NISHIMURA
& ASAHI

西村高等法務研究所

「CLOUD Act (クラウド法) 研究会」

報告書

――企業が保有するデータと捜査を巡る

法的課題の検討と提言――

2019 年 12 月

西村高等法務研究所

Nishimura Institute of Advanced Legal Studies

〒100-8124
東京都千代田区大手町 1-1-2 大手門タワー

西村高等法務研究所(NIALS)「CLOUD Act (クラウド法) 研究会」参加者(敬称略)

≪座長≫
東京大学大学院法学政治学研究科　教授　宍戸　常寿

≪委員≫
防衛大学校人文社会科学群国際関係学科　准教授　石井　由梨佳
東京大学大学院法学政治学研究科　准教授　成瀬　剛

≪事務局≫
西村あさひ法律事務所　弁護士　藤井　康次郎
同　北條　孝佳
同　石戸　信平
同　津田　麻紀子
同　角田　龍哉
同　和光　真理江
同　河野　充志
同　岩谷　雄介
同　木村　響
同　室町　峻哉

≪プレゼンテーション、ヒアリング等、協力企業≫
研究会においては、以下の国内外の通信系や IT 系の企業・団体より、ヒアリング等の協力を得た。

エヌ・ティ・ティ・コミュニケーションズ株式会社
Twitter Japan 株式会社
日本マイクロソフト株式会社
株式会社メルカリ
ヤフー株式会社
LINE 株式会社
在日米国商工会議所
他 2 社

*本研究会としての提言を含む本報告書の内容は、あくまでも NIALS としての見解を示すものであって、本研究会における座長、委員又は協力企業の見解を示すものではありません。

目　次

第1. 本研究会の目的及び本報告書の構成

2018年3月23日、米国において、捜査機関が、企業が国外に所在するサーバに保存しているデータ[1]の開示命令等を行う際の手続きを明確化したClarifying Lawful Overseas Use of Data Act(以下「**CLOUD Act**」という。)が成立した。これを受け、西村高等法務研究所(以下「**NIALS**」という。)は、2019年3月13日、CLOUD Actに関するシンポジウムを開催し、これにまつわる日本の産官学の問題意識の向上を図った。

そして、NIALSは、日本におけるCLOUD Actへの対応を出発点に、広く企業が保有するデータの捜査目的での取得の在り方について、日本の法令や国際法上の課題に加え、国家間及び官民の連携の在り方に関する課題を整理し、提言を行うことを目的として、CLOUD Act (クラウド法) 研究会(以下「**本研究会**」という。)を設置した。本研究会は、法学者が委員となり、弁護士が事務局となって運営された。本研究会における検討の過程では、相当数の国内外のインターネット企業やデータ企業からのインプットも得た。そしてで、本研究会の成果を取り纏めたものとして、本報告書を作成した。

本報告書の具体的な構成は次のとおりである。まず、**第 2.**において本報告書の提言を述べる。次に、**第 3.**において企業が国外に保有するデータの取得の在り方に一石を投じたCLOUD Act の概要・意義を把握する。これを踏まえた上で、**第 4.**では、企業が保有するデータを取得する捜査手法を巡る日本法上の課題を、**第 5.**では、特に企業が保有するデータが国外に保存されている可能性がある場合についての課題をそれぞれ整理・検討する。その後、**第 6.**では、日本が米国と行政協定を締結することによりそれらの課題を解消することも含めて、企業が保有するデータを取得する捜査手法を巡る国際的な連携の在り方に関する一定の示唆を提示する。さらに**第 7.**では、こうした課題・実情を意識しつつ実施されている、国内外の企業における捜査を目的としたデータの取得への実務対応の現状と、今後の展望に言及する。最後に、**第 8.**では、企業が保有するデータを取得する捜査手法に関する課題の整理・検討が、データの自由な移転を巡る政策等に与え得る示唆・影響と、その重要性に触れる。なお、本報告書で取り上げる主な法令や条約等については、参考資料として本報告書末尾に添付する(**参考資料：関連条文集**)。

本研究会の提言とそれを支える法的検討が、企業が保有するデータと捜査を巡るこれからの日本における法政策や国際的な枠組み作りに関する検討の一助となれば幸いである。

第2. 本研究会の提言

企業におけるデータの蓄積が進み、また、データが国境を越えて活発に移転するようになった昨今においては、日本で犯罪が行われていても、当該犯罪の捜査にとって重要な証

[1] 本報告書では、企業が管理等の権限を有するサーバに保存されたデータを「企業が保有するデータ」と表現し、国外に所在するサーバに保存されたデータを「国外に保存されたデータ」と表現することがある。なお、「管理等」の意味については後記脚注20参照。

拠となるデータを企業が保有し、しかも、当該データを保存したサーバが海外に所在する場合が増えている。そのような中で、被疑者の端末内に保存されたデータを取得することのみならず、企業が国内外において保有しているデータを取得することも、日本の捜査機関が捜査に必要なデータを効果的に取得し、日本の刑罰法令を適切かつ迅速に適用実現する上で重要な意義を持つようになっている。CLOUD Act は、そのための仕組み作りの一例として参考になる。

もっとも、企業が保有するデータの捜査を目的とした取得の場面では、データの内容に関係する本人(以下「**データ主体**」という。)[2]の権利の保障や、データを保有する国内外の企業の負担にも配慮し、さらには市民社会の理解を得ていく必要もある。

また、データは改変や消去、暗号化等による隠滅が容易であるため、そのようなデータの特性を踏まえた、捜査の実効性を担保する方法についても検討が必要である。さらに、企業が保有するデータが国外に保存されている可能性がある場合には、国際法との整合性や国際連携の在り方についても整理が求められる。

