情報通信技術の発展における犯罪捜査の課題

中　島　洋　樹

目次

1．はじめに

1949年に現行刑事訴訟法が施行されて75年が経過しようとしている。その間、急激な速度で遂げられた科学技術の発達は、我々の社会や生活態様に大きな変化をもたらした。とりわけ、コンピュータや情報通信技術の発展によって、1980年代頃からコンピュータの利用は、企業や組織のみならず個人のレベルまで普及し、情報の取り扱いやその保管方法に関して紙媒体から電磁的記録媒体への移行が進んだ。さらに、LAN やインターネット等のネットワーク構築が進むなか、とりわけ1990年代からインターネットが加速度的に普及し、多くのインターネット・サービス・プロバイダ（以下、ISP）が設立され、苛烈な競争の下に通信回線の拡充と高速化が実現されていったことによって、日常的にインターネットを利用可能な環境が整備されてきた。また、端末からインターネットを経由してサーバやストレージ等のコンピュータ資源を利用するクラウド・コンピューティングの発達・普及により、インターネットを介して提供されるサービスは Web サイトの表示やファイルの送受信に止まらず、多様で複雑・高度なオンライン・サービスが提供されるようになった。他方で、インターネットにアクセスするた

めの装置（クライアント端末）に関しても、従来、自宅等に据え置かれるパーソナル・コンピュータ（以下、PC）が主に利用されていたところ、ノート型 PC などコンピュータの小型化が進み、携行が可能になった。さらに、2000年代頃から携帯電話やスマートフォン等の携帯型端末が高機能化し、電話通信機能に加えてインターネットへのアクセス機能を担うようになった。

いまや、2022年のわが国の情報通信機器の世帯保有率は、モバイル端末全体が97.5%、スマートフォンが90.1%、PC が69.0%であり、インターネット利用率（個人）は84.9%に上る[1)]。大多数の者がこれらの携帯型端末を所有することにより、インターネットへのアクセスは情報の発信・受け取り・共有、オンライン・サービスの享受、他者とのコミュニケーションなど、必要不可欠な日常生活の一部となり、コンピュータとネットワークを介した電子情報のやり取りで形成される空間ないし領域は、もはや社会インフラ化を遂げたといえよう。今や、「サイバー空間は、地域や老若男女を問わず、全国民が参加し、重要な社会経済活動が営まれる公共空間へと変貌を遂げ、金融、航空、鉄道、医療等といった国民生活や社会経済活動を支える基盤となる機能から、警察や防衛といった治安や安全保障にかかわる国家機能に至るまで、あらゆる場面で実空間とサイバー空間が融合した社会の到来が現実となりつつある[2)]」と論じられるに至っている。

このような情報通信技術の急速な発展と高度な情報化社会の到来は、犯罪の形態や手法にも大きな影響を与えることになり、犯行の匿名性・不特定多数性、組織化、広域化・国際化、犯罪被害の拡散傾向、犯罪遂行手段の複雑化・専門化などをもたらした。これに伴い、コンピュータや情報通信技術を駆使したこれまでにない態様・方法による法益侵害行為を従来の犯罪類型に取り込み、あるいは、

1）総務省「情報通信白書［令和５年版］」〈https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r05/pdf/n4b00000.pdf〉（閲覧日：2023年７月20日）137頁以下参照。

2）警察庁「令和４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」〈https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_cyber_jousei.pdf〉（閲覧日：2023年７月１日）1頁参照。

全く新しい犯罪として規制する必要が生じてきた。そして、犯罪捜査においても電子データという無体情報を証拠化することの重要性が増し、むしろその取得は必至となっている[3)]。

2．情報通信技術の発展による刑事司法への影響

（1） 刑事的規制の動向

電磁的記録媒体への情報保存の普及、コンピュータや情報通信技術を利用した業務やサービス提供の増加は、電磁的記録を文書と同様の社会生活基盤として扱うことを要請し、大量かつ迅速な処理を可能とする電子計算機による業務を加重した法定刑により保護し、従来の詐欺罪では捕捉しきない電子計算機による不法な財産上の利得行為を補充的に処罰するなどの立法をもたらした。1987年［昭和62年］の刑法改正では、電磁的記録不正作出・供用（刑法161条の２）、電子計算機損壊等による業務妨害（同234条の２）、電子計算機使用詐欺（同246条の２）が規定された。また、公正証書原本不実記載等・行使（同157条、158条）につき、原本として用いられる電磁的記録への不実記載が追加され、公用文書毀棄（同258条）・私用文書毀棄（同259条）の客体にも電磁的記録が追加された。さらに、2001年［平成13年］改正により、支払用カード電磁的記録に関する不正作出等（刑法163条の２）、不正作出カード所持（同163条の３）、不正作出準備（同163条の４）が規定された。

そして、ネットワークの社会生活基盤としての重要性から、その秩序の維持を目的とする立法が求められた。これまで「ハッキング」や「なりすまし」は規制の対象となっておらず、上述の犯罪等を目的とする手段として関連する場合を除いて犯罪捜査の対象となることはなかったが、上記行為等によるコンピュータ・

3）例えば、スマートフォンに記録された情報から、使用や操作に紐付いたタイムスタンプや位置情報等を解析することにより、相当程度に使用者の行動を把握することも可能である。

ネットワークを介したシステムへの侵入自体が犯罪化されることになる。2000年［平成12年］に施行された不正アクセス行為の禁止等に関する法律（不正アクセス禁止法）により、不正アクセス行為[4]、他人の識別符号を不正に取得する行為、他人の識別符号を管理権者・利用者以外の者へ提供する行為（不正アクセス行為を助長する行為）、不正に取得された他人の識別符号を保管する行為、識別符号の入力を不正に要求する行為につき刑罰が設けられた。2011年［平成23年］の「情報処理の高度化等に対処するための刑法等の一部を改正する法律」では、不正指令電磁的記録に関する罪（刑法168条の２、同168条の３）および電子計算機損壊等業務妨害の未遂処罰（同234条の２第２項）が新設された。また、わいせつ物頒布等（同175条）のわいせつ物に電磁的記録に係る記録媒体が加えられ、電磁的記録その他の記録の電気通信による送信も同罪の頒布と位置づけられることとなった。

他方、インターネット・オークション詐欺等に見られるような、インターネット上に構築されているサービス提供システムを利用した詐欺、インターネットを介した児童ポルノ法違反、著作権法違反等の「その他犯罪遂行に不可欠な手段として高度情報通信ネットワークを利用する犯罪（インターネット利用犯罪）」[5]も増加の一途を辿っており、これらのサイバー犯罪に対する規制が進められてきている。また、サイバー犯罪には分類されない一般的な犯罪についても、その実現のための計画・立案、共犯者間の連絡、実行等、犯罪遂行のあらゆる過程において、スマートフォン、PC、電子メール、SNS 等が当たり前に利用されており、むしろ通常化している状況である。現代において、インターネットの利用は、犯

