

国外へのリモートアクセスによる 電磁的記録の複写の処分

(最二小決令和3年2月1日刑集75巻2号123頁)

横 山 裕 一

第1 はじめに

本件は、インターネットサイトXの運営管理会社Yの関係者Z、被告人甲及び乙が共謀の上、同サイトで公然わいせつ等の犯行に及んだことを公訴事実とする事件である。最高裁は、弁護側が上告して争った①国際捜査共助によることなく国外のサーバに対してリモートアクセスを行い電磁的記録の複写をすることの許否、②リモートアクセスにより収集された証拠の証拠能力、③リモートアクセスによる電磁的記録の複写に際して、個別に内容を確認することなく複写を行うことの適否、④インターネットサイトXを管理・運営していた被告人両名の共同正犯の成否について判断したが、本稿では、刑訴法上の問題として①乃至③について検討をする。

第2 事案の概要（認定事実）

判例が前提とした本件リモートアクセスに係る捜査の経緯等は、次のとおりである。

「ア 警察官は、平成26年9月30日、インターネットサイト「X」の運営管理会社である株式会社Y（以下「Y」という。）の業務全般を共同で統括管理するZ（以下「Z」という。）及び被告人甲並びにYの代表取締役である被告人乙らが共謀の上、同サイトにおいて公然わいせつ助動、風俗営業等の規制及び業務の適正化等に関する法律違反の各犯行

に及んだことを被疑事実とする搜索差押許可状に基づき、Y事務所及び付属設備において、搜索差押えの執行を開始した。

上記搜索差押許可状は、「差し押さえるべき物」として、「パーソナルコンピュータ」等が記載されているほか、「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」として、「差し押さえるべきパーソナルコンピュータ（中略）からの接続可能なファイル保管用のサーバの記録媒体の記録領域であって、当該パーソナルコンピュータ等の使用者に使用されているもの」、「差し押さえるべきパーソナルコンピュータ（中略）からの接続可能なメールサーバの記録媒体の記録領域であって、当該パーソナルコンピュータ等の使用者のメールアドレスに係る送受信メール、その他の電磁的記録を保管するために使用されているもの」が記載された、リモートアクセスによる電磁的記録の複写の処分（刑訴法218条2項）を許可した令状であった。

イ 警察官は、上記搜索差押えの実施に先立ち、Yではアメリカ合衆国に本社があるA社の提供するメールサービス等が使用されている疑いがあり、令状に基づきメールサーバ等にアクセスすることは外国の主権を侵害するおそれがあると考えられたことから、日本国外に設置されたメールサーバ等にメール等の電磁的記録が蔵置されている可能性があるこ

とが判明した場合には、令状の執行としてのリモートアクセス等を控え、リモートアクセス等を行う場合には、当該パソコンの使用者の承諾を得て行う旨事前に協議していた。

ウ 警察官は、上記イの方針に基づき、被告人兩名を含むYの役員や従業員らに対し、メールサーバ等リモートアクセスをしてメール等をダウンロードすること等について承諾するよう求め、アカウント及びパスワードの開示を受けるなどしてリモートアクセスを行い、メール等の電磁的記録の複写を行ったパソコンについては、被告人乙から任意提出を受ける手続をとった（以下、この証拠収集手続を「手続⑦」という。）。

しかし、警察官は、Y関係者に対し、上記リモートアクセス等は任意の承諾を得て行う捜査である旨の明確な説明をしたことはなく、原判決は、手続⑦について、関係者は上記搜索差押許可状等の執行による強制処分と誤信して応じた疑いがあるから任意の承諾があったとは認められない旨判断しており、この判断が不合理であるとはいえない。

エ 上記搜索等が開始された同日以降、Y事務所において、メール等を使用者のパソコンに複写する作業等が続いたが、なお相当の時間を要すると見込まれ、終了のめどが立っていない状況において、Yは、警察官に対し、よりYの業務に支障が少ない方法として、警察のパソコンでメールサーバ等にアクセスできるアカウントを付与するなどしてY事務所以外の場所でダウンロード等ができるようにする旨の提案を行った。その範囲や方法等について、Yの幹部と警察官との間で、Yの顧問弁護士も交えて協議が行われ、最終的に被告人乙が同年10月3日付けで承諾書を作成した。警察官は、これに基づき、Y事務所外の適宜の機器からリモートアクセスを行い、電磁的記録の複写を行った（以下、この証拠収集手続を「手続④」という。）。