以上のような問題状況を踏まえ、NIALS としては、以下を提言する。

1　企業が保有するデータを取得する捜査手法の更なる活用と新たな制度設計の検討：

日本の国内法上、捜査を目的としたデータの取得に対しては既に一定の制度設計とそれに基づく実務的対応が進んでいるものの、依然として課題が残っている。これらの課題に対して、まず短期的には、企業とも連携しながら、記録命令付差押えを積極的に活用することを通じて、データ主体や企業の利益にも配慮しつつ、企業が保有するデータの効率的かつ実効性のある取得を実現すべきである。そして、より中長期的には、データ主体や企業に対する通知等の整備を含めた手続きの公正性・透明性の担保、秘密保持の義務付け制度等の拡充、令状手続の電子化、データの保護に関する他の法令との関係性の整理等の様々な観点から、制度設計の在り方を巡る議論を深めていく必要がある(後記**第 4. の 1.**)。さらに、この制度設計の検討においては、取得できたデータの公判での利用も見据えた検討も求められる。すなわち、裁判所において証拠として提出されたデータの真正性や証明力を適切に評価するための、客観的な指標(標準等)を構築することが望ましい(後記**第 4. の 2.**)。

2　捜査目的での越境的なデータの取得に関する国際法上の議論の深化と国家間の枠組み構築への参画：

各国の捜査機関が国外に保存されたデータを取得する方法を巡る国際法上の評価ついては、国内外で議論が行われている。国際法上、他国の領域における管轄権の行使は主権侵害に当たるが、他国領域に所在するサーバに保存されたデータを捜査により取得することは、例えば、国内の企業に対して国外に保存されたデータの提出を命じ

2　データの内容に関係する「本人」という場合には、典型的には、個人情報の保護に関する法律(以下「**個人情報保護法**」という。)上の「本人」(同法 2 条 8 項)として想定する主体を想定している。

る場合等、手法次第では必ずしも他国の領域における違法な管轄権の行使とはいえないと整理することも可能である。日本としては、適切かつ迅速に国外に保存されたデータを取得することの重要性に鑑みて、他国の主権を尊重するとの姿勢を堅持しつつ、国際法に適合的な手法の検討を深化させるべきである(後記**第 5.の 1.**)。また、国際連携の進め方については、サイバー犯罪条約の追加議定書の検討に代表されるような多国間での枠組みの構築のみならず、EU のような特定の域内での連携を深める取組みや、CLOUD Act に基づく二国間での行政協定が想定しているような有志国間での連携構築を足がかりにしていく取組みも想定できる。その中で日本としては、信頼ある自由なデータの流通(Data Free Flow with Trust、以下「**DFFT**」という。)の理念に沿って、価値観を共有できる有志国間で先行して、着実に枠組み作りをしていくことが効果的であると考えられる。そのような観点からは、米国をはじめとする有志国との二国間での国際協定の締結も視野に入れ、必要な法的論点の検討を進めておくことが望ましい(後記**第 5.の 2.**、**第 6.**及び**第 8.**)。

3　企業におけるパブリック・アクセスに対する透明性確保の取組みの推進：

企業が保有するデータの捜査目的での取得について、データ主体や市民社会の理解を得る上では、政府レベルでの取組みに加えて、公的機関による企業が保有するデータの提供要請(パブリック・アクセス)に関する透明性を確保するための企業や産業界側での自主的な取組みも重要となる。このような取組みは、企業にとって、データ主体である利用者に安心感を与え、市民社会全体の企業に対するイメージも向上し、長期的には企業の競争力の源泉や利益にも資するものである。そこで、今後、企業や産業界の側においても、パブリック・アクセスに関する透明性の確保に向けた具体的な取組みについての議論がさらに深まり、その実践も増えていくことが期待される(後記**第 7.**)。

第3. CLOUD Act の概要

1.　制定の背景

米国において、CLOUD Act が制定される前は、電気通信サービス(electronic communication service)等のプロバイダに対するデータの開示手続等を定めた Stored Communications Act (以下「**SCA**」という。)等の法令上、米国の政府機関が、米国外に保存されたデータの提出を命じることを明示的に認める規定はなかった。他方で、米国政府が、米国外に保存されたデータを取得するためには、刑事共助条約(Mutual Legal Assistance Treaty、以下「**MLAT**」という。)等の手続きによることができたものの、その効率性・確実性に疑義が呈されており、SCA の域外適用を巡る議論が続いていた。そうしたところ、米国の捜査機関が、(MLAT は利用せず)Microsoft 社に対して、SCA に基づいて同社のアイルランド所在のサーバに保存されたデータの開示を求めたのに対し、Microsoft 社は、当該サー

バが米国外に所在することを理由としてこれを拒絶し、令状無効判決の申立てを行った。連邦地方裁判所はこの申立てを棄却したが、Microsoft 社が控訴したところ、第 2 巡回区連邦控訴裁判所は、SCA の域外適用を認めず、同社の主張を認めた[3]。このような中、こうした捜査を目的とした越境的なデータの取得に対する規律の明確化を求める声が更に強まり、CLOUD Act が制定されるに至った[4]。

2. CLOUD Act の概要

CLOUD Act は、2018 年 3 月 23 日、2018 年連邦歳出法(Consolidated Appropriations Act 2018)の一部(DIVISION V)として制定された。CLOUD Act が持つ主な意義としては、次の二つが挙げられる。

第一に、SCA に基づく令状(warrant)等により、米国政府が、米国の管轄権に服するプロバイダ[5]に対して、米国外に保有等しているデータの保存、バックアップ、開示を強制することができることを明確化した[6]。もっとも、データの開示を求められたプロバイダは、①当該データのデータ主体が、米国に居住していない米国人以外の者であり、かつ、②開示に応じることで米国と行政協定(executive agreement、後記**第 6.** 参照)を締結した外国政府の法令に違反する重大なリスクを伴うと合理的に信じる場合、米国裁判所に対して、当該開示命令の修正又は取消しを求めることが可能となった[7]。加えて、プロバイダは、外国の法令に違反することを理由として、一般法上のコミティ[8]に依拠して、裁判所に対して開示を争うこともできる[9]。

第二に、米国政府と外国政府とが行政協定を締結することによって、米国の管轄権に服するプロバイダが外国政府からの直接の命令に応じてデータを開示しても米国法上違法と評価されないこととなった[10]。これにより、米国のプロバイダは外国政府からの命令に直

---

3 United States v. Microsoft Corp., 829 F.3d 197 (2nd Cir. 2018)(以下「**Microsoft 事件**」という。)。

4 これを受け、連邦最高裁は、判断の必要性がなくなったとして、Microsoft 事件を終結させた(United States v. Microsoft Corp., 138 S. Ct. 1186 (2018))。