4）他人の識別符号（ID・パスワード等）を無断で入力すること（不正アクセス禁止法２条４項１号）、セキュリティ・ホールの攻撃などコンピュータの利用を制限するためのアクセス制御機能を担うプログラムの不備を衝く情報や指令を入力してアクセス制限を免れること（同項２号、３号）により、アクセス権限のないコンピュータを利用する行為と定義される。

5）統計上、「サイバー犯罪」は、この「インターネット利用犯罪」と、「不正アクセス禁止法違反」、「コンピュータ・電磁的記録対象犯罪、不正指令電磁的記録に関する罪」の３つのカテゴリに分類されている。警察庁・前掲注２）28頁参照。

罪遂行の各局面における一般的で至極ありふれた行為ということができよう。

（2） 犯罪捜査への影響

これらの犯罪の解明のためには、PC やスマートフォン等の端末に作成・保存されたファイル、メール、メッセージ等のデータ、インターネットの閲覧履歴や検索履歴、端末の位置情報、クライアント―サーバ間のアクセス・ログ等が重要な意味を持つ。これらの電磁的記録を証拠として取得するためには、保存されている PC やスマートフォン等の端末自体を捜索により発見し、差押えの後、保存されているデータを解析するという捜査手法により可能である。しかしながら、このような従来的な証拠収集方法であっても、後述するように、電子データの不可視性・不可読性、記録媒体の記録容量の増加に伴い、差押えの執行における被疑事実との関連性の確認が要請されることとの関係で、非常に困難な問題を抱えてきた[6)]。セキュリティや暗号化の技術も多様化し、パスワード認証の他に指紋認証、顔認証も実用化されており、さらに、これらを組み合わせて複雑化・多段階化されている。PC や記録媒体等のセキュリティを解除し、暗号化された電子データを復号化するために、高度な専門的技術が求められると同時に、電子データの証拠化に関して実効性を確保し得る処分の法的根拠や規律についても検討する必要がある。

また、捜査対象となる電子データがネットワーク上のサーバに保存されており、そこにアクセスする PC やスマートフォン等のクライアント端末の記録領域には対象データが存在しないことがある。この場合、当該端末を差し押さえても捜査目的は達せられない。例えば、PC 等の端末にインストールされたメールソフト上のメールデータや送受信記録を取得したければ、当該 PC 等を差し押さえるという従来の手法によって実現可能である。しかし、例えばインターネットブ

6）関連する裁判例として、大阪高判平成３・11・６判例タイムズ796号264頁、最判平成９・３・28判時1608号43頁、最決平成10・５・１決定刑集52巻４号275頁などがある。

ラウザ上で利用するWebメールサービスは、典型的なサービスとしては、ブラウザに表示される画面上でインターネット通信を介してメール・サーバにアクセスし、サーバに保管されているメール・データをブラウザ画面に表示して閲覧するサービスである。このサービスを利用してメールを送受信するとき、メール閲覧時にその都度メールサーバにアクセスして画面上に表示させているだけであり、クライアント端末の記録領域に送受信されたメール・データは保存されていない。この場合電子メールによるやりとりの内容を確認して証拠として保全するためには、端末を物理的に差し押さえるだけでは意味がなく、サービス利用者のメール・データを記録しているメール・サーバを捜査対象とする必要がある。しかし、対象データが当該サーバに存在する蓋然性が認められたとしても、対象データを証拠として保全するために当該サーバそのものを差押え対象とするには大きな問題が伴う。従来、電磁的記録は、情報容量が通常の文書と比較にならないほど膨大であり、対象データがその中の一部に過ぎない場合に、PC等や記録媒体の差押えによる被処分者の不利益（当該PC、記録媒体が利用できない、関連性のないデータに関するプライバシー侵害等）が過大であることが問題となってきた。そのような不利益を回避するために、捜索・差押えの現場において、データを選別してプリントアウトや記録媒体に出力させるなどの措置を刑訴法111条の「必要な処分」として行うことが考えられるが、それが可能でない場合は、データが保存されていた記録媒体やPCそのものを差し押さえるしかない。そして、サーバを差押え対象とする場合は、物理的・技術的な問題をひとまず措くとしても、他に莫大な数のサービス利用者が存在していることから、差押えによって惹起される不利益は、単なる個人使用のPC等を差し押える場合の比ではない。

さらに、クラウド・サーバの場合は、データを分割し、複数のサーバに分散して保存することにより、耐障害性を高め冗長性を確保してデータ欠損への保険としたり、アクセス速度を高めたりしている。すなわち、捜査対象とすべき1つのデータが細分化されて、複数サーバに分散して保存されている可能性があるのである。また、これら複数のサーバが同じ施設内に設置されているとは限らず、世

界各所に分散して設置されている可能性もある。それゆえ、ネットワーク上は対象データにアクセスすることが容易であっても、それらが保存されている多数のサーバを位置的・物理的な観点から特定することは極めて困難である。また、捜査対象となるデータが保存されたサーバが国外にある場合や、サーバの所在地が不明である場合には主権侵害の問題も生じうる。

このように、情報通信技術の飛躍的な進歩によって、これまで想定されていなかった犯罪の痕跡、つまり、新たな形態の証拠を発見・収集する必要が大きくなるとともに、他方において、捜査活動自体に関しても、現行刑事訴訟法上想定されていなかった証拠・情報収集の手法が技術的に可能な状況となった。捜査において、電磁的記録というそれ自体は無体物である情報を正面から取り扱う必要性に直面し、それに対応するための捜査手法および規律の在り方が問われるようになった。従来、電磁的記録媒体の捜索・差押えといった限定的な場面において、その不可視性・不可読性、証拠隠滅の容易性、選別・特定の困難性という特殊な性質がクローズアップされ、ともすればアドホックに論じられてきた問題状況から、電磁的記録を証拠として収集することの常態化と情報通信技術の発展によって、捜査対象とすべき範囲が物理的な軛を超えて拡張するにつれ、従来の捜査手法が抱えてきた根本的な限界が浮き彫りになり、基本原則からの見直しが迫られるほどに逼迫した状況へと展開した。電磁的記録を対象とする新たな捜査手法の創設が喫緊の課題とされたのである。

（3） 刑事訴訟法改正による対応

このように、サイバー犯罪への刑事規制強化に迫られる状況の下、2001年に欧州評議会において採択され、日本も署名したサイバー犯罪条約への批准に向けた国内法の整備のために、2003年、法制審議会に対して「ハイテク犯罪に対処するための刑事法の整備に関する諮問」がなされ、同審議会の答申を基に「犯罪の国際化及び組織化並びに情報処理の高度化に対処するための刑法等の一部を改正する法律案」が国会に提出された。しかしながら、共謀罪の新設も含めた同法案に

