について見ていく。

（2）合衆国連邦最高裁諸判例の検討

本稿において特に取り上げる判例は、Jones 事件判決、Riley 事件判決及び Carpenter 事件判決である。これらは、位置情報の取得や携帯電話のデータの取得が問題とされた事例であり、我が国への示唆も多く得られるものである。一方で、全面的に支持し得るかという点については一定の留保が付されるため、次項で特にデータの収集等に関する論考を通じて、さらに我が国における議論への示唆を得たいと思う。なお、これらの判例については、既に我が国においても検討をする論稿が多くあるとともに、紙幅の都合もあるため、判旨において特に重要と思われる点を取り上げていくこととする。

① Jones 事件判決(38)

本件は、約28日間にわたって継続的に行われた自動車への GPS 端末の取付を伴う監視型捜査の適法性が争点となった事例である(39)。本件ではこのような GPS 端末の取付を伴う監視型捜査を違法であると判断したものの、そのアプローチについては、プライバシーの合理的期待法理よりも財産的アプローチに親和性があるものをとっている。すなわち、自動車に GPS 端末を取付けてその動静を監視するのは、情報取得を目的とした私有財産の物理的占有であり、これは合衆国憲法修正第 4 条における「捜索（＝search）」を構成するものである、と判示したのである(40)。このような解釈は、合衆国憲法修正第 4 条の法文の厳格な解釈に基づくものであると思われるが、他方で、これまでのプライバシーの期待法理と異なる解釈を示すものであり、かつ、情報の収集という観点から十分に是認し得ない点があるため、Sotomayor 判事及び Alito 判事の補足意見において批判が加

えられている。そして、この補足意見の中で展開されている、いわゆる「モザイク理論（mosaic theory）」が、特にデータ収集を伴う捜査の規制において重要な意義を有するものと思われる(41)。このモザイク理論とは、情報というピースを組み合わせることによって、一つ一つのプライバシーの侵害性は低いものであっても、総合的に見た場合にプライバシーを侵害し、合衆国憲法修正第4条における不合理な捜索・押収を構成し得るものと考える。

法定意見においても言及されているように、それ自体は大きな価値を有しない位置情報のようなものであっても、大量に収集し解析することによって、個人の思想や信条といったプライバシーの合理的期待に反し得るとの指摘がなされており、これはまさにビッグデータ等の収集が問題とされ得るデジタルデータの収集において意義を有するものであると思われる(42)。

② Riley 事件判決(43)

本件は、逮捕に伴う無令状の差押えとして、スマートフォンや携帯電話を差押えた上で、その場で当該端末に保存されているデータ（写真等）を捜索（search）することが許されるか否かが争われた事例である。本件において連邦最高裁は、スマートフォン等の通信端末が大容量の記憶領域を有するものであり（本件当時の記憶容量は16GB）、これは、「数万ページもの文書、数千枚もの写真、数百本もの映像」を保存することができること、またデータが復元し得ることなども指摘しつつ、このような端末に対する捜索は、情報の収集、解析を通じて個人の私生活を再構成し得ると論じ(44)、本件において捜査官が逮捕に伴い端末の内容を確認した行為を違法であるとした。また、このような捜索（search）(45)を行う場合には、令状を取得する必要があると結論づけている(46)。

このように、本件においてもモザイク理論の語は用いられていないものの、モザイク理論と同様の理に基づいて捜査の適法性を判断している点、重要な意義を有するものと思われる。また、その他に注目すべき点とし

て、情報端末の記録容量の大きさとそれによって大量のデータが保存され得る点への言及、及び、令状が要求されると結論づけている点である。特に、データの収集について令状が有効であるかは検討すべきものである思われる。

③ Carpenter 事件判決[47]

本件でとられた捜査手法は、被疑者の携帯電話と各地の基地局との接続の記録である「基地局位置情報（Cell-Site Location Information, CSLI）」につき、キャリアにこれを提出させ、約127日間にわたる12,898箇所の位置情報を入手した、というものである。したがって、これは端末の取付を伴わない監視型捜査に分類されることとなる。このような監視型捜査の適法性について判断をしたのがこの Carpenter 事件判決である。本件は、さまざまな面において重要な意義を有するものであるが、その中でも特に取り上げるべきは次の点であると思われる。