5 米国政府は、米国の管轄権に服するプロバイダとしては、典型的には米国に所在する事業者が想定されているとしつつも、米国外に所在し、米国内でサービスで提供する事業者も、一定の場合には米国の管轄権に服することがある旨明言している(U.S. Department of Justice, *Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act*, p. 8 (Apr. 2019), *available at* https://www.justice.gov/opa/press-release/file/1153446/download)。

6 CLOUD Act Sec.103(a)(1), 18 U.S.C. Sec. 2713.

7 CLOUD Act Sec.103(b), 18 U.S.C. Sec. 2703(h).

8 コミティ(Comity、礼譲)とは、裁判所が判断を行うにあたって、権利の問題としてではなく、厚意等に基づいて、外国の判断を尊重することをいう(田中英夫編『英米法辞典』161 頁(東京大学出版会、1991)。

9 CLOUD Act Sec. 103(c).

10 CLOUD Act Sec.104, 18 U.S.C. Sec. 2511(2)(j).

接応じることができるようになり、外国政府としては、MLAT 以外の手段で迅速に国外に保存されたデータの提出を受けることが可能となる。ただし、外国政府が米国との間で行政協定を締結するためには、当該外国政府が、プライバシー及び人権(表現の自由等)に対して実質的かつ手続的に強固な保護を与えており、米国人に関する情報の取得、保持及び流布を最小限にする適切な手続きを採用していること等が、米国の司法長官により承認される必要がある [11]。なお、行政協定は相互主義に基づいており、米国と行政協定を締結した国の企業は、米国政府からの命令に対応しなくてはならないことになる [12]。

このような意義を持つ CLOUD Act に対しては、データ開示命令に関する規律を立法で明確化するものであるとして、評価する企業の声がある [13]。他方で、米国の人権擁護団体等からは、CLOUD Act の立法手続が拙速だったという指摘や、行政協定の締結に係る交渉過程が不透明なものとなることへの懸念等が表明されている [14]。

米国政府は、2019 年 4 月、CLOUD Act に関するホワイトペーパーを公表し [15]、CLOUD Act やそれに基づく行政協定の締結を通じて、捜査を目的とした他国に保存されたデータの取得に対する規律が整備されていくことへの期待等に言及している。実際、これまでのところ、米国は、CLOUD Act に基づく行政協定の締結について、いわゆるファイブ・アイズ諸国 [16]や、EU[17]との間で既に交渉を始めつつあるようであり、2019 年 10 月 3 日には、英国との間で行政協定(Agreement between the Government of the United States of America and the Government of the United Kingdom of Great Britain and Northern Ireland on Access to Electronic Data for the Purpose of Countering Serious Crime、以下「**米英行政協定**」という。)を締結したほ

---

11 CLOUD Act Sec.105(a), 18 U.S.C. Sec. 2523(b).

12 前記脚注 5 のとおり、米国政府は、米国外に所在する企業も一定の場合には米国の管轄権に服するものとして CLOUD Act に基づくデータの開示命令の対象としている一方で、CLOUD Act に基づく行政協定が米国の管轄権を拡大するものではないことを強調している(U.S. Department of Justice, *Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act*, pp.4-5 (Apr. 2019), *available at* https://www.justice.gov/opa/press-release/file/1153446/download)。

13 法案段階で公表されたものではあるが、複数の IT 企業が CLOUD Act 法案に対して賛同を示した共同書簡(https://blogs.microsoft.com/wp-content/uploads/sites/149/2018/02/Tech-Companies-Letter-of-Support-for-Senate-CLOUD-Act-020618.pdf)が存在する。

14 ACLU, *The Cloud Act Is a Dangerous Piece of Legislation* (Mar. 2019), *available at* https://www.aclu.org/blog/privacy-technology/internet-privacy/cloud-act-dangerous-piece-legislation; EFF, *The CLOUD Act: A Dangerous Expansion of Police Snooping on Cross-Border Data* (Feb. 2018), *available at* https://www.eff.org/ja/deeplinks/2018/02/cloud-act-dangerous-expansion-police-snooping-cross-border-data.

15 U.S. Department of Justice, *Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act* (Apr. 2019), *available at* https://www.justice.gov/opa/press-release/file/1153446/download.

16 米国、英国、カナダ、オーストラリア、及びニュージーランドの 5 カ国を指す。

17 European Commission, *Criminal justice: Joint statement on the launch of EU-U.S. negotiations to facilitate access to electronic evidence* (Sep. 26, 2019), *available at* https://europa.eu/rapid/press-release_STATEMENT-19-5890_en.htm.

か[18]、同月 7 日には、オーストラリアとの交渉開始を公表した[19]。

第4. 企業が保有するデータの取得及び利用に関する日本の法令上の検討課題

インターネットの発達により、多くのデータが、個人の端末のみならず、企業が管理等[20]するサーバにも保存されるようになった。CLOUD Act が改正した SCA は、そのような企業が保有する大量のデータに対して、捜査機関がアクセスするための手続きを定めたものである。これに対して日本では、2011 年の刑事訴訟法改正において、企業が管理等するサーバ内に保存されたデータに対する捜査手法についても一定の法整備がなされたが、その後のクラウドサービスの浸透等により、企業が保有するデータの量はますます増大している[21]。そこで、まずは、企業が保有するデータの捜査目的での取得に関する日本の法令上の課題を整理する。