対する批判は大きく、継続審議ののち、法案上程すらなくなり、「情報処理の高度化等に対処するための刑法等の一部を改正する法律」として結実したのは2011年であった[7]。

同法は、刑事訴訟法を改正し、①記録命令付差押え：電磁的記録を保管する者その他利用する権限を有する者[8]に命じて、電磁的記録を記録媒体に記録または印刷させてそれを差し押さえる処分（刑訴法99条の２、同218条１項、同222条１項）、②リモートアクセスによる電磁的記録の差押え：差押えの対象となっている電子計算機と通信回線で接続されている記録媒体[9]から、当該電子計算機または他の記録媒体に電磁的記録を複写したうえで、それらを差し押さえる処分（同99条２項、同222条１項、同218条２項）、③電磁的記録の複写等による差押え：差押え対象である記録媒体から電磁的記録を他の記録媒体に複写・印刷・移転させ、後者の記録媒体を差し押さえる処分（同110条の２、同222条１項）、④被処分者への協力要請：電磁的記録媒体の差押えの被処分者に対して、電子計算機の操作その他の必要な協力の要請（同111条の２、同222条１項）等、電磁的記録に関連する新たな捜査手法を新設した[10]。

7）立法の経緯について、指宿信『電脳空間と刑事手続』（2022年、成文堂）207頁以下を参照。

8）保管者とは、捜査対象とすべきデータが記録されている記録媒体を所持しているなど自己の実力支配内に置いている者、利用権限者とは、適法に、捜査対象とすべきデータが記録されている記録媒体にアクセスして当該電磁的記録を利用することができる者を意味する。後者は、排他的管理権限を有する必要はない。杉山＝吉田・後掲注10）75頁。

9）リモート・アクセスの対象となる記録媒体は、差押え対象である「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」と規定されている。

10）本法改正および新しい処分に関する論考として、池田公博「電子的記録を含む証拠の収集・保全に向けた手続の整備」ジュリスト1431号（2011年）78頁、壇上弘文「サイバー関係をめぐる刑事訴訟法の一部改正について」刑事法ジャーナル30号（2011年）37頁、杉山徳明＝吉田雅之「『情報処理の高度化等に対処するための刑法等の一部を改正する法律』について（下）」法曹時報64巻５号（2012年）101頁、笹倉宏紀「サイバー空間の捜査」法学教室446号（2017年）31頁、笹倉宏紀「クラウド捜査」芝原邦爾ほか編『経済刑法―実務と理論』（2017年、商事法務）564頁、北村篤「デジタル情報と捜査：検察の立場から」三井誠ほか編『刑事手続 ↗

高度にコンピュータ・ネットワークが発達した現代社会において電磁的記録を捜査対象とする場合、従来の捜査方法に従い、対象データが保存されている記録媒体自体を特定して差し押さえるやり方では、ネットワーク上の複数サーバに分散して保存されたデータを証拠保全するために個々のサーバの所在を特定したうえでこれらを差し押さえなければならない。そのためには、電磁的記録や情報通信技術に関して高度の専門性が要求されるという技術的問題と各サーバに対して差押え手続を執らなければならないという現実的な困難が伴う。また、被処分者に対しても、当該サーバ等の記録媒体を利用する業務に著しい支障が生じるという大きな不利益を受忍させなければならないことになる。そこで、本改正では、捜査に必要な電磁的記録が保存されている記録媒体自体を差し押さえることなく、その電磁的記録の内容を証拠化する新たな態様の差押え規定が設けられている。

まず、刑訴法110条の２等において他の記録媒体への複写や紙媒体への印刷といういわば代替的な差押えともいうべき執行方法が規定された[11)]。この新たな執行方法は、電磁的記録という実体を有しない情報そのものを証拠化して収集する捜査目的を遂行するために、その特質に適った差押えの態様であるといえる。これにより、対象データが保存されているPC、スマートフォン、サーバ等の記録媒体自体を差し押さえることに伴う被処分者が受ける不利益を回避することがで

↘の新展開（上）』（2017年、成文堂）415頁、山下幸夫「デジタル情報と捜査：弁護の立場から―コメント１」三井誠ほか編『刑事手続の新展開（上）』（2017年、成文堂）429頁、島戸純「デジタル情報と捜査：裁判の立場から―コメント２」三井誠ほか編『刑事手続の新展開（上）』（2017年、成文堂）437頁、川出敏裕『刑事手続法の論点』（2019年、立花書房）97頁、山名京子「捜査手続におけるリモートアクセス」『研究叢書第61冊　証拠の収集と保管Ⅱ』（2020年、関西大学法学研究所）１頁、指宿・前掲注７）207頁等を参照。

11）改正以前においても、事前に被処分者の協力が得られれば、対象データを複写または印刷させた記録媒体ないし紙媒体を差し押さえることができた。また、刑訴法111条２項の「必要な処分」として、差し押さえた記録媒体から対象データを複写・印刷したのち、記録媒体を直ちに還付することが考えられる。しかしながら、後者の場合は、データを移転することはできないし、差押え後に行われる処分を差押えに「必要な処分」とすることができるかは疑問である。杉山＝吉田・前掲注10）57頁。

きる。この新たな態様の執行方法は、必要な電子データが保存されていた元の記録媒体とは別の媒体に当該データを複写することにより取得するという処分態様であることから、記録媒体保管者または利用権限者に必要な電子データを記録媒体に記録・印刷させてそれを差し押さえる記録命令付き差押えや、ネットワークを介して接続される記録媒体から必要な電子データを複写して差押えるリモートアクセスによる差押えの基本形というべき執行方法である。

記録命令付き差押えによって、被処分者である管理者または利用権限者が協力的な場合には、これらの者に捜査に必要なデータを選別・複写して作成させた記録媒体を差し押さえることができ、捜査機関が自ら遂行することに伴う困難や被処分者が受ける不利益を回避しうる[12)]。また、リモートアクセスによる差押えにより、差押え対象となっている電子計算機（PC、スマートフォン等の端末）とネットワークを介して接続可能な記録媒体（Web メール・サーバ、クラウド・サーバ等における個々のサービス利用者に割り当てられた使用・記録のための領域）にアクセスして捜査の対象となっているデータを探し出し、当該 PC や他の記録媒体にダウンロード（複写）して差し押えることが可能になった。このことは、被疑事実に関連すると思料される PC やスマートフォン等を差し押さえても、その端末自体の記録領域に対象データが存在しないという事態、すなわち捜索・差押えの空振りを回避できるだけでなく、外部のネットワーク上に存在する捜査対象データを取得するために、差押え対象物である PC 等の端末のアクセスログ等からサーバ等の所在を特定して物理的に差し押さえる必要がないことを意味する。このように捜査の効率性と被処分者が受ける不利益の縮小を図りながら電磁的記録に関する差押えに関する法整備が進められたのである。しかしなが