(a) モザイク理論と同様の判断枠組みに基づくプライバシー侵害性の判断

本件の法定意見においては、Jones 事件判決の補足意見と同様に、モザイク理論と同様の判断枠組みによって CSLI の集積がプライバシー侵害を構成し得るとしている。すなわち、127日間にわたる CSLI の記録は、被疑者等の所在につき包括的に記録をするものであり、このような情報に基づいて動静を確認することは、対象の家族、政治、職業、性に関するつながりを明らかにし得る、と判示している[48]。位置情報という単体では価値の低い情報の集積が人の生活等の総体を明らかにし得る、という点において、よりさまざまな情報を含み得る他のデータの収集、集積がプライバシーの侵害を構成し得ることは自明のことであろう。

(b) 情報収集が技術の介在によって容易になる点

本来、長期間の追跡は、困難でありかつコストもかかるものであったため、これがいわば障害となって一定の制約がかかっていた。しかし、本件のような通信技術を介することによって、ワンクリックするだけで大量の情報を容易、安価、かつ効率的に収集することが可能となっている[49]。

このような技術の介在が従来の捜査手法と新たな態様の捜査手法を分つものであることが、この判示部分から解しうる。

(c) 第三者法理の適用について

本件は、被疑者所有の情報端末から発せられたCSLIという情報を取得するものである。したがって、第三者への情報の披歴とみなし得る状況がある。この点について法廷意見は、先例との類似点は認めつつも、これが大量に取得し得るものであり、情報としての量と質という側面において大きな隔たりがあること、また、必ずしも任意に提供しているものではないことから、この第三者法理の適用について否定している(50)。

以上、概括的にではあるが、データの収集に関連する連邦最高裁の判例について確認をしてきた。これらの判例は、データの収集、集積がプライバシー侵害を構成し得るというモザイク理論の適用可能性について重大な意義を示しているとともに、データの収集に対しては令状によって対処をする方法があり得ること、プロバイダへのデータの送信は、必ずしも第三者法理の適用を意味するものではないことが指摘し得ると思われる。

このような見解に基づきつつ、さらにデータの収集に対する規制のあり方について次項で検討を行っていきたい。

2．デジタルデータの収集に対する法的規制に対する若干の検討

先の諸判例における判示から確認したように、データの収集、集積はもはや有体物の収集とは異なる様相を呈し得るものである(51)。したがって、特に大量の情報を含み得るパソコンやスマートフォンといった電磁的記録媒体の差押えにはより慎重な姿勢が求められるであろう。このような場合には、合衆国憲法修正第4条の解釈に基づき、令状を取得して行うことが必要であろう。

しかし、これは対象となるデータがある程度明らかであり、それを大量に取得する場合に生じる問題、すなわち取得時の問題には対処し得るもの

であるが、例えば令状に基づき適法に電磁的記録媒体を差押えたのちのデータ検索(52)や、大量の情報の取得は伴わないが、ハッキング等によって電磁的記録媒体にアクセスして目的とする情報を取得する場合には十分に対応しきれないという問題が生じ得る(53)。前者においては、適法に媒体が差し押さえられている以上、取得後の令状等による規制が及ばないこと、後者においては、大量の情報取得という視点においてプライバシー侵害を観念しづらい点が指摘し得る。また、これらの捜査手法について我が国の現行法制度に照らして考えた場合、取得後の法的規制がないことから無制限に行われ得るものであり、また他の事件への流用についてはもはや規制が困難であること、後者においては、現実の空間概念を前提としているためにやはり規制が困難であるという問題を指摘し得る。このような問題について、前者の場合には取得後の法的規制を、アーキテクチャ概念等に基づいて行うとともに、強制処分概念を拡張して、令状ではなく立法という法的規制がなければ行い得ないと解することが要求されるものと思われる。また、後者については、平成29年最高裁大法廷判決において示された「私的領域」概念について、サイバー空間の公共的広がりを前提として、記録媒体へのマルウェア等を通じたハッキングもまた、日本国憲法35条における「侵入」を構成し得るものとして、必要な立法的措置によって適正化を図るべきであるものと思われる。

