越境的捜査活動に対する法的規律をめぐる総合的研究

研究代表者　　指　宿　信　　成城大学法学部教授

1　はじめに

本研究は、捜査機関による越境的なコンピュータ・データの収集、すなわち、管轄外に所在するコンピュータに保存（蔵置）されている電磁的記録（データ）を取得する執行方法について、国際的に大きな改革が進行していることを検討することを目的としている。

わが国では、2011 年の刑事訴訟法改正によりサイバー犯罪条約を批准するとともに、差押え対象となっている電磁的記録が差押え現場以外のサーバ等に蔵置されている場合には、当該差押え現場に存在するコンピュータからネットワークを介して接続されているサーバにアクセスして必要なデータを取得できるとする、いわゆる「リモートアクセス（遠隔捜索)」を許容する規定が導入されたところである（平成 23 年法律第 74 号「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」)。

もっとも、遠隔地に存在するサーバからデータを取得する際にはリモートアクセス先が海外となっている場合が考えられ、執行管轄の問題が簡単に発生してしまうとの懸念が改正当時より表明されていた。そのため、当時の国会審議の際の法務大臣答弁では、域外へのアクセスは控えられるべきであって国際司法共助に基づくと説明されていたところである。

かかる懸念は「クラウド・コンピューティング」の登場により一層深刻な問題として現実化している。一般に「クラウド(Cloud)」と呼ばれるこの技術は、複数のサーバの保存領域を活用してデータの保存を行うものである。これはコンピュータ資源の効率的な運用を可能とする革新的技術であり、特定のサーバにデータを蔵置する従来のストレージ・サービスの概念を大きく変えた。こんにち、個人ユーザから企業に至るまでそのサービスの普及は著しい。そのため、法執行の現場では、データの蔵置場所が特定されていない、あるいは域外に所在すると考えられるクラウドサーバにデータが保存されている場合の差押え方法について混乱が見られる。こうした事態はわが国固有の問題ではなく各国に共通のものであり、捜査機関による越境的なコンピュータ・データの証拠収集について既に海外では長い議論が重ねられている。

そうした中、2019 年５月には EU 一般データ保護規則(GDPR)が施行され、個人データを域外に移転する際には、公的セクター私的セクターの別を問わず強い規制が置かれ、データ移転や収集に関して国際的な法的枠組みに大きな修正が加えられることとなった。

本研究では、こうした海外のデータ移転をめぐる法状況を踏まえつつ、捜査機関による域外捜査に関わって米国と欧州で生まれた新たな法律並びに指令を紹介することにより、わが国における今後の域外データの取得方法について示唆を求めようとするものである。

2 クラウド・コンピューティングと越境捜索

2-1 問題の所在

国際公法上、管轄権には立法（規律）管轄権、執行管轄権、司法（裁判）管轄権の三つがある。越境捜索は執行管轄権に関わる。この執行管轄権については、捜査当局が実施する強制捜査は原則としてそれぞれの国家の領域内に限り認められるとされており、これを「属地主義の優位」と称する。したがって、外国の領土に立ち入って執行管轄権を行使できるのは、相手国との間で司法共助・捜査共助に関する特別の条約を結んでいる場合か、あるいは、相手国の明示もしくは黙示の同意がある場合に限られる。

もっとも、国外にある自国籍の船舶・航空機内での犯罪については管轄権行使が認められている。これは属地主義の反映と一般に理解されているが、船舶や航空機の場合は自国を拠点としていてもその移動先が容易に国外になり得るという特殊性から生まれた考え方である。しかし、サーバの物理的所在地が最初から海外にあるようなコンピュータ・データについてまでこうした例外的な考え方を類推することには疑問が生じ