12）このような執行の態様は、法改正以前においても、例えば、ISP 等の第三者的地位にある事業者等、比較的協力を得られそうな被処分者の場合には、事前打ち合わせにおいて選別作業と必要なデータの作成を要請し、それを差し押さえるという実務が行われていた。杉山＝吉田・前掲注10）59頁。本改正により令状発付に伴い生じる法的義務が明文化され、捜査機関からの要請と秘密保持義務との間で板挟みになる被処分者の協力が得られやすくなる。

ら、有体物を差し押さえるという従来の処分態様を維持しながら、その枠組みを前提に電子データの複写という処分を組み込んでおり、被処分者の権利保障や電子データを取得する処分としての実効性について検討する余地がある。

3．電磁的記録媒体の差押えにおける「被疑事実との関連性」

（1） 有体物の不可分性に起因する問題

従来から、差押えの対象は有体物に限定されると考えられており、コンピュータに記録されている電子データそのものは有体物ではないので差押えの対象にはならず、それが保存された電磁的記録媒体やプリントアウトされた文書という有体物の形態になっていれば、それらが差押えの対象とされてきた[13]。この点に関して、電子データそれ自体には可視性・可読性がなく、コンピュータやソフトウェア等より出力されることにより証拠としての意味を持つことから、「電磁的記録の捜索・差押えで対象となるのは、実質的には、コンピュータや電磁的記録媒体そのものではなく、『無体情報』としての『電磁的記録』それ自体である」として、記録媒体やプリントアウト等の有体物に化体することをもって有体物と一体的にとらえて捜索・差押えの対象としうるとする見解もある[14]。この見解を前提にすれば、記録媒体を差し押さえることに処分の実質があるわけではなく、必要な電子データを取得する処分といえる。それゆえ、その内容にとどまらず当該電子データに関連する外部的・付随的情報（当該電子データを含む記録領域の使用状況、作成・変更・消去等のログ等）や記録媒体の状態そのものに証拠価値を有する場合は格別、その処分の態様は、当該電子データを他の媒体へ複写してそれを差し押えるか、プリントアウトした紙媒体の差押えが原則であるという考え方も採り得るだろう。しかしながら、このような見解に対しては、可視性・可

13）田宮裕『刑事訴訟法［新版］』（1996年、有斐閣）102頁、107頁。
14）安富潔『ハイテク犯罪と刑事手続』（2000年、慶應義塾大学出版会）163頁以下参照。

読性がなく一定の情報処理を介することにより内容を認識し得るのは、外国語・暗号等による文書や録音・録画を内容とする磁気テープでも同様であり、電磁的記録媒体に限って押収対象物を無体情報と観念するのは理論的に一貫しない[15]、記録媒体自体の証拠物としての側面を看過しており一面的に過ぎる[16]などの批判があり、刑事訴訟法99条１項の「証拠物又は没収すべき物」の解釈から、物理的に管理可能な有体物を差押えの対象とするのが一般的な理解である。それに従い、記録媒体を差押え対象と考える場合、当該記録媒体と被疑事実との関連性の確認において、その内容である各電子データに対する権利侵害に関して、記録媒体ひいては有体物の不可分性に起因する問題が生じ得る。

電磁的記録媒体には被疑事実と関連性のないデータも大量に記録されていることが考え得るが、日記や帳簿など通常の文書を差し押さえる場合と同様、被疑事実に関連するデータを含む蓋然性が認められるのであれば、相当な理由や特定性は肯定できると解されてきた[17]。しかし、電磁的記録媒体が有する膨大な記録容量に鑑みると、とりわけ被処分者が被疑事実とは無関係な第三者の場合、記録媒体の差押えは、そこに保存されている被疑事実とは無関係な大量のデータが差し押さえられることによるプライバシー侵害だけでなく、当該記録媒体の利用が妨げられることにより被処分者の業務等に支障を生じさせる事態を惹起することも考えられる。第三者に対してそのように過大な不利益を受忍させることに関して、相当性の観点から疑問が生じる場合はあり得るだろう。これに関連して、東京地裁平成10年２月27日決定[18]は、顧客データ差押えの取消しを求める準抗告の

15）的場純男「コンピュータ犯罪と捜査」松尾浩也＝井上正仁編『刑事訴訟法の争点［新版］』（1991年、有斐閣）94頁。

16）小川新二「磁気ディスクと捜索差押え」平野龍一＝松尾浩也編『新実例刑事訴訟法Ⅰ』（青林書院、1998年）251頁。

17）田宮・前掲注13）107頁。

18）東京地決平成10・２・27判例時報1637号152頁。本決定に関する評釈として、梅林啓・研修604号13頁、北村篤・別冊ジュリスト174号［刑事訴訟法判例百選［第８版］］（2005年）56頁、高崎秀雄・別冊ジュリスト203号［刑事訴訟法判例百選［第９版］］（2011年）56頁等参照。

申し立てに対して、差押えの被処分者であるプロバイダは、被疑者ではない上、利用者のプライバシー保護が強く要請される電気通信事業法上の特別第二種電気通信事業者であるから、本件捜索・差押えの適法性を判断するにあたっては、捜索・差押えの必要性と並んで利用者のプライバシー保護を十分に考慮する必要があると説示し、被疑者を含む428名の氏名・住所・電話番号を内容とする顧客データが記録されたFD（フロッピー・ディスク）１枚の差押えに関して、「被疑者に関するものについては、本件被疑事実との関連性、差押えの必要性は明らかであるが、その余の会員に関するデータについては、…本件被疑事実との関連性を認めがたく、差押えの必要性は認められないというべき」として、これを取り消した。これまでの考え方によれば、顧客データが記録された１枚のFDという有体物が差押えの対象であり、これに被疑者であるアカウントに対応する氏名等の情報が記録されている蓋然性が認められる以上、当該FDの差押えの必要性は肯定されるはずであろう。しかしながら、本決定は、同一のFDに記録される大量の被疑者以外の顧客情報に着目して、これらと被疑事実との関連性を否定した。これは、１枚のFDという有体物単位で関連性を判断するのではなく、FDに記録されている情報ごとに判断したものと解される。現在は、記録命令付差押え（刑訴法218条１項）や他の記録媒体への複写による差押え（刑訴法110条の２）により、必要な情報だけを記録した記録媒体の差押えというより侵害的でない処分が可能であるから、当該FD自体を差し押さえるべき特段の事情のない限り、差押えの必要性は認められないと解すべきである[19)]。そう考えられるのであれば、実質的には電磁的記録自体を差押えの対象とする考え方に漸進していると評価することも可能であろう。