以上、アメリカ法の、特に判例における解釈を通じて我が国に欠けている視点を指摘しつつ、なお残された課題について簡単にではあるが私見を提示したものである。

第4章　おわりに

本稿は、捜査機関によるデジタルデータの収集に対する法的規制について、まずは全般的な検討をおこなったものである。これにより、無対物たるデータを大量に収集、解析することは重大なプライバシー侵害を生じ得

るものであるが、この点について我が国では十分な規制が及んでいないこと、また、データの収集に関しては、従来の理解では対応しきれない問題が生じ得ることから、これに対する簡単な解決策を示すことを試みたものである。今後は、デジタルデータの収集に関して、越境型捜査の問題や、アーキテクチャによる取得後の規制といった各論的問題について検討を重ねていきたいと考える。

注

（1）　総務省「情報通信白書（令和３年版）」50頁参照（https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r03/pdf/n1100000.pdf，最終閲覧日、2022年３月１日）。

（2）　なお、スマートフォンの普及率は、iPhone の日本での販売が始まった2008年以降爆発的に飛躍しており、2010年は調査対象全体の10％程度であったのが、2020年には本文の通り世帯保有率80％を超えるものとなっている。同上、参照。

（3）　経済産業省 商務情報政策局 情報経済課「令和２年度 産業経済研究委託事業（電子商取引に関する市場調査）報告書」11頁（https://www.meti.go.jp/policy/it_policy/statistics/outlook/210730_new_hokokusho.pdf，最終閲覧日、2022年３月28日）。

（4）　なお、本文に示した数値は、我が国における情報通信端末の普及・利用率及び電子商取引に関する数値であるが、純粋に世界的にやり取りされるデータの総量に目を向けてみると、年間約64.2ZB（ゼタバイト）に上るとの推計が、米国の International Data Corporation より発表されている。ZB は、10の21乗 B、即ち10垓 B に換算される。まさに天文学的な情報量が日々やり取りされていることとなる。

See, IDC's report, Data Creation and Replication Will Grow at a Faster Rate than Installed Storage Capacity, According to the IDC Global DataSphere and StorageSphere Forecasts（https://www.idc.com/getdoc.jsp?containerId＝prUS47560321，最終閲覧日、2022年３月29日）.

（5）　サイバー空間がもはや公的空間と同様の広がりを持つものであるという理解は、広く共有されているものであると考えられる。この点、例えば、総合セキュリティ政策会議を引き継いで設置されたサイバーセキュリティ政策会議によって作成された報告書などでも同様の言説がなされている。また、同報告書においては、サイバー空間を公共空間と同等のものと見做

した上で、実生活と同様の安全と安心が確保されるべき旨、指摘されている。

サイバーセキュリティ政策会議「実空間とサイバー空間とが融合したデジタル社会の安全・安心の確保（令和３年12月17日）」３～４頁参照（https://www.npa.go.jp/cybersecurity/pdf/20211217_2.pdf，最終閲覧日、2022年３月29日）。

（６） サイバー犯罪の語については、法律上の明確な定義が与えられているわけではなく、また、学説上も一致した見解があるわけではない。ここでは差し当たり、警察庁が採用している「インターネット等の高度情報通信ネットワークを利用した犯罪やコンピュータ又は電磁的記録を対象とした犯罪等、情報技術を利用した犯罪」を定義としてあげておきたい。このように表現をすれば、対象とする問題の全体を把握することが可能であると考えられる。なお、警察庁が統計として計上している範囲は、①不正アクセス禁止法に規定された不正アクセス。②刑法に規定された不正指令電磁的記録に関する罪及びコンピュータ・電磁的記録対象犯罪、③インターネットを主な手段とした各種の犯罪の総称であるインターネット利用犯罪が挙げられており、これもサイバー犯罪の理解において重要なものであると考えられる。同様の指摘として、中野目善則・四方光「サイバー犯罪の現状と対策研究の意義」同編著『サイバー犯罪対策』４頁（成文堂、2021年）。