オ 手続⑦、④の各リモートアクセスの対象である記録媒体は、日本国外にあるか、その蓋然性が否

定できないものである。なお、上記各リモートアクセス等について、外国から反対の意思が表明されていたような事情はうかがわれない。」

第3 決定要旨 (以下「本決定」という。)

上告棄却。

1 本決定は、以下のとおり判示して、警察官が手続⑦、④により収集した証拠の証拠能力を認めた（本決定引用部分の下線は筆者による。以下、本稿において同じ。）。

「所論は、日本国外に所在するサーバへのリモートアクセスによる電磁的記録の取得行為は、現行刑訴法によっては行うことができず、あくまで国際捜査共助によるべきものであるところ、警察官が、これらの点を認識した上、国際捜査共助を回避し、令状による統制を潜脱する意図の下に手続⑦、④を実施した行為は、サーバ存置国の主権を侵害するものであり、重大な違法があるから、各手続によって収集された証拠は違法収集証拠として排除すべきである旨主張する。

しかしながら、刑訴法99条2項、218条2項の文言や、これらの規定がサイバー犯罪に関する条約（平成24年条約第7号）を締結するための手続法の整備の一環として制定されたことなどの立法の経緯、同条約32条の規定内容等に照らすと、刑訴法が、上記各規定に基づく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同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。

その上で、まず、手続⑦により収集された証拠の証拠能力について検討すると、手続⑦は、Y関係者の任意の承諾に基づくものとは認められないから、

任意捜査として適法であるとはいえず、上記条約32条が規定する場合に該当するともいえない。しかし、原判決が説示するとおり、手続⑦は、実質的には、司法審査を経て発付された前記搜索差押許可状に基づく手続ということができ、警察官は、同許可状の執行と同様の手続により、同許可状において差押え等の対象とされていた証拠を収集したものであって、同許可状が許可する処分の範囲を超えた証拠の収集等を行ったものとは認められない。また、本件の実事関係の下においては、警察官が、国際捜査共助によらずにY関係者の任意の承諾を得てリモートアクセス等を行うという方針を採ったこと自体が不当であるということとはできず、警察官が任意の承諾に基づく捜査である旨の明確な説明を欠いたこと以外にY関係者の承諾を強要するような言動をしたとか、警察官に令状主義に関する諸規定を潜脱する意図があったとも認められない。以上によれば、手続⑦について重大な違法があるということとはできない。

なお、所論は、令状主義の統制の下、被疑事実と関連性の認められる物に限って差押えが許されるのが原則であり、警察官は、被疑事実との関連性を問わず包括的に電磁的記録を取得した違法があるとも主張する。しかし、前記の事実関係に照らすと、前記搜索差押許可状による複写の処分の対象となる電磁的記録には前記被疑事実と関連する情報が記録されている蓋然性が認められるところ、原判決が指摘するような差押えの現場における電磁的記録の内容確認の困難性や確認作業を行う間に情報の毀損等が生ずるおそれ等に照らすと、本件において、同許可状の執行に当たり、個々の電磁的記録について個別に内容を確認することなく複写の処分を行うことは許されると解される。所論は採用することができない。

また、前記⁽¹⁾の経過によれば、手続④についてY関係者の承諾の効力を否定すべき理由はないとした原判断が不合理であるとはいえず、上記で説示したところにも照らすと、手続④について重大な違法があるということとはできない。

以上によれば、警察官が手続⑦、④により収集した証拠の証拠能力は、いずれも肯定することができ、これと同旨の原判決の結論は正当である。」

2 なお、本決定には以下のとおり三浦守裁判官の補足意見が付されている。

「リモートアクセスをして記録媒体から電磁的記録を複写するなどして収集した証拠の証拠能力について補足する。

電磁的記録を保管した記録媒体が外国に所在する場合に、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、当該外国の主権との関係で問題が生じ得るが、法廷意見が説示するとおり、その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される。