公益財団法人電気通信普及財団
研究調査助成報告書　第37号　2022年度

てくる。
これまで、データの差押えのため捜査機関が域外データにアクセスするには、三つの方法が存在すると考えられてきた。すなわち、①データ蔵置国の承諾なく直接法執行を実施してデータを取得する（直接執行方式）、②データ蔵置国の法執行機関に協力を依頼し、間接的にデータを入手する（司法共助方式）、③相手国との協定・条約等に基づいて事前の包括的な合意の上でデータを取得する（協定方式）という三つである。もっとも、①の方法は前述の執行管轄権に抵触することになり妥当でない。そのため、わが国では先に触れた大臣答弁のように②が適当と考えられてきたのだが、この方法は関与するアクターが多数あって手続が大変煩瑣で時間を要するという意見が強かった。基本的なプロセスだけを見ても１０段階に渡って依頼・要請・命令・交付がリレーされることとなり、これらに要する手間と時間が迅速な証拠収集の妨げになると批判されていたところである。

2-２ 国内の判例状況

横浜地判平成 28 年 3 月 17 日（公刊物未登載）では、刑事訴訟法 219 条 2 項にいう「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「メールサーバの記憶領域」等が記載された捜索差押え許可状により被疑者方を捜索し、パーソナルコンピュータ（以下 PC）等を差し押さえようとしたところ、捜査機関にはメールサーバにアクセスするパスワードが判明していなかったためこの処分が実施されなかった。そこで捜査機関は、解析を経た本件 PC を用いて今度は検証許可状によってメールサーバに警察署内からアクセスし、被告人の利用するメールサーバが海外法人所有のものであると判明していたにも関わらず、特にこの点に顧慮することなく被告人のアカウントにログインして、同人のメールアドレスに関わる送受信メールをダウンロードし、これを保存した。
この事件の公判で弁護人は、上記経緯で入手された情報を手がかりに進められた本件捜査によって得られた証拠の排除が相当と主張した。裁判所は、本件メールサーバが米国法人のものであるため、当該メールサーバが他国に存在している場合にこれにアクセスすることは他国の主権に対する侵害が問題となり得るとし、捜査機関としては国際捜査共助を要請する方法によることが望ましいとした上で、主権侵害の問題等に適切な配慮を怠り捜査の目的を優先させて「検証許可状に基づくリモートアクセス」という法が許容しない捜査方法を断行した点に鑑み、捜査の違法は重大で令状主義の精神を没却するとして、検証の結果得られたデータをまとめた捜査報告書について将来の違法捜査抑止の見地から証拠能力を否定した（東京高判平成 28 年 12 月 7 日高刑集 69 巻 2 号 5 頁、控訴棄却）。
他方、京都地判平成 29 年 3 月 24 日（裁判所ウェブ登載）は、わいせつ電磁的記録媒体陳列、公然わいせつ被告事件につき、捜索差押許可状（リモートアクセス令状）に基づいて、捜査機関が被告人と共犯者らが共謀の上管理するサーバに対して、役員や従業員らから任意の承諾（基本的には口頭だが役員や主要な従業員については承諾書）を得て、その承諾に基づいてリモートアクセスして米国に本社があるグーグル社の提供するメールサーバ等からメール等の電磁的記録をダウンロードして収集し、承諾に基づいて電磁的記録をダウンロードした PC 本体の提出を受けてデータを収集し、また、被処分者の承諾を得て管理画面等を表示させてその画面を検証許可状に基づいて検証し写真撮影する等して収集した、というものである。
この事件では、被告人と役員らは顧問弁護士と相談の上、警察官らに対して上記メールサーバ等に警察側のパソコンを使ってアクセスできる別アカウントを付与し、警察署で押収対象データをダウンロードしてもらうこととして、最終的には被告人らもこれを承諾していた。
弁護人はこれら捜査時に収集されたデータについて違法収集証拠として争ったが、裁判所は、「現代社会においては、国際的なコンピュータネットワークが発達したことにより、国外のサーバに蔵置された電磁的記録を利用する権限のある者が、国境を越えて自由にアクセスして利用できることが当然の前提になっていることからすれば、その正当な権限のある者の合法的かつ任意の承諾が得られる場合において、その承諾に基づいて我が国の警察官が国外に設置されたサーバにリモートアクセスするなどしても、サーバ設置国の主権を侵害するものとはいえないし、必ずしもサーバ設置国の捜査共助を要請しなければならないものともいえず」、本件のリモートアクセスの場合は「サーバ管理者の意思に反してその権利・利益を侵害する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を用いたということはできず、強制処分には該当しない」として、弁護人の主張を退けて証拠として採用された（平成 29 年 1 月 20 日付証拠決定）。
判決も、任意の承諾に基づき電磁的記録をダウンロードしたパソコン自体の提出を受けて収集したこと、