1. 企業が保有するデータを取得する捜査手法及びそれらを巡る検討課題

(1) 現状の整理

捜査機関が、企業が管理等するサーバに保存されたデータを取得する際の手法は、大きく以下の三つの方法に整理することができる(**図**参照)。

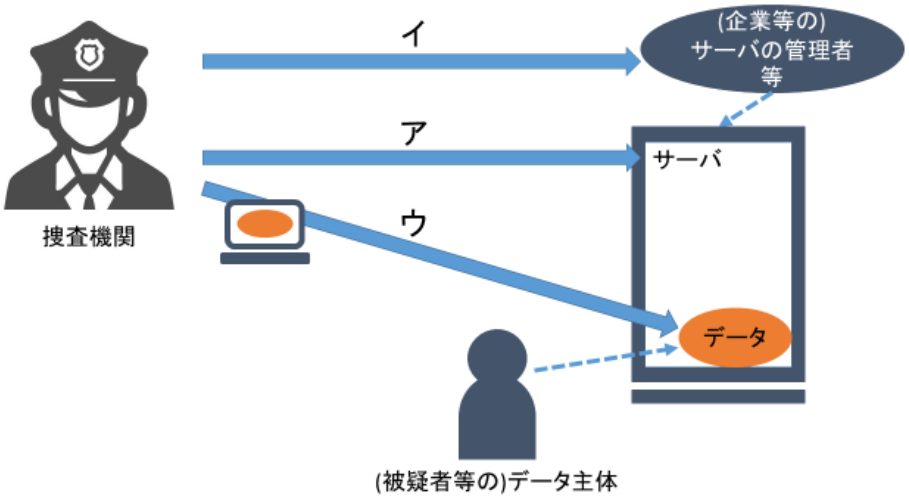
---

18 U.S. Department of Justice, *U.S. And UK Sign Landmark Cross-Border Data Access Agreement to Combat Criminals and Terrorists Online* (Oct. 3 2019), *available at* https://www.justice.gov/opa/pr/us-and-uk-sign-landmark-cross-border-data-access-agreement-combat-criminals-and-terrorists.

19 U.S. Department of Justice, *Joint Statement Announcing United States and Australian Negotiation of a CLOUD Act Agreement by U.S. Attorney General William Barr and Minister for Home Affairs Peter Dutton* (Oct. 7 2019), *available at* https://www.justice.gov/opa/pr/joint-statement-announcing-united-states-and-australian-negotiation-cloud-act-agreement-us.

20 本報告書では、企業が特定のサーバに対する所有権等に基づきこれを管理する権限を有する場合のほか、特定のサーバの記憶領域に対して利用権限を有する場合を包含して、「管理等」と表現する。また、サーバを管理等する企業等を指して「管理者等」ということがある。

21 2025 年には世界中で保存されたデータの 49%がパブリッククラウド(クラウドサービスプロバイダ等が提供するクラウド環境)上に保存されることが予想されている(IDC, *The Digitization of the World - From Edge to Core*, p.4 (November 2018), *available at* https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf)。



図：企業が管理するサーバに保存されたデータを捜査機関が取得する手法の分類

ア　データが保存されたサーバを差押対象とする方法

一つ目の方法は、捜査機関が、必要とするデータが保存されたサーバそれ自体を差し押さえる方法である(同法 218 条 1 項)。捜査機関は、それに代えて、当該サーバ内のデータのうち、捜査機関が必要とするデータのみを他の記録媒体に複写等した上で、当該他の記録媒体を差し押さえることも可能である(同法 222 条 1 項、110 条の 2)。

これらの手続きにおいて令状を請求するためには、差し押さえるべき物となるサーバ自体を特定する必要があるが、クラウドサービスの普及によってデータが不特定の複数のサーバに分散して保存されていたり、企業がその所在を明かさなかったりする等の理由から、差し押さえるべき物としてのサーバの特定が困難又は不可能である場合も少なくない。さらに、仮にデータが保存されているサーバを特定できたとしても、当該サーバが国外に所在する場合は、当該サーバを差し押さえることは、国外での管轄権の行使に該当し、他国の主権を侵害してしまうことから、不可能である(後記**第 5. の 1. (2)** 参照)。

イ　データが保存されたサーバの管理者等にデータの提出を求める方法

二つ目の方法は、捜査機関が、企業等のサーバの管理者等に対して、必要なデータの提出を求める方法である。

強制処分として行う場合については、捜査機関はサーバの管理者等に対して、捜査機関が必要とするデータを記録媒体に記録させ、当該媒体を差し押さえる記録命令付差押えの手続きを利用することができる(同法 218 条 1 項)。記録命令付差押えのための令状には「差し押さえるべき物」ではなく「記録させ若しくは印刷させるべき電磁的記録」(データ)が記載

される[22]ため、当該データが保存されているサーバを特定する必要がない。

また、強制処分に当たらない方法として、捜査関係事項照会に基づきサーバの管理者等に対して提出を求めるという方法もある(同法 197 条 2 項)。

ウ　データが保存されたサーバにアクセスしてデータを取得する方法

三つ目の方法は、捜査機関が、被疑者が保有する端末等のクライアント端末を通じて、データが保存されているサーバにアクセスし、データを取得する方法である。

刑事訴訟法上、この方法を明示的に認めたものとして、クライアント端末である電子計算機に電気通信回線で接続している記録媒体(サーバ)からデータを複写し、電子計算機を差押える方法(以下「**リモートアクセス**」という。)が存在する(同法 99 条 2 項、218 条 2 項)。ただし、リモートアクセスはあくまで「その電磁的記録を当該電子計算機又は他の記録媒体に複写した上、当該電子計算機又は当該他の記録媒体を差し押さえる」方法として定められていることから、クライアント端末を差し押さえる前に行う必要がある。そのため、クライアント端末を差し押さえた後でないと必要なデータにアクセスできない状況(差押え実施時点でデータへのアクセスに必要なパスワードが不明な場合、特定のアプリの起動が必要となる場合等)には対処し切れない面がある。

こうした状況を踏まえ、更に二つの手法が提案されている[23]。まず、一度クライアント端末を差し押さえた後に、改めてリモートアクセスによる複写処分を可能とする差押令状を請求・取得し、サーバへのアクセスを行う方法である。もっとも、クライアント端末自体は既に差押え済みである状況において、捜査機関が差押えの付随処分であるリモートアクセスを実施する必要性があることをもって、再度の差押えを実施する必要性があると言えるかという問題が指摘される[24]。

次に、サーバ自体に対する検証として、必要なデータにアクセス・認識し、それを複写する方法がある(同法 218 条 1 項)。ただし、このような行為が、サーバ自体に対する「検証」として許容される範囲に含まれるか、仮に含まれるとしても、2011 年の刑事訴訟法の改正によりリモートアクセスが制度化されたことによって、それ以外の方法によるリモートア