本件においては、手続⑦及び④の各リモートアクセスの対象である記録媒体は、日本国外にあるか、その蓋然性が否定できないものであって、同条約の締約国に所在するか否かが明らかではないが、このような場合、その手続により収集した証拠の証拠能力については、上記の説示をも踏まえ、権限を有する者の任意の承諾の有無、その他当該手続に関して認められる諸般の事情を考慮して、これを判断すべきものと解される。」

(1) 本稿第2「事案の概要（認定事実）」参照

第4 本決定についての検討⁽²⁾

1 序論

1980年代から90年代にかけて、日本では、企業と個人とを問わずコンピューターの導入・利用が急速に進み、それに伴い情報の保管・管理の媒体もそれまでの紙から電磁的記録（以下「電子データ」という。）へと徐々に移行が進んだ。2000年代に入りインターネットが普及したことで、電子データの送受信に電子メールや各種ウェブサービス等でインターネット通信が用いられることがごく当たり前の状況となったが、それでもなお電子データそのものは利用者のコンピューター端末やフロッピーディスク、CD-R及びハードディスク等の各種記録媒体に保存する方法が通常であったため、犯罪捜査の過程において電子データの内容を証拠として保全する場合には、有体物としての前記録媒体を差し押さえるという運用がなされていた。その意味では、コンピューターの導入・利用が進んでいたとはいえ、捜査機関の行う証拠の収集活動としては、差押対象物が紙であるか電磁的記録媒体であるかはいずれも有体物であるという点で異なるところはなく、差押えの場面における両者の差異は、主に関連性の問題として包括的な差押えの可否という観点で論じられてきた⁽³⁾。

ところが、近時においては、事業者がコンピューター資源（サーバやソフトウェア等）を用意し、利用者がインターネット回線を通じて同資源にアクセスして様々なサービスを楽しむというクラウドコ

ンピューティングサービス（以下「クラウドサービス⁽⁴⁾」という。）の利用も一般的となっており、個人においても、スマートフォンが普及したことにより、電子データの取扱い方法は大きく変容を遂げている。常時インターネットに接続して各種サービスを利用できることが機能的特徴であるスマートフォンは、取り扱う電子データを端末上に保存することが必ずしも前提とはなっておらず、むしろ電子データの取扱いに関してそれがローカル（端末）の電子データかオンライン（クラウドサービス）の電子データかを利用者に意識させない作りを目指すソフトウェアが開発される場合もある。これは、スマートフォンに限った話ではなく、パソコンで利用される電子メールも同様で、旧来は、利用者がメールサーバからメールをすべてダウンロードしてメールサーバ上からは削除するというPOPが主流であったが、その後、パソコンにおいてもインターネットの常時接続が当たり前となったことで、メールを開く際にその都度メールサーバ上の電子データを参照するIMAPが主流となった。すなわち、POPが主流であった時代では、メールがダウンロードされたコンピューター端末を差し押さえれば、同時に同端末に記録された電子メールの内容を証拠として保全することを達することができたが、IMAPが主流となって以降は、メールの送受信に利用しているコンピューター端末を差し押さえたとしても、必ずしもその端末内に電子メールの電子データが記録されているとは限らないため、有体物の差

(2) 本決定の解説・評釈として、岩崎正「外国に所在する記録媒体へリモートアクセスして収集した証拠の証拠能力」新・判例解説 WatchNo.142（2021年）、四方光「越境リモートアクセスにより収集された証拠の証拠能力とわいせつ動画の投稿を促すサイト管理者の刑事責任」法学教室491号75頁（2021年）、吉戒純一「最高裁時の判例」ジュリスト1562号98頁（2021年）、星周一郎「わいせつ動画の投稿・配信を促すインターネットサイト管理者の共同正犯責任および日本国外に所在する蓋然性のある記録媒体に越境リモートアクセスをして収集した証拠の証拠能力」刑事法ジャーナルNo.69 264頁（2021年）等がある。

(3) 最決平成10年5月1日刑集52巻4号275頁等。

(4) 一般に、クラウドサービスはそのサービス形態によってSaaS、PaaS、IaaSに分類されるが、本稿では特段の記載のない限り、電子メールや電子データをクラウド上に保存するSaaSを指してクラウドサービスの語として用いる。

(5) 総務省『令和3年版情報通信白書』314頁によると、企業におけるクラウドサービスの利用状況は、2016年は46.9%であったが、2020年は68.7%となっている。