そして、任意の承諾を得て管理画面等を表示するなどしてその画面上の表示を検証許可状に基づき検証して写真撮影したことを前提に、その収集過程に令状主義の精神を没却するような重大な違法は認められないとした。また、本件の事実関係においては、サーバ設置国の主権を侵害する重大な違法があるとも、サーバ管理者の権利・利益を侵害する重大な違法があるとも認められないとした。

控訴審である大阪高裁は、上記捜索に関して被処分者による任意の承諾があったとは認め難いとして違法があったと断じつつ、越境捜索については「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」で、「たとえサーバ所在国の主権侵害や海外のサーバ管理者の権利侵害があったとしても」、「我が国の刑訴法に準拠した捜査が行われている限り、関係者の権利、利益が侵害されることは考え」られず、「司法審査を経た本件捜索差押許可状に基づいて行われていると評価することができる」ので、証拠能力を失わせるほどの重大な違法には当たらない」と評価し控訴を棄却した（大阪高裁 2018 年 9 月 11 日裁判所ウェブ登載）。

３ 米国の動向：２０１８年クラウド法の制定まで

3-1 マイクロソフト事件

2016 年 7 月、合衆国第二巡回区裁判所はマイクロソフト社が求めていた連邦捜査局からのアイルランドに所在するメールサーバのデータ提出を拒否する権利を承認する判断を下した。

同社は、フリーメール・サービスを顧客に提供していたが、利用者のメールサーバが領域外であるアイルランドに所在していたところ、連邦捜査局は、ニューヨーク連邦地裁に対して Stored Communications Act(SCA)に基づいて蔵置されたメールデータの提出を求める令状を請求し、当該令状を取得した。同社は、当該サーバの所在地が域外である以上、当該令状は無効であると主張したが、これが地裁によって退けられたため上訴していたのである。なお、同社は合衆国内に蔵置されていたデータについてはすべて政府に提出している。訴外 Apple 社も本件について意見書を提出し、求められたデータを蔵置しているサーバの所在地に従って管轄を決定するべきだという見解を示していた。

第二巡回区裁判所は、SCA に基づく令状によって海外所在のサーバに蔵置されたデータを取得することは越境捜索に該当するため許容できないとした。また、こうしたケースは国際司法共助の枠組みを通してのみデータの取得が可能となること、また、合衆国政府はすべての国からデータを取得する能力を有するものではないことを指摘した。

これに対して連邦政府側が合衆国最高裁判所に上告し、2018 年 2 月 27 日に口頭弁論が開かれた。判事らの政府側に対する質問は厳しく、クラウド技術がない時代に作られた SCA に依拠することの問題が浮き彫りとなった。最高裁には、実に 32 本もの「外部からの意見書(amicus curie)」が提出され、それらのうちにはデータが所在していた欧州からのものも少なくなかった。欧州連合の政策執行機関である欧州委員会や英国政府等の公的機関を始め、欧州内の情報セキュリティの専門家集団や欧州内の国際法の専門家が意見を出しており、いずれも米国が同国の法律に基づいて単独で域外である欧州圏内からデータを取得することについて懸念が表明されていたのである。

3-2 クラウド法の制定

そうした中、2018 年 2 月に、捜査機関が域外サーバに蔵置されているデータを強制的に取得する手続を定めた通称 CLOUD Act が突如として議会に提案され可決され 3 月 23 日にトランプ大統領が署名、発効した。この法律の正式名称は”Clarifying Lawful Overseas Use of Data Act”と言い、クラウド・サービスをもじってクラウド法(CLOUD Act)と呼ばれている。捜査機関に対して、海外にあるサーバから米国市民に関するデータを直接収集することを許容することを目的として定められた。この法律が制定される以前には、米国内の企業が犯罪の証拠となるとしてクライアントに関するデータの提出を捜査機関から求められても、先のマイクロソフト事件のように当該データが域外に蔵置されていることを理由に提出を拒むという事態が生じていた。