22　裁判所職員総合研修所『令状事務(三訂版)』231 頁(司法協会、2017)。

23　本文で紹介する二つの手法に加えて、捜査機関がクライアント端末の所有者の同意を得た上で任意捜査としてデータが保存されたサーバにアクセスすることもある。ただし、住居等について任意の捜索が禁止されているように(犯罪捜査規範 108 条)、承諾があったからといって直ちに手続保障上問題がないことにはならない。また、被処分者が自らの意思に基づき真意から承諾したとはいえないとして、同意の存在を否定した裁判例もある(京都地判平成 29 年 3 月 24 日 LEX/DB25448598、大阪高判平成 30 年 9 月 11 日 LEX/DB25449705(上告中))。

24　笹倉宏紀「クラウド捜査」芝原邦爾ほか『経済刑法――実務と理論』)575 頁(商事法務、2017)、川出敏裕『刑事手続法の論点』113 頁(立花書房、2019)。

クセスは認められないのではないかという指摘がある[25]。

(2) 捜査機関と企業との連携

前記(1)のとおり、現状の企業が保有するデータの捜査目的での取得手法には、各々一定の課題がある。これに対しては、中長期的には後記(3)で整理するような法律上の手当ても含めた検討が必要となる一方で、並行して、前記**第 2.** でも述べたとおり、捜査機関が企業側と協力・連携をしながら足元の課題に対処する道筋も検討していく必要がある[26]。

ア　捜査機関からの命令・要請に対する企業側の対応方針・状況

本研究会での国内外の通信事業者やIT企業等へのヒアリングによれば、多くの国内外の企業が、裁判所による司法審査を経た令状に基づく手続きである記録命令付差押えには基本的に応じているとのことである。また、捜査関係事項照会により報告を求められた場合には、企業は報告をすべき法的義務を負うものと解されるところ、実際にも、特に緊急性がある場合等には照会に応じている模様である。

このような捜査機関からの命令・要請への対応に関連して、企業の中には、捜査機関からの命令・要請に対応する場合に、利用者に一定の通知を行う旨をその利用規約やプライバシーポリシー等において明示しているものがある。これにより、利用者が企業に対して、捜査機関からの命令・要請に応じることへの不服を述べる機会が与えられることもある。また、いくつかの企業は、捜査機関からの開示要請の件数や対応した件数等をまとめた透明性レポートを公表し、企業による捜査機関への対応状況に関する透明性を高めている(後記**第 7.** 参照)。

イ　記録命令付差押えのさらなる活用

このような企業側の対応方針・状況を踏まえると、捜査機関においては、企業が保有するデータの取得のために、記録命令付差押えをさらに活用していくことが望まれる。

前記(1)**ウ**のとおり、現行法上のリモートアクセスは、捜査機関にとって使い勝手のい

25　横浜地判平成28年3月17日LEX/SB25542385、東京高判平成28年12月7日高刑集69巻2号5頁、笹倉宏紀「サイバー空間の捜査」法学教室 446 号 31 頁、35-36 頁(2017)、川出敏裕『刑事手続法の論点』(立花書房、2019)114-115頁。なお、検証令状に基づくGPS捜査の可否について判断した最判平成29年3月15日刑集52巻4号275頁も参照。

26　特にインターネット空間の場合、空間の管理者がインターネットサービスプロバイダ等の私人であるため、管理者が公的機関である道路や公共施設等と異なり、インターネット上での捜査活動では捜査機関が企業側からの協力を得て情報を取得する必要性が大きいことについて、山本龍彦「続・インターネット時代の個人情報保護―実効的な告知と国家の両義性を中心に」『プライバシーの権利を考える』155頁、168-169頁(信山社、2017)。

いものであるとは言い難い。これに対して、記録命令付差押えについては、前記**ア**のとおり、多くの企業がこれに応じているという現状がある。加えて、クライアント端末の側では削除済みであるデータについても、企業が管理等するサーバには同一のデータが保存されている場合がある[27]ため、サーバの管理者等を名宛人とする記録命令付差押えによれば、当該管理者等を通じて、当該データを取得できる可能性もある。また、仮にデータを保存したサーバが国外に所在する場合でも、後記**第 5.の 1.(2)ア**で検討するとおり、記録命令付差押えであれば、日本の管轄権が及ぶ企業に対して行う限り、違法な執行管轄権の行使と評価される可能性は低く、より安定的な手段であるともいえる。

また、国際的にプライバシーの保護に対する意識が高まっている現状に鑑みると、今後、データの提出に際して令状を求める企業が増えていくことも予想される。このような観点からは、令状に基づく記録命令付差押えを更に活用していくことが検討されるべきであろう[28]。

ウ　記録命令付差押えの運用に関する捜査機関と企業の連携の在り方

前記**(1)イ**のとおり、記録命令付差押えのための令状には「差し押さえるべき物」ではなく「記録させ若しくは印刷させるべき電磁的記録」が記載される[29]。その記載方法については、あまりに概括的になってしまうと、企業側の対応に困難が生じ得るほか、データ主体の権利保護の観点でも問題が生じる一方、あまりに厳格な特定性を要求してしまうと、通常、具体的にどのようなデータが、どのような形式で保存されているかを予め把握することができない捜査機関は、令状を請求することができなくなってしまう。

また、この他、記録命令付差押えの運用に当たっては、令状の呈示やデータの提出の具体的方法も問題となり得る(将来的な課題として、後記**(3)ウ**も参照。)。

そこで、捜査機関と企業の間で協働しながら、両者にとって円滑に連携し易い形で、「記録させ若しくは印刷させるべき電磁的記録」の記載方法その他記録命令付差押えの運用

27　例えば、クライアント端末がクラウドサービスを利用している場合、クライアント端末側で、あるデータを削除した場合であっても、クラウドサービスを提供する企業のサーバには当該データが提出可能な形で保存されている可能性がある。