押えにより電子データの内容を証拠として保全する方法に限界が生じることとなった。このことは、電子メールに限らずオフィスソフト等で作成された文書等も同じで、電子データをクラウドサービス上に保存することは決して珍しいことではなくなった。

そこで、IT技術の進歩に対して捜査手段をこれに適合させるべく、平成23年6月に刑法が改正（平成24年6月施行）され、刑法99条2項及び218条2項により、コンピューター等の電子計算機の差押えに際して、当該電子計算機に接続された記録媒体のうち当該電子計算機で管理されているデータ領域⁽⁶⁾にアクセスして電子データを複写して差し押さえることができるよう改正がなされた。なお、電子データの複写は、コンピューター等の差押え前になすことを要するとされている⁽⁷⁾。もっとも、同規定は日本国内に存置された記録媒体へのリモートアクセスには当然に適用されるものの、当該記録媒体が外国に存置されている場合における処分の適法性については、平成23年の改正では依然として確かな解決に至らなかった。

一般に、クラウドサービスの主たるメリットは、利用者があらゆる場所・あらゆる端末から同じ電子データにアクセスできる点や、クラウドサービス上の電子データをバックアップとして利用できる点にあるとされている⁽⁸⁾。そして、クラウドサービス事業者、特に世界中でサービスを展開する海外事業者は、より充実したクラウドサービスを提供するために、電子データを記録するデータサーバを世界中に

分散させて冗長化を図ることもあり得、場合によっては2カ国以上の国に同じ電子データが記録されているデータサーバが存置されている可能性⁽⁹⁾もあり、同じ利用者がクラウドサービス上に保管した同じ電子データであっても、アクセスごとに異なる国のデータサーバに繋がる可能性も否定できない。このように、クラウドサービスに対するリモートアクセスは、そもそも当該リモートアクセスの対象たる記録媒体が日本を含めいずれの国に存置されているのかを確認することが極めて困難であるという特色がある。そして、リモートアクセスの対象たる記録媒体が国外に存置されている可能性がある場合に、果たして国際捜査共助によらずに刑法218条2項に基づく搜索差押許可状により電磁的記録の複写をすることが可能であるのかという問題へと繋がるのである。

本決定以前には、後述するサイバー犯罪条約32条の存在を根拠に、リモートアクセスの対象となる記録媒体が外国に存置されていると思料される場合の捜査方法として、捜査機関が、被疑者らクラウドサービス利用権者の同意を得て任意捜査としてリモートアクセスを行う方法や、クラウドサービス事業者の日本支社を通じて同事業者の同意を得る方法を試行し、これらの同意が得られない場合に国際捜査共助⁽¹⁰⁾の手段を執ることが提案された。他方で、記録媒体が外国に存置されている可能性があるもののいずれの国に存置されているか判明しない場合には、同意を求めたり国際捜査共助を要請することな

-
- (6) 池田修・前田雅英『刑事訴訟法講義』（第6版 東京大学出版会 2018）181頁は、218条2項の「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」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」の例として、差し押さえるべきコンピュータにリモート・ストレージ・サービスのアカウントの設定がなされている場合を挙げている。
- (7) 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105頁（2012年）
- (8) マイクロソフトが展開するクラウドサービスであるAzureは、どこからでも、どのようなデバイスからでも電子データにアクセスして「リモートで安全かつ生産的に作業する」こと等がクラウドサーによって実現できることを謳っている。（<https://azure.microsoft.com/ja-jp/overview/why-azure/>）
- (9) セキュリティ上の観点から、個別的なデータサーバの所在地を公表していないことも多い。
- (10) 桑名仁ほか『外事犯罪捜査ハンドブック』（第2版 立花書房 2020年）121頁

く直ちにリモートアクセスが認められるべきであるとする考え方もある。⁽¹¹⁾

本件は、越境リモートアクセスの可否について様々な考え方が唱えられる中、刑訴法218条2項に基づいて日本国外に所在するサーバのデータ領域にリモートアクセスして電子データを複写することの適否から始まり、これと密接に関係する問題として、当該リモートアクセスにより収集された証拠の証拠能力及び個々の電子データについて個別に内容を確認することなく複写の処分を行ったことの適否について最高裁が判断を下した事案である。