また、類語としてコンピュータ犯罪やハイテク犯罪などが我が国において用いられてきたが、欧州評議会によって起草されたサイバー犯罪条約の批准がなされたことなどもあって、基本的には、コンピュータや情報通信技術を用いた、あるいはそれを対象とした犯罪をサイバー犯罪として呼ぶことが定着しているものと思われる。このようなサイバー犯罪をめぐる社会的変化や語の変遷について、安富潔「情報化社会における刑事立法の役割：コンピュータ犯罪からサイバー犯罪へ」慶應法学42号（2019年）382～383頁参照。

（７） 警察庁「令和３年におけるサイバー空間をめぐる脅威の情勢等について（速報版）」３頁参照（https://www.npa.go.jp/publications/statistics/cybersecurity/data/R03_cyber_jousei_sokuhou.pdf，最終閲覧日、2022年３月28日）。

（８） 同上、８頁。

（９） 以下の議論について、前掲注（５）中村真利子「サイバー犯罪捜査」150頁以下も参照している。

(10)　寺崎嘉博『刑事訴訟法〔第３版〕』（成文堂、2013年）155頁。なお、同様の指摘として、滝沢誠「ドイツにおけるオンライン捜索について」山口厚ほか編『寺崎嘉博先生古稀祝賀論文集〔上巻〕』（成文堂、2021年）179頁。

(11)　その他、被処分者への協力要請（222条１項、111条の２）、プロバイダ等への保全要請（197条３項）等も挙げられるが、本稿は主として被処分者に対して捜査機関が直接デジタルデータを収集し得る場面を対象として論じるものであるため、これらの規定についてはあくまで注に挙げるにとどめる。

(12)　複写・印刷・移転はそれぞれ類似した性質を有するものである。しかし、複写は目的とするデータを他の記録媒体にいわゆるコピー・ペーストをすること、印刷はデータを紙媒体にプリントアウトすること、移転は目的とするデータを他の記録媒体に複写した後、元となったデータを保存元の情報記録媒体から削除すること、とそれぞれ定義されている。後藤昭・白取祐司編『新・コンメンタール刑事訴訟法〔第３版〕』（日本評論社、2018年）249～250頁参照。

(13)　同上。

(14)　同上、233頁。

(15)　クラウドについては、「共有化されたコンピュータリソース（サーバ、ストレージ、アプリケーション）などについて、利用者の要求に応じて適宜・適切に配分し、ネットワークを通じて提供することを可能とする情報処理形態」として理解されている。

経済産業省「クラウドサービス利用のための情報セキュリティマネジメントガイドライン（2013年度版）」８頁参照

（https://www.meti.go.jp/policy/netsecurity/downloadfiles/cloudsec2013fy.pdf，最終閲覧日、2022年３月29日）。

クラウドサービスの利用率について、企業による割合ではあるが、約70％の企業がクラウドサービスを利用している（前掲注（１）313～314頁参照）。クラウドにデータを保存することはセキュリティの面でメリットがあること、Apple や Google、Microsoft といったクラウドサービスを提供する企業が増えていること、保存し得る情報の容量も増加していることなど、コロナ禍によってリモートワークが推進されていることから鑑みると、今後も個人、企業の需要は高まり、捜査における重要性はさらに増していくものと思われる。

(16)　同旨の判断を示すものとして、東京高判平成28年12月７日高刑集69巻

2号5頁参照。また、同様の指摘として、前掲注（6）島田健一「デジタルデータの証拠法」184頁参照。

(17)　前掲注（11）、551頁。

その他、本文に挙げた問題以外に、遠隔地にあるサーバと差押え対象たる記録媒体を一体のものとして捉えることは、令状における記載の要件の観点から困難であること、認証情報が一般に要求されるものである以上、クラウドのデータに対する現行法の規定のようなリモートアクセスは想定することが困難であることが指摘され得る。このようなリモートアクセスに関する全般的な問題について、早乙女宜宏「リモートアクセスによる差押えに伴う問題点の一考察」日本大学法科大学院「法務研究」第16号（2019年）61頁、70-71頁参照。

