押収済みパソコンを用いて検証許可状に基づき海外メールサーバにアクセスした捜査に重大な違法があるとして証拠を排除した事例

【文 献 種 別】 判決／横浜地方裁判所
【裁判年月日】 平成 28 年 3 月 17 日
【事 件 名】 有印私文書偽造、有印私文書偽造（変更後の訴因有印公文書偽造）、有印公文書偽造、建造物損壊、非現住建造物等放火被告事件
【裁 判 結 果】 有罪
【参 照 法 令】 刑事訴訟法 218 条 2 項・219 条 2 項
【掲 載 誌】 判例集未登載
LEX/DB 文献番号 25542385

事実の概要

1 被告人Xは、国立大学の学生証、危険物取扱者免状、自動車運転免許証、私立大学の学生証、のそれぞれを偽造した事件および建造物損壊と非現住建造物等放火の事件で起訴された。これに対して被告人はいずれの事件にも関与を否定した。

2 捜査段階において、神奈川県警生活安全部生活安全総務課サイバー犯罪対策室は、平成 24 年 9 月に携帯電話通信役務の不正な利用の防止に関する法律ならびに偽造有印公文書行使幇助の罪でXを通常逮捕し、それらの被疑事実に基づいて捜索差押許可状の発付を受け、鹿児島県鹿屋市のX方を捜索し、パーソナルコンピュータ（以下 PC と略）等を差し押さえた。

3 上記許可状は刑事訴訟法 219 条 2 項の「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、いわゆるリモートアクセスによる複写処分が許可されていた。しかし差押えの時点で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、捜査機関はこの処分を実施できなかった。

4 その後捜査機関は解析を経た本件 PC を用いて、検証許可状によってメールサーバにアクセスを試みることとした。その際、捜査機関は、Xが利用するメールサーバが海外法人P社所有のものであると判明していたことから、当該サーバが海外に所在する可能性が高いことを認識していたが、特にこの点に顧慮することなく検証許可状を得て、Xのアカウントにログインし、X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。

5 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相当数の証拠は違法収集証拠に当たるとして、証拠排除が相当と見るべきだと主張した。

判決の要旨

1 刑訴法 218 条 2 項で電子計算機の差押えの際のリモートアクセスによる複写として許容された処分とは、「電子計算機を差し押さえるに当たり、当該電子計算機に接続されたサーバ内に記録されている、当該電子計算機から作成・変更・消去が可能なデータを当該電子計算機等に複写した上で、同電子計算機を差し押さえる処分」のことをいい、電子計算機の差押えに先立って行われるものであって、本処分が当該電子計算機の差押え後に実施されることは法律上想定されていない。

2 そうすると、捜査機関が検証許可状に基づいて本件 PC の状態を検証する権限を有することになったとしても、その PC からネットに接続して被告人が利用しているメールサーバにアクセスすることは当然には許されない。

3 メールサーバ上のメール送受信履歴とその内容は、サーバ管理者等以外は閲覧することが予定されておらず、捜査機関がそれを閲覧した上、内容を保存する行為は管理者等の権利・利益を侵害する強制処分に当たる。

4 本件メールサーバは米国法人のものであり、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、当該他国の主権に対する侵害が問題となりうる。この点についての国際的に統一された見解は存在せず、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。本件での捜査機関によるメールサーバへのアクセスならびにXの送受信記録の閲覧と複写保存は、不正アクセス行為の禁止等に類する法律上の問題ともなりうる。

5 確かに、本件では捜査機関においては検証許可状を取得しているので令状主義を潜脱する意図があったとは認められない。しかし、主権侵害の問題など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れば、法令遵守の姿勢が欠けていたことも否定できず、検証に基づく捜査の違法は重大で令状主義の精神を没却するとの評価を免れない。