2 国際捜査共助

国外における証拠収集が必要な場合に、当該国の政府に捜査協力依頼をし、外国の捜査機関が収集した証拠を自国に送付してもらうという捜査手段を用いることになり、このような刑事事件の捜査・訴追・裁判のための証拠の取得に関する国際協力を国際捜査共助⁽¹²⁾いう。日本は、アメリカ、韓国、中国、香港、EU、ロシアとの間で捜査共助に関する刑事共助条約又は協定を締結しており、締約国との間では、法務省ないし警察庁と相手国の司法当局との間で直接捜査共助の要請や、証拠等の授受を行うことになる。⁽¹³⁾

他方、非締約国との間での捜査共助は、国内では警察庁あるいは検事正が捜査共助要請書を作成して法務省から外務省を通じ、その後、相手国の外務省を介して相手国の司法当局へたどり着き共助が実施されることになる。⁽¹⁴⁾

これらの国際捜査共助の手順からしても明らかとなり、後者に比して前者の方がいくらか迅速な捜査共助の実現が期待できるとはいえ、それでも実際に捜査手続に着手するには相当の期間を要することは間違いない。国際捜査共助がこのような迂遠な

手続を要するという実情も、本決定の結論と無関係ではないように思われる。

3 本決定前の裁判例の状況

本決定の第1審判決に先立つ東京高判平成28年12月7日（高刑集69巻2号5頁）は、リモートアクセスによる複写の処分が許可された搜索差押許可状に基づいて差し押さえたパソコンの内容を別のパソコンに複製した上で、検証許可状の発付を受けて複製され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（以下「本件検証」という。）との事案において、「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。しかも、そのサーバが外国にある可能性があったのであるから、捜査機関としては、国際捜査共助等の捜査方法を取るべきであったともいえる。」とし、上記搜索差押許可状及び検証許可状の発付を受けていたことを考慮したとしても「違法の程度は重大なもの」であるとして、本件検証の結果である検証調書及び捜査報告書の証拠能力を否定した。このように、国外に存在するサーバへのリモートアクセスについては国際捜査共助によるべきとされ、国際捜査共助によらないリモートアクセスは重大な違法につながるとされた裁判例が表れた後に、同じく国際捜査共助によらないリモートアクセスが行われた事案について判断をしたのが本決定である。

4 越境リモートアクセス（①）及び違法収集証拠排除法則（②）について

本決定は、まず、国際捜査共助によることなく国外のサーバに対してリモートアクセスを行って電磁的記録の複写をすることの許否（①）についての見解を示した上で、手続⑦及び手続④のそれぞれについて、証拠能力を排除すべき違法収集証拠に該当す

(11) 川出敏裕「コンピュータ・ネットワークと越境捜査」井上正仁先生古稀祝賀論文集（有斐閣 2019年）429頁

(12) 城祐一郎『特別刑事法犯の理論と捜査 [1]』（立花書房 2010年）194頁

(13) 衆名・前掲注(10) 114頁

(14) 衆名・前掲注(10) 112頁

るか否か（②）について判断を行っている。なお、認定事実にもあるとおり、手続⑦は、刑訴法218条2項に基づく本件搜索差押許可状の発付を受けていたものの、リモートアクセス先の記録媒体が日本国外に存置されている可能性があると思料されたため、任意捜査に切り替えてYの関係者から承諾（ただし、裁判所は当該承諾は錯誤によるもので有効な承諾ではないとした。）を得た上でリモートアクセスを実行したという経緯であり、刑訴法218条2項に基づく令状の執行としての越境リモートアクセスの可否を直接判断したという事案ではない。

本決定は、①について、「刑訴法99条2項、218条2項の文言や、これらの規定がサイバー犯罪に関する条約（平成24年条約第7号）を締結するための手続法の整備の一環として制定されたことなどの立法の経緯、同条約32条の規定内容等に照らすと、刑訴法が、上記各規定に基づく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同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、サイバー犯罪に関する条約32条bに該当する場合には、国際捜査共助によることなくリモートアクセス及び複写を行うことを認めたものと読むことができる。