ところが、このクラウド法の成立により、合衆国連邦捜査機関は米国を本拠とする企業が世界のどこにデ

ータを蔵置していても米国市民が捜査の対象となっている場合には関連するデータの提出を求める令状を得ることができるようになった。企業側がこの令状を受け取った場合、データが蔵置されている国のプライバシー法規に抵触しない限り、命令に応じなければならない。同法は次のように定めている（CLOUD Act Section 103(a)）。

> 電子的コミュニケーションあるいは遠隔コンピュータサービスを行うプロバイダは、顧客や契約者に関係する通信(wire)や電子的コミュニケーション、及び、いかなる記録や情報についてもこれを所有し、管理し、あるいは制御している場合、そのコミュニケーションや記録、その他の情報が合衆国の内外のいずれにあろうとも、保全(preserve)、バックアップ、あるいは提出(disclose)するという義務に［SCA による令状、裁判所命令、召喚状、あるいはその他の列挙されている背普段で政府に開示するよう要請があった場合は］服さなければならない。

また、合衆国政府は、特定の国と二国間協定を締結することにより、外国政府もしくは裁判所からの適法な命令があれば、合衆国内の企業に対して当該命令に応じてデータを提出するよう義務付けることができる。この協定は行政によって締結できるが５年毎に議会の審査を受けることとされている。

ただし、クラウド法には、裁判所が令状等を発付する場合に遵守すべき「礼譲(comity)」事項が置かれている。礼譲とは、国際法上権利問題としてではなく好意や他国の判断に対する尊敬に基づくという指針である。礼譲が要求されるのは、①要請されている開示が「適合する(qualifying)」外国政府の法律等に違反しているような場合、②状況を総合的に考慮すると開示が妥当でない場合、③開示要請の対象データが合衆国市民のものではない、あるいは合衆国に非居住者のものである場合と定められている。

②の総合考慮の内容としては、合衆国政府の利益、外国政府の利益、プロバイダが開示した場合に受ける制裁、対象者の居場所と国籍、プロバイダの業務の性質や範囲、捜査における必要性、開示によって発生し得る重大な損害、そして捜査の利益が挙げられている。クラウド法は、そうした考慮に基づいて裁判所が令状を取り消したり修正したりすることができると定める。

本法の成立を受けて、合衆国最高裁に係属していたマイクロソフト事件では 2018 年 4 月 17 日に実体判決無しの訴訟終了宣言がなされた。

４ 欧州の動向：２０１８年欧州指令の発出まで

4-1 越境捜索をめぐる枠組み

これまで欧州圏では、越境捜索の執行方法について二つの機関でその検討が進められてきた。第一は、人権､民主主義､法の支配の分野で国際社会の基準策定を主導する汎欧州の国際機関である欧州評議会(Council of Europe)である。欧州評議会では、インターネットに関わる犯罪とその捜査手続の国際合意を記したサイバー犯罪条約中に定める越境捜索を禁じた第 32 条を改訂するための検討が重ねられてきている。第二は、EU の執行機関である欧州委員会(European Commission)である。欧州委員会では、各国捜査機関による越境的な電子的証拠取得の方法が検討されており、欧州における統一的な執行方法の確立が目指されてきた。

4-2 サイバー犯罪条約改訂

2011 年に生まれたサイバー犯罪条約では、具体的な越境捜索のあり方について署名国に提案することができず、第３２条で以下のように定めて「原則的に」越境的なアクセスを禁止するという立場を採っていた。

> 締約国は、他の締約国の許可を得ることなく、以下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・データが地理的に所在する場所にかかわらず、当該データにアクセスすること。
>
> （ｂ）他の締約国に所在する蔵置されたコンピュータ・データを、コンピュータ・システムを通じて開示する法的権限を有する者の合法的かつ任意の同意が得られる場合には、自国の領域内におけるコンピュータ・システムを通じて、当該データにアクセスし、またはこれを受領すること。