（２） 選別困難な状況に起因する問題

被疑事実との関連性が、確認・選別困難な状況との関係において問題となる場

19）壇上・前掲注10）39頁等参照。

合がある。電磁的記録の変更、消去、複製、移転が容易であるという特性から、関連性の確認過程において必要な電磁的記録が隠滅されるおそれがあるため、差押え現場において関連性を確認することができないことなどが考えられる。

大阪高裁平成３年11月６日判決[20]の事案では、フロッピーディスク271枚が被疑事実との関係性を確認することなく差し押さえられた。本判決は、そのままでは記録内容が可視性・可読性を有しないフロッピーディスクを差押え対象とする場合でも、被疑事実との関連性を確認することなく一般的探索的に広範囲にこれを行うことは、令状主義の趣旨に照らし、原則的には許されず、差押え現場で被疑事実と関連性がないものを選別することが容易であるならば、差押え対象から除外すべきであるが、「その場に存在するフロッピーディスクの一部に被疑事実に関連する記載が含まれていると疑うに足りる合理的な理由があり、かつ、捜索差押の現場で被疑事実との関連性がないものを選別することが容易でなく、選別に長時間を費やす間に、被押収者側から罪証隠滅をされる虞れがあるようなときには、全部のフロッピーディスクを包括的に差し押さえることもやむを得ない措置として許容されると解すべきである」として、本件差押えを適法と判断した。

また、最高裁平成10年５月１日決定[21]の事案では、捜査機関は、記録された情報を瞬時に消去するコンピュータソフトを開発しているとの情報を得ていたことから、捜索・差押えの現場で内容を確認することなくPC１台及びフロッピー

20）判例タイムズ796号264頁。本判決の評釈として、山田道郎・ジュリスト臨時増刊1024号［平成４年度重要判例解説］（1993年）192頁、小津博司・別冊ジュリスト148号［刑事訴訟法判例百選［第７版］］（1998年）54頁参照。

21）刑集52巻４号275頁。本決定に関する評釈として、甲斐行夫・研修605号（1998年）13頁、津村政孝・法学教室221号（1999年）124頁、柳川重規・現代刑事法１巻５号（1999年）79頁、川出敏裕・ジュリスト臨時増刊1157号［平成10年度重要判例解説］（1999年）181頁、笹倉宏紀・ジュリスト1191号（2000年）80頁、池田修・最高裁判所判例解説刑事篇平成10年度（2001年）78頁、池田修・ジュリスト増刊：最高裁時の判例４刑事法編（2004年）205頁、村瀬均・別冊ジュリスト174号［刑事訴訟法判例百選［第８版］］（2005年）54頁、加藤克佳・別冊判例タイムズ26号（2010年）175頁、平木正洋・別冊ジュリスト203号［刑事訴訟法判例百選［第９版］］（2011年）54頁、宇藤崇・別冊ジュリスト232号［刑事訴訟法判例百選［第10版］］（2017年）48頁、宮木康博・法学教室470号（2019年）15頁等参照。

ディスク108枚等を包括的に差し押えた。本決定は、「令状により差し押さえようとするパソコン、フロッピーディスク等の中に被疑事実に関する情報が記録されている蓋然性が認められる場合において、そのような情報が実際に記録されているかをその場で確認していたのでは記録された情報を損壊される危険があるときは、内容を確認することなしに右パソコン、フロッピーディスク等を差し押さえることが許される」として、差押え処分を是認した原決定を肯定した。

両判示における「被疑事実との関連性」についての判断は、「選別することが容易でなく、選別に長時間を費やす間に、被押収者側から罪証隠滅をされる虞れ」ないし「その場で確認していたのでは記録された情報を損壊される危険」があるなど、差押え現場における内容の確認に困難な事情がある場合（①）は、「被疑事実に関連する記載が含まれていると疑うに足りる合理的な理由」ないし「被疑事実に関する情報が記録されている蓋然性」（②）が認められれば、内容を確認することなく、全てのフロッピーディスク等について包括的に差し押さえることも許されるというものである。このような判断の論拠として、ⅰ）②における「疑うに足りる合理的な理由」や「蓋然性」の存在は、「関連性」の疎明とはいえないが、①のような内容確認に重大な支障がある場合、「関連性」の要件は②のような「蓋然性」まで緩和され得ると解する見解[22]、ⅱ）差押えの許否は客観的・事後的判断によるのではなく、現場において可能な合理的判断であることから、関連性判断は必ずしも記録媒体の内容を確認しなければ判断できないものではなく、具体的状況等に照らして当該犯罪の証拠が当該媒体に記録されていると疑うに足りる合理的理由がある場合には、一応関連性ありと推認し得ることを前提として、技術的問題、時間、罪証隠滅の危険等を考慮して現実的に可能と認められる確認手段を尽くしたうえで被疑事実と関連性がないことを確認できない場合は、関連性があるものとして差押えを許容する見解[23]、ⅲ）このような問題は、

22）池田・前掲注21）89頁。同様の見解として、甲斐・前掲注21）20頁、津村・前掲注21）125頁、村瀬・前掲注21）55頁など参照。
23）小川・前掲注16）261頁参照。

可視性・可読性のない電磁的記録の差押えに限定された問題ではなく、一般的に、「関連性ありとの判断」の内実は、「（関連するであろうとの）蓋然的予測」であって、やむを得ない例外的事情の有無に関わりなく、そもそも「関連性」とは最低限「関連する蓋然性」という意味であるとする見解[24]などがある。ⅰ）、ⅱ）の見解は、正当な理由を基礎付ける関連性の程度について、令状執行の際の具体的状況によって変動しうるものであるという考え方がその背景にある[25]。

しかしながら、現場の状況次第で差押えの許される範囲が変わる、すなわち関連性の内容が変わることに対しては、差押え範囲を限界付ける「関連性」要件は、令状主義の要請を受けて一般的な形で設定された「固い基準」であり、（とりわけ上記ⅰ）、ⅱ）の見解に対して）個別の利益衡量に依拠して変動させ得るものではないとの批判[26]も強い。そもそも、①のような選別困難な状況に関してやむを得ない事情があることが、「関連性」の有無の判断に影響を与える論理的な根拠は不明確である。内容確認に重大な支障があることは、それを考慮すべきか否かはひとまず措くとしても、当該犯罪の証拠となり得る可能性を示す「被疑事実との関連性」とは概念として異にするものであり、それに包摂される要素や従属する事象でもない。また、蓋然性で足りる（場合がある）との判断は、証拠存在の蓋然性、すなわち捜索すべき範囲に関する判断（刑訴法102条、222条１項）であり、捜索と差押えの要件を混同するものである。したがって、①のような事情を根拠として「関連性」要件を「蓋然性」や「疑うに足りる合理的理由」にすり替えることは、捜査の実効性を確保するという要請から、一方的に「関連性」要件をなおざりにしているとの誹りは免れない。