サイバー犯罪に関する条約（訳文）

第三十二条

蔵置されたコンピュータ・データに対する国境を越えるアクセス（当該アクセスが同意に基づく場合又は当該データが公に利用可能な場

合）締約国は、他の締約国の許可なしに、次のことを行うことができる。

- a 公に利用可能な蔵置されたコンピュータ・データにアクセスすること（当該データが地理的に所在する場所のいかんを問わない。）。
- b 自国の領域内にあるコンピュータ・システムを通じて、他の締約国に所在する蔵置されたコンピュータ・データにアクセスし又はこれを受領すること。ただし、コンピュータ・システムを通じて当該データを自国に開示する正当な権限を有する者の合法的なかつ任意の同意が得られる場合に限る。

次に、手続⑦、④について、それぞれ排除すべき違法収集証拠に該当するか否かの検討を行っている。

手続⑦については、（第1審の認定とは異なり）Y関係者の承諾は任意になされたものではなく任意捜査として適法でないとし、かつサイバー犯罪条約32条にも該当しないとしながらも、実際に押収された電子データは、司法審査を経て発付された当初の刑訴法218条2項による搜索差押許可状で押収することを予定した範囲から逸脱しておらず、また、警察官に令状主義の潜脱の意図⁽¹⁶⁾は認められないことから、重大な違法があるということとはできず、証拠能力は排除されないとした。

手続④については、手続⑦と異なり任意の承諾であること、当初の搜索差押許可状の範囲内であることから、これもまた重大な違法があるとはいえないとして証拠能力を認めた。

本決定は、「電磁的記録を保管した記録媒体が同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

(15) 外務省ウェブページによると、平成28年2月現在の締約国は48か国（全てのG7諸国を含む。）、署名済み未締結国は6か国。（<https://www.mofa.go.jp/mofaj/gaiko/soshiki/cyber/index.html>）

(16) 白取祐司『刑事訴訟法』（第10版 日本評論社 2021年）400頁は、排除法則が適正手続の要請でもあることに鑑みると、捜査官の主観的要件は重視すべきでないとする。

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。」として越境リモートアクセスの許否について一応の基準を示しながらも、この基準のみをあてはめるのではなく、実質的には違法収集証拠排除法則の枠組みの中で手続⑦及び手続④のリモートアクセスの許否を判断するとの仕組みとなっていると考えられる。

すなわち、序論で述べたとおり、クラウドサービスの性質上データサーバがいずれの国に存置されているかを確認することは極めて困難であり、サイバー犯罪条約32条bの「他の締約国に所在する設置されたコンピュータ・データ」の要件を充足しているか否かが果たして裁判上明らかになるのかという点である。そうすると、およそ上記基準を満たす完全に適法な越境リモートアクセスを意図的に実現することは著しく困難ではないかという疑問が生じる⁽¹⁷⁾。もっとも、サイバー犯罪条約が制定・締結された経緯からも明らかなとおり、IT技術の急速な進歩により、越境リモートアクセスによる電子データの証拠収集は、犯罪捜査の上で不可欠の証拠収集方法であることは間違いない。証拠の収集過程における捜査手続の違法は、その問題の帰趨は当該証拠の証拠能力の問題に行き着くことが少なくないから、違法収集証拠排除法則の枠組みの中で、個別具体的に越境リモートアクセスの実質的な適否を検討することは理にかなっていると考えられる。

また、本決定のうち「なお、上記各リモートアクセス等について、外国から反対の意思が表明されていたような事情はうかがわれない。」との認定部分は、その直前の「手続⑦、④の各リモートアクセスの対象である記録媒体は、日本国外にあるか、その蓋然性が否定できないものである。」との部分との関係で、当該記録媒体が日本国外に存在しない蓋然