本条項は、捜査機関による域外からのデータ閲覧やデータ取得を許容する条約締結国間における協調的手法を生み出すことができなかったことから策定された一種の「妥協案」であった。2001 年 11 月に日本が条

約に署名した当時、国際的に越境捜索をどのように執行すべきかについて意見の一致を見ることができなかったからである。

そうしたところ、2013 年、越境捜索に関して、より直接的で効果的な法執行権限を付与する場合に、どのような付加的な手続や条件、また安全策が必要とされるかを検討するため、専門家による特別部会が欧州評議会内に創設された。この部会のミッションは、インターネット上の越境捜索の実施についての可否に関わる提案と、権限を付与する場合の国際法と国家主権の原則の双方を満足させるような方法の開発であった。

同部会では、情報コミュニケーションがボーダレスになる一方、市民を犯罪から守る目的のために法執行機関が国境を超えて証拠を収集することが極めて困難となって、サイバースペースにおける法の支配が弱体化しているため、何らかの解決法が用意されなければならないという意見が支配的となった。

同時に、公聴会では、データ保護に関わる政府機関や、ICT 産業等の私的セクターといった様々な立場からの要請を反映することが容易でないことも明らかとなったため、越境捜索から個人の権利を保護し、その濫用を防止する安全策と条件が整えられる必要があることが明らかにされた。

その上で、即時の改訂が困難であるとしても、特別部会は当面、注釈書の改訂を目指すべきであり、その場合に考えられる実際的な越境捜索として以下のような方向性が示された。すなわち、①同意に基づく、制限のない越境捜索、②同意はないが合法的に獲得された信任状に基づく越境捜索、③緊急もしくはその他の事情がある場合の越境捜索、④自己の管轄と同様の制限のない拡張された捜索、⑤関連する処分権、である。

そして、2013 年の中葉までに準備される条約改訂に向けて私的セクター等からの意見聴取を進め、2014 年末までに 32 条注釈の改訂を目指すことが提案され、2014 年、特別部会から暫定報告書がまとめられた。ところが、2013 年頃から欧州連合において個人データに関するより強固な保護を進める政策が進められた結果、特別部会に対してもデータ保護に関する厳格なルールへの変更が伝えられ、調査活動の延長が余儀なくされることとなった。個人データの移転を規制する EU 一般データ保護規則(GDPR)の施行が決まったためであった。GDPR の策定は欧州圏におけるデータ保護政策の強化を意味するが、そうした動向が特別部会、ひいては欧州評議会において安易な越境捜索に対する制限的な姿勢を強めるきっかけとなっていった。

GDPR の施行により、他国の法執行機関が欧州圏から越境捜索によってデータを取得する場合には、欧州におけるデータ保護基準に従わなければならない。そうなると、越境捜索にあたっては、条約加盟国であっても正当な権限がある場合でも、常に相手国ないし相手地域のデータ保護基準を順守しなければ国際法上違法なデータ移転と見なされることになってしまう。

現実には多くの国の法執行機関が、域外からデータの所在地が不明なまま一方的な越境捜索を進めていたが、そうした行為はプライバシー侵害やコンピュータ濫用罪に該当し得る。特別部会はかかる状況を「ジャングル状態」と呼んで何らかの規制が必要であるとの見解を示した。

4-3 2018 年欧州新指令

こうした欧州評議会の動きとは別に、欧州連合の公式の執行機関である欧州委員会においても、捜査機関による電子的証拠の越境的収集方法について検討が進められている。2015 年 4 月に欧州委員会において「安全に関する欧州アジェンダに関するコミュニケ」が発出された際にも、オンライン上の電子的証拠(e-Evidence)の取得問題の解決を目指すことが表明されていた。これを受けて、2016 年 6 月、欧州理事会(European Council)からは「サイバースペースにおける刑事司法の改革に関する結論」と題する文書が公表され、プロバイダとの協力推進や捜査共助の効率化やサイバースペースにおける執行管轄の判断の解決策を講じることとされた。