6 以上の判断に基づき、裁判所は、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。他方で、それ以外の証拠については、いずれの公訴事実との関連性を見てもそれ自体が否定されるか、あるいは肯定したとしても密接性が否定されるほか他の証拠から犯罪事実の認定ができるとして排除相当とは考えられないとし、証拠排除がなされなかった証拠に基づいて有罪と判断し、懲役8年（求刑9年）を言い渡した。

判例の解説

一 本判決の背景と意義

1 法改正まで

2011（平成23）年に成立した刑事訴訟法改正によって、日本のサイバー犯罪捜査は大きく変化を遂げた。改正は、我が国が2001年11月に署名し、2004年4月に承認された「サイバー犯罪条約」の諸条項に対応する国内法整備の一環として進められてきたものである。2004年には「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、翌年から審査が開始されたが、審査未了となっていた。そこで内閣は国会に対し、大きな争点であった共謀罪を除いた「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案」を2011年4月1日付で提出した。法律案は同年6月17日に可決成立し、同月24日に公布された。

2 改正の内容

同改正では、実体法関連のものではウィルス作成罪が導入され、手続法関連では以下の6項目の改正・創設があった。①これまで物理的な対象物が捜索差押えの客体であったところ、「電磁的記録媒体の差押えの執行方法」と、これを被処分者に命令して記録することのできる「記録命令付き差押え」の創設（刑訴法99条2項他）、②捜索差押え処分の対象となっているコンピュータが電気通信回線で接続された外部のサーバ等にデータを蔵置している場合に、かかるデータを捜索差押えの対象となっているコンピュータを通じて複写することを許可する「電気通信で接続している記録媒体からの複写」（通称リモートアクセス）（99条の2他）、③執行を受ける者への「協力要請」（111条の2）、④通信事業者への通信記録に関する60日を超えない保全要請（197条3項）、⑤秘密保持要請（197条5項）、⑥有体物の没収に代わる不正に作られた電磁的記録の没収（498条の2）である。

法案審議の過程において、上記第2のリモートアクセスにつきクラウド・サービスなどの端末から外部への常時接続が普及している今日の技術ならびに利用者環境を前提とすれば、日本国外にあるサーバへの捜索差押え行為が容易に発生しかねないことが予想され、かかる場合についての限界づけが必要という問題が生まれた[1)]。法改正の契機となった「サイバー犯罪条約」でも第32条にリモートアクセスが規定されていたところ、同意承諾のない越境的な捜索に関する言及はなかった[2)]。そのためリモートアクセスが「越境捜索」として許容されるのか否かについて条文上明確にされないまま改正が行われた[3)]。

3 判決の意義

本判決は、同法改正後初めて海外サーバに対する無承諾のリモートアクセス、すなわち域外捜査の適法性について裁判所が判断したものであり、大きな意義をもつ。内容面でも、刑訴法218条2項（前述の99条2項準用）に定める、リモートアクセスに基づく複写処分について、これを差押えに先立ってのみ実施することが許されると解した点および、差押え後に捜査機関が検証許可状を用いて実施された無承諾アクセスによってサーバに蔵置されていたメールの送受信記録の閲覧保存行

為を違法と断じ、かかる捜査によって得られた証拠を排除した点が重要である。

なお、本判決は証拠収集手続の違法が及ぶ範囲について各犯罪事実との関係を個別に審査してその射程を確定しているが、日本で初めて捜査機関の遠隔捜査の適法性を正面から扱い、かつ違法判断を示した点に鑑み、本稿では証拠排除の射程範囲については評釈対象としていない。