性を補強するための説明程度の趣旨であるようにも読めるが、他方で、外国から反対の意見が表明された場合にはそのような事実（当該国が主権の侵害を主張したとの事実）を重視して証拠能力を判断する可能性を示唆しているようにも読める。本決定の原審である大阪高判平成30年9月11日（高検速報（平成30年）344頁）は、「我が国の捜査機関が、刑法218条2項のリモートアクセス令状に基づいて、外国に存在するサーバ等の記録媒体に対し海外リモートアクセス等の処分を行うことが、当該他国の主権を侵害するか否かについては、国際的に統一された見解があるわけではなく、また、後述のサイバー犯罪に関する条約（平成24年条約7号。以下「サイバー犯罪条約」という。）32条も、どのような場合にこのような処分が許されないこととなるかを明示的に規定しているわけではない。もっとも、電磁的記録を複写すべき記録媒体が他国の領域内にあることが判明した場合において、同条約32条によりアクセス等を行うことが許されている場合に該当しないときは、当該他国の主権との関係で問題を生じる可能性もあることから、この処分を行うことは差し控え、当該他国の同意を取り付けるか、国際捜査共助を要請することが望ましいとの指摘が少なからず存在する。このように、我が国の捜査機関が、国際捜査共助の枠組み等により相手国の同意ないし承認を得ることなく、海外リモートアクセス等の処分を行った場合には、強制捜査であれ、任意捜査であれ、その対象となった記録媒体が所在する相手国の主権を侵害するという国際法上の違法を発生させると解する余地がある。そして、相手国の主権を侵害しており、国際法上の違法があるといえる場合には、この違法が当該捜査手続に刑法上も違法の瑕疵を帯びさせることになると考えられる。

(17) 注(15)のとおり主要な国は締約国に含まれているため結果的に充足するということは十分にあり得ようが、確証のないままに締約国にデータサーバが存置されているとの前提で捜査に着手すべきでないし、そもそも仮に締約国だったとしても裁判上でそれを明らかにすることはやはり困難であろう。

(18) 外務省『サイバー犯罪条約に関する説明書』（https://www.mofa.go.jp/mofaj/gaiko/treaty/pdfs/treaty159_4b.pdf）2004年

しかしながら、相手国が捜査機関の行為を認識した上、国際法上違法であるとの評価を示していればともかく、そうではない場合に、そもそも相手国の主権侵害があったといえるのか疑問がある。」（下線は筆者による追記。）と判示している。同判決は、サイバー犯罪条約32条に該当せず、かつ国際捜査共助等により相手国の同意ないし承認が得られないままにリモートアクセスを行った場合、相手国が国際法上違法であるとの評価を示せば同国に対する主権侵害があったといえ、この違法は刑訴法上の違法性の評価にも影響を与えるとの考え方に立ったものと思われる。これまで見てきたとおり、本決定は、法廷意見としては外国の主権侵害が生じた場合について具体的に言及しておらず、ともすれば外国の主権侵害の問題と、日本国内における刑訴法上の問題を切り離したものであるかのようにも思える。しかしながら、原審において明確に「国際法上違法であるとの評価を示していればともかく」との具体的な例示を伴った説示がなされていることを踏まえると、本決定における「上記各リモートアクセス等について、外国から反対の意思が表明されていたような事情はうかがわれない。」との部分は、やはり原審の上記説示を意識した言及であると読むのが素直であると考ええる。リモートアクセスは、捜査員が被疑者からクラウドサービス利用者の正規のID及びパスワード等でログインするため、クラウドサービス事業者からはこれを直ちに本来の利用者以外の第三者によるアクセスであると判断することは困難であり、すなわち、相手国が日本の捜査機関によるリモートアクセスだと認識して主権侵害を主張すること自体が稀な状況であることが予想されるが、仮に相手国が主権侵害を主張してきたという事実が認定されるような事案の場合には、裁判所は、違法収集証拠排除法則の適用の判断に際して、これを一つの

考慮要素として位置付けることが予想される。

総括すると、本決定は、①及び②について、越境リモートアクセスの許否についてサイバー犯罪条約32条bに該当する場合には、国際捜査共助によることなく越境リモートアクセスをすることは許されるとした上で、手続⑦及び④について、いずれも司法審査を経て発付された当初の刑訴法218条2項による搜索差押許可状で押収することを予定した範囲から逸脱しておらず、警察官に令状主義の潜脱の意図も認められないことを主な理由として、違法収集証拠排除法則における重大な違法に該当せず、証拠能力が認められるとした。