さらに、関連性要件の緩和は証拠隠滅のおそれがある場合に限定されるのか、

24）佐々木正輝・猪俣尚人『捜査法演習［第２版］』（立花書房、2018年）490頁以下［佐々木正輝］。現場の状況その他から、対象物のいずれかに証拠たり得るものが含まれているという合理的疑いが認められる以上、FD 等の電磁的記録媒体であるか通常の文書であるかを問わず、一般的探索とは一線を画した、一定の範囲内の正当理由ある捜索・差押えであるという。

25）川出・前掲注21）182頁。

26）笹倉・前掲注21）82頁。

内容確認に長時間を要する場合や技術的に困難な場合等においても想定され得るのか定かではない（ただし、上記iii）の見解は、そのような事情は関係なく、そもそも「関連する蓋然性」があれば良い）。処分の実効性を確保することに主眼を置くのであれば、証拠隠滅のような被処分者側に確認困難な状況を創出した責任があるという事情が存することは必ずしも不可欠な要素とはいえない[27]。電子データは内容の変更・消去が容易であり、セキュリティ技術の発展がめざましく、大量の電子データを記録可能であることに照らせば、電磁的記録媒体の差押えにおいて実効性確保の下に関連性要件の意義が縮減していくことは容易に想像される。

他方、現場における差押えそれ自体ではなく、令状記載の差押目的物に該当するか否かを確認するための、「捜索の一過程」ないし捜索・差押えに「必要な処分」として、令状執行現場では内容確認をせずに運び出す処分と考えるべきとする見解[28]がある。被処分者から見れば、捜索現場での内容確認作業も、当該記録媒体につき占有の核心である利用可能性を奪うものであることに相異はない。それゆえ、その所在が捜索現場にあるか、警察署等の持ち出し先にあるかは、被処分者の利益に本質的な差異を生じさせない[29]。したがって、内容確認のための持ち出しは、本体の捜索処分に付随するものとして当初から想定されている権利侵害の範囲内にとどまるといえるため「必要な処分」として許容しうると考えるのである[30]。これに対しては、被処分者の権利保障上の問題として、占有の核心が利用

27）津村・前掲注21）125頁は、セキュリティ等との関連で、専門家であっても第三者には現場における内容確認が困難な状況も十分考えられるため、差押え時の「コンピュータをめぐる状況からみて合理的な努力をしてもなお捜索現場における内容確認に困難がある」場合に、甲斐・前掲注21）20頁は、内容確認に長時間を要する場合や技術的に困難な場合についても包括的差押えを認める。池田・前掲注21）87頁は、罪証隠滅のおそれが全くないときは「蓋然性」により関連性を認めることは許されず、捜査員の増員や専門的知識を有する者を補助者とすることで対応すべきとする。

28）川出・前掲注21）183頁。他に、酒巻匡「捜索・押収とそれに伴う処分」刑法雑誌36巻３号（1997年）95頁以下、笹倉・前掲注21）80頁以下、宇藤・前掲注21）48頁以下などがある。

29）川出・前掲注21）183頁。

30）笹倉・前掲注21）83頁。

可能性であるとしても、現場において占有者が利用できない状態と持ち出されて被処分者の占有が排除されることは異なるのではないかとの疑問がある。また、持ち出し先における選別・確認作業および差押えへの立会いや、持ち出された物件に関する目録の交付等が手続上保障されていない点については、押収目録に準じて持ち出した記録媒体の目録を交付する旨など、令状への適当な条件を記載することにより解決を図ることができると論じられる[31]。しかし、現行法の下では、「必要な処分」に関して目録交付を義務付けることができるか検討の余地があり、立会いや不服申立てについても問題となりうる以上、法改正なしには認められないと指摘[32]される通り、このような条件付捜索・差押え許可状は「新たな令状の創造」であるといわざるを得ない。

（3） 2011年法改正との関係

しかしながら、既に見たとおり、2011年刑事訴訟法改正において、内容確認のための取得に関して規律する内容は含まれていない。それゆえ、現在においても電磁的記録媒体の差押えにおける関連性判断については未だ議論の余地があると言わざるを得ない。上記判例では、記録容量が1.44 MB（メガバイト）のFDに関する包括的差押えが問題とされていた。現代で使用される主だった記録媒体であるUSBメモリやメモリ・カードの記録容量の単位はGB（ギガバイト：1 GB = 1024 MB）であり、HDDに至ってはTB（テラバイト：1 TB = 1024 GB）単位である。PCを構成する記録媒体はHDDやSSD[33]であるから、数百GBから数TBの記録容量を有している。このような技術発展に伴い、現場における内容確認は困難どころか事実上不可能ではないかと懸念され、また、法改正により

31）酒巻・前掲注28）97頁。
32）村瀬・前掲注21）55頁。
33）Solid State Drive（ソリッド・ステート・ドライブ）の略。磁気ディスクで構成されたHDD（ハード・ディスク・ドライブ）と異なり、SSDはフラッシュメモリで構成されている。HDDのように外付けや内蔵ストレージとして使用できる記録媒体。

新設された電磁的記録に係る記録媒体の差押えの執行方法やリモートアクセスを経ての差押えとの関係において、むしろ問題性を拡大・深化させているといえる[34]。法改正を経ても問題は依然として解決されずにより重要性を増し、基礎的・根本的な観点から、従来の捜索・差押えに関する従来の考え方の見直しが迫られている。

4.「電磁的記録」か「記録媒体」か？

（1） 複写物の差押え：電磁的記録と記録媒体の乖離

2011年改正により新設されたリモートアクセスによる電磁的記録の差押え（刑訴法99条２項、同222条１項、同218条２項）は、差し押さえるべき電子計算機を特定のうえ、ネットワークで接続された領域にある必要な電子データを「差押え対象の電子計算機」に複写して、それを差し押さえるという形式の令状を執行するものであるが、当該電子データを「他の記録媒体」へ複写することも認めている。つまり、「差押え対象の電子計算機」か「他の記録媒体」のいずれかに複写して差し押さえることを許容しているのであり、当該電子データ自体の取得により捜査目的を達することができるのであれば、それを複写した「他の記録媒体」を差し押さえて、令状に記載された「差押え対象の電子計算機」については差し押さえないという選択もあり得る[35]。電子データとそれが保存されていた記録媒体との結びつきは絶対ではなくなったといえよう[36]。

34）笹倉・前掲注10）38頁は、現場での点検や選別を経ない事態はもはや例外ではなく、むしろ最高裁平成10年５月１日決定に従った処理が認められる場合が常態となりつつあると指摘する。