28　米国において、無線キャリア(wireless carrier)が保有する位置情報の継続的・網羅的な取得によるプライバシー侵害に着目して、当該データ取得行為は米国憲法第 4 修正の「捜索(Search)」に該当し令状が必要であるとの連邦最高裁判決が下されている(Carpenter v. United States, 201 L. Ed. 2d 507, 2018)。同判決を紹介する邦語文献として、田中開「『ビックデータ時代』における位置情報の収集と連邦憲法修正四条――アメリカにおける近況(Carpenter v. United States,, 585 U.S. (2018))」『井上正仁先生古稀祝賀論文集』433 頁(有斐閣、2019)がある。日本への示唆は今後の更なる議論を待つ必要があるが、データを取得する捜査における令状の要否に関して、プライバシー侵害に着目した判決として、今後参照される可能性がある。

29　米国では、日本とは異なり、捜索差押えの対象には情報(information)も含む旨が明示的に規定されており(18 U.S.C. §3111. (Property seizable on search warrant), Rule 41 (a)(2)(A) of the Federal Rules of Criminal Procedure)、対象となる情報の範囲を特定することで、捜索差押えの範囲を限定している。

の在り方を模索していくことが期待される。

(3) 中長期的な制度設計を見据えた検討

企業が保有するデータの取得手法を巡る中長期的な検討課題としては、以下のようなものが考えられる。

ア　通知等の手続きの公正性担保の手段

日本の刑事訴訟法上、手続きの公正性を担保し、被処分者の権利利益を保護する手続きとして、被処分者に対する令状の呈示が存在する(同法 222 条 1 項・110 条)。

もっとも、企業が保有するデータの取得の場面では、必ずしもデータについて重要な利害関係を有するデータ主体が被処分者となるわけではない(前記(1)参照)。そこで、被処分者に対する令状呈示のみならず、データ主体に対する通知といった手続きの公正性を担保するための措置を設ける必要があるかどうか等についても検討することが考えられる [30]。この点について、犯罪捜査のための通信傍受に関する法律(以下「**通信傍受法**」という。)では、通信傍受の性質上、通信当事者に対して事前に処分の存在を知られてはならず、通信当事者は傍受令状の呈示の対象とされていない(同法 10 条参照)一方で、通信当事者に対する事後通知の制度(同法 30 条)が存在する [31]。

また、リモートアクセスに代表されるような、捜査機関がデータが保存されているサーバに直接アクセスする捜査手法の場合、企業等が自らが管理するサーバにアクセスされたことを覚知し得ないという問題も生じ得る。この点について、ドイツの刑事訴訟法上では、一定の場合には捜索すべき場所と空間的に離れた場所にあるサーバにアクセスしてデータを保全することが認められているが(ドイツ刑事訴訟法 110 条 3 項)、かかる処分はサーバの管理者等にも通知される [32]。

もっとも、手続きの公正性を担保する手段としては、通知のほかに、第三者の立会い(刑事訴訟法 222 条 1 項・114 条)等の仕組みも存在し [33]、企業が保有するデータの取得全てに

30　例えば、刑事訴訟法 100 条 3 項は、郵便物の差押え等を行った場合にその旨を送受信者に通知しなければならない旨を定めているが、同項は、捜査機関が企業に対して記録命令付差押えに基づき電子メールを記録させて差押えた場合には、電子メールを送受信者間でやり取りすること自体はできることを理由に、適用されないと考えられている(樺清隆「インターネットのプロバイダのメールサーバ内の電子メールに対する捜索差押許可状を発付することの可否」別冊判例タイムズ 35 号 154 頁、155 頁(2012))。

31　井上正仁『捜査手段としての通信・会話の傍受』81 頁、226 頁(有斐閣、1997)、鈴木秀美「通信傍受法　憲法上の問題点はなにか」法学教室 232 号 26 頁、26 頁(2000)。

32　池田公博「ドイツにおけるサイバー犯罪の捜査」刑事法ジャーナル 51 号 42 頁、44 頁(2017)。

33　最判平成 29 年 3 月 15 日刑集 71 巻 3 号 13 頁参照。

ついて単純一律に事後通知を義務付けることが最適解であるとは限らない。また、仮に事後の通知の制度を定めるとしても、どのような条件で、誰に対して、いつ通知を行うかについては、更なる検討が必要である[34]。例えば、後記**イ**でも指摘するとおり、通知によって罪証隠滅等が誘引されるという問題もあることから、通知のタイミングについては特に慎重な検討を要する。

なお、制度設計にあたっては、データが保存されたサーバやそれを管理する企業が国外に所在する場合や、サーバの所在場所が判明しない場合があり得る点についても留意する必要がある。

イ　企業に対する秘密保持の義務付け制度の拡充

前記**ア**のとおり、捜査機関がデータの取得にあたってデータ主体やサーバの管理者等に通知を行う制度を設けることは検討に値する。また、前記**(2)ア**のとおり、捜査機関から命令・要請があった場合に、利用者に一定の通知を行うこととしている企業も存在する。もっとも、これらによって被疑者その他の関係者が捜査が行われている事実を知り、罪証隠滅を誘引してしまうことが懸念される場合もある[35]。

刑事訴訟法上、この点に関する制度として、通信履歴の保全要請に係る秘密保持の義務付け(同法197条5項)が存在する。しかしながら、この制度は、その対象が通信履歴の保全要請に限定され、記録命令付差押え等の処分の存在自体は秘密保持対象とならない[36]上、秘密保持の義務付けの相手方が、電気通信事業者等に限られている等、限定的な制度となっている。中長期的には、企業に対して秘密保持を義務付ける制度の拡充も検討されるべきである。この点、SCA では、米国の捜査機関が、一定の場合にはプロバイダによる通

34　前記の通信傍受法に基づく事後通知は、傍受記録(同法 29 条)が作成された場合に、傍受記録に記載されている通信の当事者に対してなされる。これは、通信傍受においては、傍受令状記載の傍受すべき通信に該当するか判断するため必要最小限度の傍受を行うことが許容されている(同法 14 条)ところ、そのような該当性判断の傍受についても全て通知が必要であるとすることは現実的でないばかりか、通知の過程でかえってプライバシー侵害を生じさせてしまう可能性があるためである。