5 個別に内容を確認することなく複写を行うことの適否（③）

搜索差押許可状の執行にあたっては、一般令状を禁止する令状主義の趣旨に照らし、被疑事実と差押え対象物との関連性が要求される⁽²⁰⁾。差押え対象物が電磁的記録媒体である場合、関連性の有無の判断をするためには、その記録内容を逐次パソコン等に読み込ませてディスプレイ上に表示する必要があるが、搜索差押えの現場でこれを実行することは困難であるという特徴がある。そのため、電磁的記録媒体の差押えについては、個々にその記録内容を確認せずに差押えを行うといういわゆる包括的差押えの可否が問題となる。本件は、リモートアクセスにより取得した電磁的記録の複写の処分における事案であるが、被疑事実と複写の対象となる電磁的記録との間にも関連性が要求されることは、前記令状主義の趣旨から当然であり、本件でも、リモートアクセスによる電磁的記録の複写に際して、個別に内容を確認することなく複写を行うことの可否が問題となった。

包括的差押えの可否について判断した最決平成10年5月1日刑集52巻4号275頁は、前述のような電

(19) 近年では、SMS認証等の2段階認証を導入しているサービスが増えたため、そもそも捜査員がアカウントとパスワードを被処分者から聞き出ただけではログインできない事態も想定される。

(20) 白取・前掲注(16) 135頁

磁的記録媒体の特徴に照らし、「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⁽²¹⁾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ものと解される。」と判示し、一定の場合に電磁的記録の内容を確認することなく包括的に差し押さえることが許容されとした。本決定においても、この判例を踏襲する形で、越境リモートアクセスにより取得した電磁的記録に被疑事実と関連する情報が記録されている蓋然性が認められること、原判決が指摘するような差押えの現場における電磁的記録の内容確認の困難性や確認作業を行う間に情報の毀損等が生ずるおそれがあることを指摘し、個々の電磁的記録について個別に内容を確認することなく複写の処分を行うことは許されとした。⁽²²⁾

6 今後の検討課題

上記第3の3でみたとおり、本決定は、越境リモートアクセスの許否に関して一応の基準を示しているものの、今後も、その実質的な判断は違法収集証拠排除法則の枠組みの中に集約されていくように思われる。本決定の事案は、確かな前例がない中で、警察官は任意の承諾が得られれば適法に越境リモートアクセスができるとの考えに基づいて越境リモートアクセスに及んだものであるが、これに対して、最高裁は、刑訴法218条2項に基づく搜索差押許可状の発付を受けた上で、同許可状の執行ではなく被疑者らの承諾を得た上で越境リモートアクセス

を実施したとしても、違法収集証拠排除法則の適用を受けないとの結論を導き出したものである。しかしながら、上記判断はあくまで違法収集証拠排除法則の枠内での判断であり、それは、最判昭和53年9月7日刑集32巻6号1672頁が示す「令状主義の精神を没却するような重大な違法」と「将来における違法捜査の抑制の見地」から当該証拠の証拠能力を排除すべきかどうかを個別具体的に判断したということであり、類似の事案において全く同じように証拠能力の有無が判断されるとは限らないため、今後の判例の動向にも注視をしたい。

また、本決定で「電磁的記録を保管した記録媒体が同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。」という文言が置かれていることから、締約国以外に記録媒体が存置されていることが証拠上明らかになった場合に、これが結論にどのような影響を及ぼし得るかも検討を続ける必要がある。さらには、上記引用部分の裏返しとして、締約国以外の国に存置されたデータサーバに対して越境リモートアクセスを試みる場合には、これが国際捜査共助によらないかぎり許されないということにもなり得るが、事案によっては、捜査官が許されない越境リモートアクセスとなり得ることを承知した上でのこれを実施したということも生じうるため、これらの事情が違法収集証拠排除法則適用の判断にあたりどのような影響を及ぼすのかについても、今後の検討課題としたい。

以上

(21) 蓋然性の具体的意味内容については、佐々木・猪俣『捜査法演習』（第2版 立花書房 2018年）485-495頁に詳しい。

(22) 原審は、「事務所の外にある記録媒体の記録領域については、保存されている情報が極めて多量に上ることも考えられ、複写に先立って被疑事実との関連性を個別に確認しようとすれば、それ自体に相当長時間を要するのみならず、本件の証拠構造上、捜査官らがその場で直ちに当該情報の収集の要否を判断することは困難であったといえ、さらに、確認作業を行う間に情報の毀損、変更が生じるおそれは、同事務所内に所在するサーバ等の記録媒体の内容を確認する場合と比べても、格段に大きかったといえる。」としている。