その背景には、各プロバイダに対する加盟国からの捜査の必要のあるデータの提出要請が年々増加していることが挙げられる。すなわち、2013 年には提出要請は 3 万 5 千件程度であったが、2016 年には 6 万件を超え、今後もその増加は激しくなると予想され、産業界からも犯罪捜査の証拠となるデータを迅速かつ効率的に収集するための法的枠組みの整備が求められるようになっていたのである。

欧州理事会が欧州委員会に対して 2017 年 6 月までに中間報告を行うことを求めたため、欧州委員会は、加盟国の実務者や私的セクター、人権 NGO 等から意見を聴取し非公式回答書が策定された。

こうして、欧州における捜査機関による域外データ取得につき、従来の主要なルートであった捜査共助方式に代えて差押え対象となるデータを蔵置しているプロバイダに対して捜査機関が開示請求あるいは開示命令を出すという官民協力方式が採用されることが確定したのである。

2018 年 4 月 18 日、いよいよ欧州理事会が新指令を発出し、「欧州データ保全命令(European Preservation Order: EPO)」ならびに「欧州データ提出命令(European Production Order: EPrO)」を創設するとともに、欧州域内においてデータ・サービスを行う全てのプロバイダは代理人を置くことを義務付けられ、かかる命令に関する当局からの命令を取り扱う窓口とするという計画が発表された。

これまで欧州圏では、捜査共助に基づくデータ（電子的証拠）の取得（10 ヶ月以内）や 2017 年に創設された欧州捜査令状(European Investigation Order: EIO)に基づく相手国における司法機関・捜査機関を通じたデータの取得（120 日以内）といった方法が取られていたところ、今回発出された指令の定める「欧州データ提出命令」では、捜査対象となっているデータを保有するプロバイダに対して通常で 10 日以内、緊急の場合には 6 時間以内のデータの提出を義務付けるという官民協力を前提とする。

対象となるデータは４つに分類され、加入者データ、アクセスデータ、処理に関するデータ、コンテンツ・データである。最初の二つのデータはあらゆる犯罪に関して処分の対象となり、後の二つは刑量が長期３年以上のサイバー犯罪が対象とされている。

もちろん、新指令のこうした提案については批判もある。例えば、プライバシー擁護団体からはアクセスデータや加入者データが容易に収集され過ぎるとの懸念が表明されており、直接法執行機関から私企業への命令が可能になることで「中間項」が省略されてしまい、私企業における過度のコンプライアンス負担や法執行機関による権限濫用の虞も生じると指摘され、大量監視に対する防御策が十分に講じられていない等、枠組みの不十分さが批判されている。

とはいえ欧州でも、犯罪捜査に関わって域外においてアクセスならびに取得したいデータを蔵置するプロバイダ（事業者）に対して直接請求する方法が主流となっていくと考えられる。この新指令は欧州議会では執筆時点ではまだ採択されていないが、新指令の方向性がどのように反映されるのか注目されるところである。

５ おわりに

米国のクラウド法も、欧州新指令も、プロバイダに対してデータの提供を求める新しいタイプの越境的なデータ取得方法を導入した。そうした中で、日本の最高裁判所は前述ケース②の上告審で、２０２１年２月１日、警察による越境的なデータ取得に際して被処分者による同意承諾の取得手続に違法があったとの判断を示しつつ、かかる越境捜索を重大な違法とはみなすことがなかった（刑集７５巻２号１２３頁)。

しかしながら、GDPR４４条は「移転の一般原則」において、現在処理中の、または処理を予定されている個人データのいかなる移転も、第三国または国際組織から別の第三国または別の国際機関への個人データの再移転を含めて、４５条以下の条件遵守を求めており、同４８条は例外的な場合を除いて、行政機関（捜査機関を含むと解される）や裁判所の決定について移転・開示を禁止しているのである。

欧州においては、個人のデータ移転が例外的に認められるためには、国際協定の締結が条件とされているのである。無論こうした要請には特例（例外）が存在するが、作業部会では個人データ移転にかかる特例の適用を制限的に解すべきとされていて、「公共の利益の重要な理由のために必要な場合」の移転が認められると規定されているものの（同４９条１項ｄ号)、テロ対策を目的とする捜査のためのデータ移転であっても第三国の機関からの要請だけでは不十分で、GDPR は EU または加盟国の法律から導かれる公共の重要な理由がある場合に限ってこの条項が適用されるとの厳格な方針が示されているところである。