35　象徴的な例として、2015 年 6 月改正前の「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」においては、捜査機関の要請に応じて通信事業者が利用者の移動体端末の GPS 情報の提供を行うことの要件として、当該移動体端末の鳴動等の方法により当該位置情報が取得されていることを利用者が知ることができることが要求されていたが、2015 年 6 月の改正により、捜査の実効性を害することを理由として当該要件が削除されたことが挙げられる。改正趣旨については、同ガイドラインの解説の改正に関する意見公募手続の資料である「『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』の改正について(案)」(2015)(https://search.e-gov.go.jp/servlet/PcmFileDownload?seqNo=0000127697)も参照。

36　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 55 頁、117 頁(2012)。

知を差し止める旨の命令を求めることができるとされている点も参照に値する[37]。

ウ　令状手続の電子化

令状審査を通じた司法統制の要請と、迅速な捜査の要請のバランスをいかに図っていくかについての検討も重要である。この点については、デジタル手続法[38]による電子化の取組みが進められている現状も考慮して、令状手続の電子化・オンライン化による手続きの迅速化を目指すことが検討課題となり得る。

実際に、米国では、すでに多くの州や連邦レベルで令状の請求・発付手続について信頼できる手段でのオンライン化を認めている[39]。この点について、日本では、法令上、令状は物理的な書面であることが前提とされ(刑事訴訟法219条1項参照)、また、令状の請求は書面で行うこととされている(刑事訴訟規則139条)。したがって、令状手続を電子化・オンライン化するには、少なくともこれらの規定を改正する等の法令上の手当てが必要となる[40]。なお、本研究会における国内外の企業へのヒアリングによれば、今後、令状手続の電子化が実現された場合、これに対する回答方法についても、電子化・オンライン化を実現することができれば、事業者側の協力がより得やすくなるとの意見が多かった。

さらに、オンライン化を進める上では、これを審査するための令状裁判官の確保の問題や、無令状での捜索における緊急性判断への影響等の課題がある[41]。また、実際に令状手続を電子化する場合、オンラインシステムのセキュリティ確保をいかにして図るかも課題となる[42]。この点については、証券取引等監視委員会が、不公正取引に関する当局を含む市場関係者間の情報交換の仕組みとして、専用線を用いたネットワーク回線である「コン

37　18 U.S. Code §2705(b).捜査機関において、被処分者に捜査の事実を知らせることなく捜査を行うことを可能とする立法例も存在する(PATRIOT Act, Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline over Monitoring Act of 2015(USA FREEDOM Act of 2015))。

38　正式名称は、「情報通信技術の活用による行政手続等に係る関係者の利便性の向上並びに行政運営の簡素化及び効率化を図るための行政手続等における情報通信の技術の利用に関する法律等の一部を改正する法律」である。

39　米国では、電子化文書の信頼性や電子手続における通信の安全性が向上したこと及び令状の請求に必要な捜査資料が増大したことから、2006年に電子捜索令状が制度化され、2011年には逮捕令状、訴追請求状、及び召喚令状も電子化された(Rule 4.1 of the Federal Rules of Criminal Procedure)(石川雅俊「アメリカの電子令状」捜査研究823号94頁、96頁(2019)、石川雅俊「アメリカにおける令状の電子化と証拠排除」青山法学論集60巻4号99頁、102-104頁(2019))。

40　行政手続等における情報通信の技術の利用に関する法律(以下「**行政手続オンライン化法**」という。)は、申請や処分通知といった行政手続を電子的に行うことができるようにするため必要な事項を定めているが、同法は刑事手続には適用されない(同法2条6号等)。

41　石川雅俊「アメリカにおける令状の電子化と証拠排除」青山法学論集60巻4号111-115頁(2019)。

42　捜査関係事項照会のオンライン化に関する議論として、総合セキュリティ対策会議「サイバー犯罪捜査及び被害防止対策における官民連携の更なる推進」12頁(2016年4月)(https://www.npa.go.jp/cyber/csmeeting/h27/pdf/h27_honpen.pdf)参照。

プライアンス WAN」[43]を構築している例が参考になる。また、一部の企業は、自らパブリック・アクセス用のオンラインシステムを構築しており、捜査機関に公用ドメインのメールアドレスを登録させる等の方法により、セキュリティを確保している。この他に、電子化した令状の真正性を担保するため、電子署名技術等の活用も検討できる(行政手続オンライン化法 3 条 4 項等参照)。

エ　データの保護を目的とした他の法令との関係

刑事訴訟法において、企業が保有するデータの捜査を目的とした取得を実施するための環境を整備する中で、そのようなデータを提出する企業の側にとっても他の法令に抵触することのないよう、関連法令が適用される場面との関係も、併せて整理していく必要がある。

(ア) 電気通信事業法

電気通信事業法上、通信の秘密として保護される情報の範囲は広く解されており、メールの件名や本文、添付ファイル、閲覧しているウェブサイトの内容、通話の際の音声等のいわゆるコンテンツデータのみならず、通信日時、送信者・受信者情報、IP アドレス、端末情報等のいわゆるメタデータを含む、通信の意味内容を推知できる可能性がある情報全てが通信の秘密として保護されると考えられている。

そして、かかる通信の秘密として保護される情報を含め、個人データを保有する電気通信事業者は、当該データを政府機関を含む第三者に対して提供することが原則として禁止されている一方で、例外として、記録命令付き差押えに基づく場合を含め、法令による行為(刑法 35 条、以下「**法令行為**」という。)などの違法性阻却事由が認められる場合[44]には、第三者に対して当該データを提供しても同法に違反しないと解されている(電気通信事業法 4 条 1 項、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[45]15 条 1 項 1 号及びその解説[46]3-5-1(1)参照)。

もっとも、電気通信事業者が通信の秘密の保護を義務付けられることを踏まえ、通信の

43　証券取引等監視委員会「『コンプライアンス WAN』の利用開始について」(2009 年 1 月 25 日)(https://www.fsa.go.jp/sesc/news/c_2009/2009/20090126.htm)。

44　宍戸常寿「通信の秘密に関する覚書」高橋和之古稀『現代立憲主義の諸相(下)』487 頁、514 頁(有斐閣、2013)。

45　総務省「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(平成 29 年 4 月 18 日総務省告示第 152 号)」(2017 年 9 月 14 日)(http://www.soumu.go.jp/main_content/000507466.pdf)。