35）杉山＝吉田・前掲注10）105頁。

36）もちろん、記録媒体自体が証拠物としての証拠価値（物理的な痕跡等）を有する場合や、当該記録媒体に当該データが記録されていることに意味がある場合、記録媒体のなかの各データの所在、階層情報、タイムスタンプ、削除されたデータの痕跡等が証拠価値を有する場合など、電子データと記録媒体を切り離すことが適切でない状況も十分考えられる。

このことは、実質的には電子データそのものを処分対象としているようにも見える。そもそも、ネットワークを介して遠隔地に所在するサーバに記録されている電子データを、当該サーバ自体の差押えによることなく、遠隔操作により複写して取得するという本処分の性格に照らせば、事実上、オンライン上の電子データの差押えに等しく、電子データを処分の客体と考えることに違和感はない。電子データの取得が目的であり、「他の記録媒体」への複写という選択が可能である以上、令状記載で差押え対象となっている電子計算機の差押えを避け、より侵害的でない「他の記録媒体」への複写による差押えを原則とすべきという考え方も解釈としてあり得る。

しかしながら、電磁的記録に係る記録媒体の差押え（刑訴法110条の２）に関して、それが可能である場合に、より侵害的でない方法を選択し得ることとするものの、同条の処分を選択するか否かは、基本的に差押えをする者の裁量に委ねられているのであって、同条の処分は差押えに当たっての原則的な在り方となるものではない[37]と解されている。そして、リモートアクセスによる複写に関しては、「差押え対象の電子計算機」の記録容量が足りない場合やデータの削除痕跡について解析を行う必要がある場合[38]などを想定して「他の記録媒体」への複写が認められたものと解説されている[39]。このように、「他の記録媒体」への複写

37）杉山＝吉田・前掲注10）57頁以下。

38）ハードディスク等の記録媒体はその記録領域をセクタごとに区割りされ、保存データはセクタ単位の容量に分割されて各セクタに断片化された状態で保管される。各セクタにはアドレスが振られており、ファイルシステムは、このアドレスによりデータの所在を管理している。データの削除とは、通常、データそのものの消去ではなく、ファイルシステム上管理されているアドレスが削除されるだけである。それゆえ、削除データは、その記録領域が新たなデータにより上書きされないかぎり、ファイルシステムのアドレス管理から外れて見ることのできない断片化されたデータ群として存在しているため、専用のソフトウェアによる修復が可能である。差し押えるべき PC のハードディスクに残存する削除データを復旧する必要があるならば、リモートアクセスによりデータを複写した際に、ファイルシステム上は存在しないが削除データが残存する領域に上書きされる可能性があり、それを回避するため他の記録媒体への複写を認めたものである。

39）杉山＝吉田・前掲注10）104頁参照。

は、あくまで処分の実効性確保に主眼を置いた処分と考えられており、電子データごとに生じる権利侵害への配慮は、少なくとも、相対的に優先度が低く解されていると言わざるを得ない。既に見たように、被処分者の権利を保障する令状主義の内実として重要な機能を担う「関連性」の判断において、関連性要件を緩和することを認める見解に通底する処分の実効性を最重視する価値は、利益衡量を本質とする捜査比例の原則に規律される「執行方法の選択」という局面では、一層前面に押し出されやすいだろう。あくまで、令状に「差し押さえるべき物」として掲げられたPCの差押えであって、ネットワーク上に保存された電子データをリモートアクセスにより複写する際に、当該PCへ複写すると不都合が生じる場合における応急措置としての「他の記録媒体」への複写といえる。

外部の記録領域を遠隔操作して複写することにより必要なデータを取得するのであるから、複写の対象となる電子データについて、差押えの「正当な理由」である被疑事実との関連性が認められなければならない。サーバ等から電子データを複写するのであり、サーバ等自体を差し押さえるわけではないから、有体物の差押えに関して生じる不可分性の問題が生じることはなく、複写対象とすることが可能な範囲で必要な電子データだけを選別して複写することができる。問題となるのは、選別困難な状況が存する場合である。この点に関して、条文上、複写の対象が、差し押えるべき電子計算機で作成・変更した電磁的記録、または当該電子計算機で変更・消去することができることとされている電磁的記録に限定されている以上、「このような電磁的記録については、通常、被疑事実との関連性があると思料されるものと考えられるから、個々の電磁的記録について、個別に被疑事実との関連性の有無を判断しなければならないわけではない」との指摘がある[40)]。しかしながら、複写可能な電子データが上記のように限定されていることを根拠に、個々の電子データについて個別に関連性の有無を検討する必要がないとする論理は明確ではない。他方で論者は、「区別が容易である場合に、捜査

40）杉山＝吉田・前掲注10）103頁。

機関が、明らかに被疑事実との関連性がないと思料される電磁的記録の複写を殊更に行うことは許されない[41]」と述べていることから、実質的には、確認・選別が容易とはいえない状況が認められるのであれば、関連性を確認することなく（あるいは、当該電子データが差し押さえるべき PC 等から作成・変更・消去できるという関連性の程度で）、係る電子データを複写できると解していると考えられる。とりわけ、データ量が膨大であることや高度の専門知識・技術を要するため関連性確認が容易でない状況は常態的にあり得ることであるから、処分の実効性を確保するために関連性要件を緩やかに考える傾向に拍車がかからざるをえない。また、リモートアクセスによる差押えは、ネットワークで接続されたサーバ等の外部領域についても、差押え対象の PC と機能的に一体と考えられる記録領域として差押えの対象とする処分と解されている[42]。PC を差し押える際、差押えの現場において当該 PC 内の全電子データやファイルについて関連性を確認・選別するわけではない。従来通り、差押え対象は無体情報たる電子データではなく、有体物たるその記録媒体であることを前提とすると、被疑事実と無関連なデータも、単一の有体物である PC の記録内容として構成されている以上、当該 PC 諸共取得することができる。同じ論理が、拡大された差押え対象であるサーバ等の外部領域内に保存されているアクセス可能な全てのデータについても妥当するという考え方もあり得よう。

（2）「電磁的記録の取得が目的であること」と「有体物を差し押さえる処分であること」のジレンマ

リモートアクセスによる差押えが、令状において「差し押さえるべき物」として特定された電子計算機を対象とする処分であるという建前を堅持して、その差

41）杉山＝吉田・前掲注10）103頁。

42）杉山＝吉田・前掲注10）97頁は、ネットワークに接続して遠隔地にあるサーバ等の記録媒体に電磁的記録を保管することが多いという「現在の電子計算機の利用形態に鑑み、電子計算機の差押えに当たり、その範囲をこれと一体的に使用されている記録媒体にまで拡大しようとするもの」と解説している。