以上、本研究を通じて明らかになった欧米の動向は、わが国の法執行機関による域外データ取得問題について示唆的であろう。２０１１年の改正法によりプロバイダに対するデータ保全の要請が導入されたが(刑訴法１９７条３、４、５項)、これはあくまで国内プロバイダが管理する域内のデータが対象と考えられており、域外データや域外にあるプロバイダはそもそも処分の対象とされていなかった。そのため前出の国内事例に見られるような現場の混乱を招いていると言えるだろう。クラウド法や欧州新指令では、わが国でこれまで検討もされたことがなかったプロバイダ協力方式が採用されたため、わが国でも今後は海外からのデータ提出要請に応じる処分の創設や、欧米諸国との二国間協定の締結などが課題となって来るはずである。越境的なデータ取得に向けた法執行のあり方について国際動向を見据えた対応が求められなければならない。

（了）

〈発表資料〉

題名	掲載誌	年月日
越境するデータ，越境する捜索――域外データ取得をめぐる執行方式に関する欧米の立法動向＜論説・解説＞	Ｌａｗ＆Ｔｅｃｈｎｏｌｏｇｙ ８２号 ４５～５７頁	２０１９年1月
海外サーバからの電磁的記録の差押え等の適法性が争われた事例（平成３０．９．１１大阪高判）	『速報判例解説（２４）(法学セミナー増刊)』所収 １８７～１９０頁	２０１９年4月
特集の趣旨（特集 サイバー捜査における諸問題）	自由と正義 ７１巻1号 １７～２０頁	２０２０年1月
越境捜索を合憲適法とした最高裁判所令和３年２月１日決定――クラウド時代における域外データ取得方法とその課題	Ｌａｗ＆Ｔｅｃｈｎｏｌｏｇｙ ９２号 ４０～４４頁	２０２１年7月
最高裁判所決定の背景と問題の所在（令和３．２．１最高二小決）	Ｌａｗ＆Ｔｅｃｈｎｏｌｏｇｙ ９３号 ３２～３６頁	２０２１年１０月

【参考文献】

Microsoft Corp. v. United States, 829 F.3d 197 (2016)

18 U.S.C. §§2701-2712(2012)

In re Warrant to Search a Certain E-mail Account Controlled & Maintained by Microsoft Corp., 15 F. Supp. 3d 466 (S.D.N.Y. 2014)

Ad hoc sub-group of the T-CY on jurisdiction and transborder access to data and data flows Terms of Reference, T-CY(2011)5E (2011)

Cybercrime Convention Committee(T-CY) Ad-hoc Subgroup on Transborder Access and Jurisdiction, T-CY(2013)30

Cybercrime Convention Committee(T-CY) Transborder access to data and jurisdiction: Options for further action by the T-CY, T-CY(2014)16

T-CY Guidance Note #3 “Transborder access to data (Article 32)”, (3 Dec., 2014)

Article 29 Data Protection Working Party, Working Document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995

『情報通信白書平成２８年版』

宮下紘『EU 一般データ保護規則』(勁草書房、２０１８)

杉原高嶺『国際法学講義 第２版』(有斐閣、２０１３)

小松一郎『実践国際法 第２版』(信山社、２０１５)

杉原他『現代国際法講義 第５版』(有斐閣、２０１２)

小寺ほか『講義国際法 第２版』(有斐閣、２０１０)

酒井ほか『国際法』(有斐閣、２０１１)

丸橋透「刑事における電子証拠の欧州提出命令及び欧州保全命令」法と情報雑誌第3巻第8号(2018)201~275頁

夏井高人「指令 2014/41/EU」法と情報雑誌第 3 巻第 7 号(2018)199~245 頁

「米 MS、国外サーバーの保存データ開示問題で勝訴」日本経済新聞２０１７年７月１５日付
「米最高裁、マイクロソフトの国外保存メール開示問題で審理へ」ロイター2017 年 10 月 17 日配信。