二　リモートアクセスの許容範囲

1　域外捜索禁止の原則

本件捜索差押えに当たって捜査機関が得ていた捜索差押え許可状には可能な処分として「リモートアクセスによる複写処分」が記載されており、また複写すべきものの範囲として「メールサーバの記録領域」が明示されていた。したがって、被処分者のコンピュータに接続するインターネット上の記録領域にアクセスすることができていれば捜査機関はこれを複写することも許されたと解される。判決は、捜査機関が被処分者のコンピュータを差し押さえた後、検証許可状を得た上で海外サーバにアクセスして記録を取得した点に関わり、サイバー犯罪条約 32 条が「当該アクセスが同意に基づく場合は又は当該データが公に利用可能な場合という限られた場合を除いて、どのような場合にリモートアクセスによる複写の処分が許容されるかを明示していない」ことを踏まえて、サーバが海外に存在すると認められる場合については「基本的にリモートアクセスによる複写の処分を行うことは差し控え、国際捜査共助を要請する方法によることが望ましい」として、「(捜査共助によらず海外に存在するメールサーバからデータを取得するような) 処分を行うことは基本的に避けるべきであった」と判示し、コンピュータ・ネットワークを介した域外捜索を回避し国際捜査共助を原則とするとの指針を示した点が重要である。

2　リモートアクセスの時期的限界

また、判決が「リモートアクセスによる複写の処分は、電子計算機の差押えに先立って行われるものであり、差押え終了後に行うことは想定されていない」と判示した点も重要である。すなわち、改正刑訴法 218 条 2 項は「当該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つて、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」からのデータの差押えを許容しているところ、判決は同項にいう「状況」が現存している、すなわち有体物であるコンピュータが外部に接続している状態での差押えに限定されるという文理解釈を示した。

3　善意の例外

なお、仮にメールサーバが海外に蔵置されてるかどうかが不明なまま捜査機関において記録の複写が実施された場合の違法性について判決は言及していない。この点、将来、令状主義の潜脱の意図がなかった、すなわち一種の「善意の例外」として扱われる余地は残されていよう。

三　海外サーバへのアクセスを伴う捜査手法

1　域外捜索の方法

サイバー犯罪条約ではその 32 条に、対象となるデータが「公に利用可能」な場合やデータについて「正当な権限ある者の合法的で任意の承諾」があるとき、締約国が他の締約国の個別の許可なくアクセスすることを許容する規定を置く。条約が許容を予定する場合以外に域外サーバに捜査機関がアクセスする「越境捜索」の枠組みとしては、おおよそ次の 3 つの方法が考えられる。

第 1 は、相手国やアクセスするデータの管理者等の承諾なく行うものであり、捜査機関が特に法的権限ないまま外国に所在するサーバに承諾なくアクセスするか（諜報機関が行っている非合法な手法[4]）、あるいは、国内法によって域外サーバへのアクセスを許容するような法制度を設ける方法である。後者の例として、2014 年に初めて米国議会に上程され、2015 年に再上程された、米国のプロバイダが海外にデータを蔵置している場合で当該データが米国市民に関する者であるときに法執行機関に越境的捜査を承認する THE LAW ENFORCEMENT ACCESS TO DATA STORED ABROAD ACT (“LEADS ACT”) がある[5]。いうまでもなく、主権のある他国の管轄に相手国の承諾や相手国に通知なくアクセスするわけであるから、相手国におけるハッキング相当の犯罪行為となりうるものであり[6]、本判決文中にも権限を有する者の承諾なく行ったサーバへのアクセスは不正アクセス等に該当すると指摘されている[7]。

第 2 は、国際捜査共助に基づき相手国の捜査

機関に対象となるサーバにアクセスしてもらい、取得すべきデータを入手するよう依頼する方法である。国会答弁等でも日本国の公式見解はこの方法を取るべきとされており、学説も主権国家間のサーバ侵入は主権の侵害に当たることからこの方法を支持している[8)]。ただし、この方法による場合はデータ取得の必要性が生じた時点から時間を要することや相手国への協力依頼に手間を要すること等の実務上の難点が指摘されている[9)]。

第3は、事前に協定・条約等において参加国同士で法執行機関による越境的アクセスについて一定の留保や条件の下で実施することを了解する相互承認型の方法である。前記条約締結当時は越境的捜索が許容されるかについて議論がまとまらず、条約注釈においても「一般的なルールを策定することは困難」であるとされていた[10)]。しかし、その後欧州での議論の深化を受け、2017年5月からこの相互承認型のEuropean Investigation Order（欧州捜査令状）という令状方式が実施されようとしている[11)]。同令状は、免責ないし証人保護、国防上の観点、情報への到達不可能性、当該捜査行為と同種の手法が存在しないといった例外を除いて締結国は承認を拒否できないとされており、対象はコンピュータ関連犯罪で最低3年以上の刑期が予定されている罪種となっている[12)]。