押え執行の前提的処分ないし付随的処分として、ネットワークを介した電磁的記録の複写を認めるという構造の処分であることは、直ちにリモートアクセスが困難な場合にも大きな問題をもたらす。

例えば、①令状執行の現場において、そもそも差押え対象のPC等にログインするためのID・パスワードが判明しない場合や、当該PC等の内容からWebメール・サーバやストレージ・サーバ等を利用していることが認められるが、それらにアクセスするためのID・パスワードが判明しない場合など、令状執行の現場における当該PCの操作によりリモートアクセスすることが困難な場合、あるいは、②リモートアクセス自体は可能であっても、当該PC等から接続する領域に保存されているデータが膨大であったり、偽装や暗号化されていたりするなど、令状執行の現場において被疑事実との関連性を確認して複写すべきデータの選別を行うことが困難な場合が頻繁にあり得ることは想像に難くない。このような場合、被処分者に協力を要請してID・パスワードや必要な電磁的記録の所在を開示させることが適切な状況[43]で、かつ、被処分者がそれに応じる場合[44]でなければ、令状執行の現場におけるリモートアクセス差押えは事実上不可能である。それゆえ、当該PC等の占有を取得したうえで、執行現場から持ち出し、その精査に必要な設備が整った施設において、ID・パスワード等を割り出すために時間をかけて当該PC等の記録領域を解析する必要がある。しかしながら、差押え後の解析によりID・パスワードが判明するとしても、リモートアクセスによる複写は、差し押さえるべき電子計算機の差押えに際して付随的に認められる処分であり、「飽くまで、差押えの前に電磁的記録の複写が行われることが前提とされている[45]」ことから、差押え後、持ち帰った先において、ネットワークで接続されたサーバ等に対して判明したID・パスワードを用いてリモートアクセ

43）被疑者やその関係者、被疑事実に関与しているとおそれがある組織・団体が被処分者の場合は、証拠隠滅等のおそれがあるため適切ではない場合が多いだろう。
44）刑訴法111条の2により要請を受けた被処分者に協力する法的義務が生じるが、応じない者に対する刑事罰等による制裁はなく、ID・パスワードの開示を強制することもできない。
45）杉山＝吉田・前掲注10）105頁。

スすることは許されない。それゆえ、執行現場においてID・パスワードが判明するか否かでリモートアクセスの可否が分かれるという事態に陥るのである。

5．むすびに代えて

2011年の刑事訴訟法改正によりリモートアクセスによる電磁的記録の差押えが新設されたが、差押え現場においてID・パスワードが判明しなかったり、確認に長時間を要したりするなど何らかの事情により差押え現場においてリモートアクセスを実施しなかった場合、上述のように、差押えの執行後に同処分を実施することは認められない。それゆえ、差押え後に当該PCを解析して、あるいは被処分者の説明を受けて得られたID・パスワードを用いてネット上に保存された電子データを取得する方法を別途模索しなければならない。

本来、ID・パスワードが判明したのであれば、それらを用いて外部サーバ等にアクセスするのに差押えたPCを利用して行う必然性はない。しかしながら、現行法上、任意の場所から任意の端末を用いてサーバ等にアクセスして必要なデータを取得する「オンライン捜索」については、被処分者の承諾のない限り、具体的な根拠規定がないため許されない。そこで、ひとつの考え方として、令状呈示や立会いとの関係において困難があるように思われるものの、サーバを対象とする検証としてリモートアクセスするという方法が指摘されている[46)]。また、リモートアクセスによる電磁的記録の差押えとして行うのであれば、差押えの現場において差し押さえるべきPCからアクセスする必要があることから、差押え後の既に占有下にあるPCを対象とするリモートアクセス令状の発付を受け、差

46）笹倉・前掲注10）35頁。捜索・差押えの時点でPCにログインするパスワードが判明しておらずリモートアクセスできなかったため、差押え後に当該PCを対象とする検証令状の発付を受けてリモートアクセスした事案について、東京高判平成28・12・7は、「本件検証は、本件パソコンの内容を複製したパソコンからインターネットに接続してメールサーバにアクセスし、メール等を閲覧、保存したものであるが、本件検証許可状に基づいて行うことができない強制処分を行ったものである」と判示している。

押え（の仕直し）に伴いリモートアクセスを実施する方法も考えられるが、「二重押収[47]」の是非はともかく、「差し押さえるべき物」であるPCについて既に差押えが完遂されているにもかかわらず、付随的処分たるリモートアクセスのためだけに重ねて差押えをすることに疑問を感じざるを得ない[48]。

この2度目の差押えは、PCの占有取得という主たる処分の観点からは全く意味を有しない処分であり、純粋にネットワーク上のサーバから電子データそのものを差し押える処分と見ることができる。ここまで電子データと記録媒体の乖離を認めることができるのであれば、有体物の差押えに付随することなく、電子データ自体を取得するために適切な処分を設けるべきではないか。クラウド・サービスの利用が普及し、利用者が携帯する端末自体の内容はスリム化が進んでいる現状において、端末には証拠とすべき電子データはない。それらの多くがサーバ上に保管されているのであれば、差し押さえるべき物とされる端末は、もはや証拠そのものではなく、証拠とすべき電子データに通じる「扉」ないし「その鍵が隠された保管庫」にすぎない。差押えの対象は有体物に限定されるという建前上、付随的処分として扱われる電磁的記録の複写とそれ自体証拠価値の乏しい記録媒体の差押えの捻れた関係は、そろそろ維持することが不可能な境地に至っているのではないだろうか。電子データを取得する処分を正面から認め、それにより不利益を受ける被処分者の権利保全との関係で適切に規律する方策を模索する必要があるだろう。

情報技術の発展が捜査手続にもたらす問題は多岐にわたり、全ての議論の前提となる電子データの同一性の確保の問題に加え、ID・パスワード、指紋認証、

47）民事上、行政上の差押え中の物についても、各々目的が異なるため差押え可能であり、他の捜査機関あるいは裁判所が差押え中の物についても重ねて押収することは可能であると解されている。団藤重光編『法律実務講座刑事篇2巻』（有斐閣、1953年）315頁［足立進］、伊藤栄樹ほか編『注釈刑事訴訟法［新版］2巻』（立花書房、1997年）154頁［藤永幸治］、河上和雄ほか編『大コンメンタール刑事訴訟法［第2版］第2巻』（青林書院、2010年）269頁［渡辺咲子］参照。同書［渡辺］は、このような二重押収は実務上多く行われると指摘する。

48）笹倉・前掲注10）34頁。

生体認証等のセキュリティ解除、越境リモートアクセスに伴う主権侵害の問題など枚挙にいとまがない。これらの問題に関しては引き続き検討課題としたい。