また、サーバ等については必ずしも日本国内に設置されているわけではないため、外国主権との国際捜査共助等の問題も生じ得る。この点について判断したものとして、最二小決令和3年2月1日刑集75巻2号123頁。本件において最高裁は、「刑訴法が、（中略）日本国内にある記録媒体を対象とするリモートアクセス等のみを想定しているとは解されず、電磁的記録を保管した記録媒体が（サイバー犯罪に関する条約）の締約国に所在し、同記録を開示する正当な権限を有する者の合法的かつ任意の同意がある場合に、国際捜査共助によることなく同記録媒体へのリモートアクセス及び同記録の複写を行うことは許されると解すべきである」と判示している。

(18)　この定義は、滝沢、前掲注（10）180頁を参照したものである。

(19)　我が国においてジオフェンス令状について論じた先駆的論考として、指宿信「スマホ位置情報の「一網打尽」捜査：「ジオフェンス令状」の正体」世界952号（2022年）52-61頁。

See, also Note: *Geofence Warrants and the Fource Amendment*, 134 Harv.L.Rev. 2508 (2021).

ジオフェンス令状が実際に問題とされた事例においては、特定の日時において端末からサーバに送信されて保存されていた位置情報をジオフェンス令状によって取得し、周辺で発生した強盗事件の被疑者を割り出すといった手法が取られている。この場合において、位置情報を取得したことについて被疑者には通知されておらず、突如としてGoogleから7日以内に裁判所に出廷するよう求められたこと、また、実際には冤罪であったことが問題とされた。

この点について想起されるのが、カフカの『審判』である。主人公は、突如として見知らぬ男たちにその身柄を拘束され、自身の様々な欲望を暴

露されていくこととなる。これは、当時はあくまでフィクションとして捉えられていたが、繊細なプライバシー情報を大量に持ち歩くことが可能となり、また端末がサーバ等と電気通信回線を通じて継続的に通信をしている現代においては決して夢物語とは言い切れない状況となっている。

(20)　山本龍彦『プライバシーの権利を考える』（信山社、2018年）67頁以下。

(21)　同上、76頁以下。

(22)　笹倉宏紀「捜査法の体系と情報プライヴァシー」刑法雑誌55巻３号（2016年）425頁。

(23)　この点、捜査法の分野においては情報プライバシー権という概念が十分に受容しきれていないことが指摘されている。同上、424頁以下参照。

(24)　最二小決平成10年５月１日刑集52巻４号275頁。

(25)　大阪高判平成30年９月11日高裁刑事裁判速報平成30年11号。

(26)　平成30年大阪高裁判決の事例において、サーバはアメリカに存在していたため、このような外国に設置されているサーバに対するリモートアクセスの適法性も争点となっている。この点に対する上告審が、前掲注（17）の令和３年最高裁決定である。このような外国主権との関係におけるリモートアクセスの問題については、また別稿にて論じたい。

なお、このような越境型リモートアクセスの問題について論じるものとして、前掲注（８）163-166頁、川出敏裕「コンピュータネットワークと越境捜査」後藤昭ほか編『井上正仁先生古稀祝賀論文集』（有斐閣、2019年）409頁以下など。

(27)　島田、前掲注（15）171頁。

(28)　最判平成29年３月15日刑集第71巻３号13頁。

(29)　合衆国憲法修正第４条は、次のように規定している。

「不合理な捜索及び押収に対して、身体、住居、書類、及び所持品についての安全を保障される人民の権利は、侵害されてはならない。また、宣誓又は確約によって支持された相当な理由に基づき、且つ捜索される場所及び逮捕される人又は押収される物について明示していない限り、令状は発付されてはならない」。

なお、search と seizure の語については、日本における捜索、押収と重なり合う部分もあるが、必ずしも同一の概念であるとは言えない（search には検証としての性質を有するものが含まれ得る。また、seizure には身体の拘束の意味も含まれる）。しかし、ここでは便宜上 search を捜索、seizure を押収として訳出をする。

(30) Katz v. United States, 389 U.S.347 (1967).