2　捜査共助と相互承認型捜索について

判決文によれば、本件においても捜査機関は上記検証許可状でのアクセス後に暫時日米司法共助条約に基づいて捜査共助の要請を行っていたようであり、全く上記第2の道が全く考慮されなかったわけではないようである[13)]。この点、刑訴法改正時の注釈類においては、「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（電気通信回線で接続している記憶媒体からの複写のこと・筆者注）を行うことは差し控え、当該他国の同意を取り付けるか、捜査共助を要請することが望ましいのではないか」として、上記第2か第3の手法を採るよう示唆されているところであった[14)]。本判決が第2の捜査共助のみを検討して第3の可能性については言及していなかったこと、改正時の国家公安委員会規則の整備に関わっても第2の捜査共助のみが具体的に例示されていたこと、そして相互承認型の令状方式が国会で議論された経緯がないこと等に照らすと、現時点で第3の手法は日本ではまだ現実的とはなっていないと解さざるを得ないであろう。

●――注

1）拙稿「サイバースペースにおける証拠収集とデジタル証拠の確保――2011年改正法案を考える」法時83巻4号（2011年）84頁、特に87～88頁を参照。

2）サイバー犯罪条約については、以下の外務省サイトhttp://www.mofa.go.jp/mofaj/gaiko/treaty/treaty159_4.html（2016年12月27日閲覧）参照。

3）筆者は改正法案審議時に参考人として召喚された際に、この点について疑問を指摘していたところである。まさにその懸念が具体化したのが本件であろう（平成23年5月31日衆議院法務委員会議事録参照）。

4）この点、スノーデン事件が明確な証拠となろうが、ここでは詳述しない。

5）https://www.congress.gov/bill/114th-congress/senate-bill/512/text（2016年12月27日閲覧）。

6）越境的捜索事例につき、FBIがロシアのハッカーに関する証拠を収集するためロシア国内のサーバに侵入し、起訴まで至ったゴルシュコフ事件参照。当該事件につき裁判所は、被告人側の修正4条違反に対して憲法修正条項は域外に適用されないとしてその主張を退け有罪を言い渡している。United States v. Gorshkov, No. Cr00-550C, 2001 WL 1024026 (W.D. Wash. May 23, 2001).

7）Comment, Law Enforcement and Data Privacy: A Forward-Looking-Approach, 125 Yale L. J. 543 (2015-2016); Comment, A Step in the Wrong Direction: The Case for Restraining the Extraterritorial Application of the Stored Communication Act, 42 Rutgers Computer Tech. L. J. 26 (2016); A. K. Woods, Against Date Exceptionalism, 68 Stanford L. Rev. 729 (2016).

8）井上正仁「コンピュータ・ネットワークと犯罪捜査（2・完）」法教245号（2001年）49頁等参照。

9）この問題につき、Ian Walden, Computer Crimes and Digital Investigations, Oxford. 2016, see at 325-340.

10）なお、王志安「越境コンピューター捜索の法的地位――サイバー犯罪条約の残した課題」駒沢法学3巻3号（2004年）1頁（132頁）も参照。

11）Directive 2014/41/EU of the European Parliament.

12）Jodie Blackstock, The European Investigation Order, New J. of European Crim. L. vol. 1, Issue 4, 481 (2010); Anthony Farries, The European Investigation Order: Stepping Forward with Care, New J. of European Crim. L. vol. 1, Issue 4, 425 (2010).

13）平成26年版犯罪白書によれば、警察による共助要請は平成24年で62件、受託は98件であった。

14）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）」曹時64巻5号（2012年）55頁、101頁。

成城大学教授　**指宿　信**