(31) *Id*, at 360.

(32) Katz 事件判決以前は、特に Olmstead 事件判決（Olmstead v. United States, 277 U.S. 438［1928］）及び Goldman 事件判決（Goldman v. United States, 316 U.S. 129［1942］）によって、財産権への侵入の有無によって捜査行為の合理性が判断されていた。

See, also Harry Henderson, *Privacy in the Information Age*（1999）66 etc.

(33) ただし、プライバシーの合理的期待が必ずしもそれ以前の財産権的アプローチからの転換を図ったものではなく、むしろその基本的な枠組みについては同一であるとする見方もある。Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and The Case for Caution*, 102 Mich. L. Rev 801, at 815-816 (2004). また、この点について検討する邦語文献として、稲谷龍彦『捜査手続におけるプライバシー保護』（弘文堂、2017年）194頁以下。

(34) Smith v. Maryland, 442 U.S. 735 (1979).

(35) United States v. Miller, 425 U.S. 435 (1976); United States v. Graham, 824 F.3d 421 (4th Cir. 2016).

(36) Orin S. Kerr, *The case for Third-Party Doctrine*, 107 Mich. L. Rev. 561, 563-564 (2009).

なお、学説においては、全面的に支持されているわけではなく、被疑者等のプライバシーについてより柔軟な解釈をすべきであるといった批判などが加えられている。See, Richard A. Epstein, *Privacy and the Third Hand: Lessons from the Common Law of Reasonable Expectations*, 24 Berkley Tech. L. J. 1199 (2009) ; Daniel J. Solove, *Understanding Privacy* at 103-106 (2008) etc.

(37) しかし、連邦最高裁はこのような事例においては、以下の判例に見るように、必ずしも第三者法理に肯定的な姿勢を示してはいない。

(38) United States vs. Jones, 565 U.S. 400 (2012).

(39) この点、我が国の平成29年最高裁大法廷判決にも影響を与えていることが、最高裁調査官による解説などからも明らかである。

(40) *Id* at 404-405.

(41) 補足意見においてはモザイク理論との語は用いられていないものの、その理はモザイク理論と同様のものであると言える。このように考える邦語文献として、指宿信「アメリカにおける GPS 利用捜査と事前規制」季刊

刑事弁護85号（2016年）91-92頁参照。

(42)　*Supra note* 38 at 415.

(43)　Riley v. California, 573 U S. 373 (2014).

(44)　*Id* at 394-397.

(45)　本件においては、端末の内容を確認する行為を「捜索（search)」として論じているが、情報の取得を「押収（seizure)」として解する見解もある。See, Orin S. Kerr, *Fourth Amendment Seizures of Computer Data*, 119 Yale L.J 700, at 702 (2010)

(46)　*Id* at 403.

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

(48)　*Id* at 2217-2218.

(49)　*Id* at 2218.

(50)　*Id* at 2219-2220.

(51)　この点についてSoloveは、データの収集が「aggregation（集約)」と呼ばれる新たな問題が生じ得るものと指摘している。これは、データを収集し解析することによって、単なる総体よりもより大きな情報を得ることができるとするものである。データを組み合わせて解析することで、様々な側面からの情報を得られることを端的に表しており、まさにこの点においてデータの収集の問題が生じ得るものであると思われる。

See, Daniel J. Solove, *Digital Dossers and the Dissipation of Fourth Amendment Privacy*, 75. S. Cal. L. Rev. 1083, 1157 (2002).

(52)　Emily Barman, *When Database Queries are Fourth Amendment Search*, 102 Minn. L. Rev. 577, 578 (2017).

(53)　Jonathan Mayer, *Government Hacking*, 127 Yale. L. J.570, 576-577 (2018).