46　総務省「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(平成 29 年総務省告示第 152 号。最終改正平成 29 年総務省告示第 297 号)の解説」(2019 年 1 月)(http://www.soumu.go.jp/main_content/000603940.pdf#page=60&zoom=100,0,822)。

秘密として保護される情報を捜査関係事項照会に対応して提供することは「原則として適当ではない」とされている[47]。また、「我が国における通信の秘密に対する姿勢は極めて慎重であり、知得する目的の正当性を厳格に吟味するとともに、これを第三者に開示する際には厳格な手続きを要求する傾向にある」とも評されている[48]。

今後、前記**ア**乃至**ウ**で述べたような、企業が保有するデータを取得する捜査手続を実施するための環境を刑事訴訟法において整備するにあたっても、中長期的な課題としては、特定された範囲の情報については、類型的に政府機関に対する情報提供を電気通信事業法上も正当化できるよう、手当てすることが望ましいと考えられる。具体的には、個別具体的な事例ごとにその成否が検討・判断される正当業務行為やその他の違法性阻却事由を利用するのではなく、企業が保有するデータを取得する捜査手続を類型ごとに法令でなるべく具体的に定めることにより、法令行為として、データを取得する捜査に対応する企業の行為を整理するとともに、被処分者たる企業にとって取得手続の透明性を高めるよう制度設計を行うことが考えられる。その際、情報の特定の仕方等については、企業側とも協議していくことが有益であると考えられる。

また、中長期的には新たな捜査手続を創設することも検討課題となり得るが、その場合には、EUや米国等の諸外国の法制も参考にしつつ、メタデータやコンテンツデータといったデータの類型・性質ごとに、取得のための手続きを細分化・精緻化する方向性も一つの選択肢となる。もっとも、そのような方向性を検討していくにあたっては、通信の秘密として保護される範囲についての従来の解釈との関係や、電気通信事業者の通信の秘密を保護する義務への配慮及び通信当事者の通信の秘密に対する権利・利益の保護等を考慮しつつ、通信の秘密を第三者に開示する手続きとして相応しい適正手続を具備した捜査手続となるよう、留意することが必要となる。

(イ) 個人情報保護法

個人情報保護法上、個人情報取扱事業者は、原則としてデータ主体の同意がない限り当人の個人データを第三者に提供することが禁止されている(同法 23 条 1 項)。その例外として第三者提供が適法とされる類型の中には、「法令に基づく場合」(同項1号)が存在するところ、データを取得する捜査に応じて企業が保有するデータを提供する場合は、かかる「法令に基づく場合」として正当化されると解されている。実際に、現在の捜査活動において

---

47 総務省「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(平成 29 年総務省告示第 152 号。最終改正平成 29 年総務省告示第 297 号)の解説」3-5-1(1)(2019 年 1 月)(http://www.soumu.go.jp/main_content/000603940.pdf#page=60&zoom=100,0,822)。捜査関係事項照会による場合では、端的に、必ずしも違法性が阻却されないとする見解もある(山本龍彦「続・インターネット時代の個人情報保護―実効的な告知と国家の両義性を中心に」『プライバシーの権利を考える』155 頁、178 頁(信山社、2017))。

48 高嶋幹夫『実務　電気通信事業法』778 頁(NTT 出版、2015)。

も、令状に基づく強制処分又は捜査関係事項照会により課せられる義務に応じて企業が政府に対して個人情報を提供する場合は、「法令に基づく場合」に該当すると解されている[49]。

中長期的には、前記**ア**乃至**ウ**で述べたような、企業が保有するデータを取得するための新たな捜査手続を創設することも検討課題となり得るが、その場合も、従来の捜査手続と同様に個人情報保護法上の「法令に基づく場合」に該当するように手続きや条件を定め、法定の手続きに従う限り類型的に個人情報保護法に反しないことを担保することが、関係者の予測可能性の確保等の観点から望ましい。

また、新たな手続きを創設する際には、個人データの中でも、データの類型・性質や、当該データの提供によりプライバシー侵害が生じる危険の類型的な高低に応じて、捜査機関による取得の手続きを細分化・精緻化していく方向性も一つの選択肢となり得る。そのような方向性を模索する場合には、プライバシー侵害の危険や性質に応じて適正手続の内容を変えるなど、より適切な法制度の設計に向けた議論が今後蓄積されることが期待される[50]。

(ウ) 行政機関の保有する個人情報の保護に関する法律・個人情報保護条例

さらに、データを取得する捜査手法の活用が進むと、捜査機関に大量の個人情報が蓄積されることになるため、その利用・保存に対する規律の在り方も検討課題となり得る。

例えば、既に、行政機関の保有する個人情報の保護に関する法律は、行政機関の保有個人情報に対するデータ主体の開示請求権(同法 12 条 1 項)、訂正請求権(同法 27 条 1 項)及び利用停止請求権(同法 36 条 1 項)を法定しているものの、これらの請求権は刑事事件等に係る裁判、検察官等が行う処分などには適用されない(同法 45 条 1 項)ほか、訴訟に関する書類及び押収物に記録されている個人情報にも適用されない(刑事訴訟法 53 条の 2 第 2 項)。この点について、中長期的な課題としては、これらに類する請求権を刑事手続に関連して

---

49 捜査関係事項照会を受けた場合も報告義務が生じ、個人情報保護法上「法令に基づ」く個人データの提供として正当化されることについて、個人情報保護委員会「個人情報の保護に関する法律についてのガイドライン(通則編)」45 頁、29 頁(2019 年 1 月)(https://www.ppc.go.jp/files/pdf/190123_guidelines01.pdf)、個人情報保護委員会「『個人情報の保護に関する法律についてのガイドライン』及び『個人データの漏えい等の事案が発生した場合等の対応について』に関する Q&A」Q5-17、A5-17(2019 年 6 月 7 日)(https://www.ppc.go.jp/files/pdf/1906_APPI_QA.pdf)、及び宇賀克也『個人情報保護法の逐条解説(第 6 版)』166-167 頁(有斐閣、2018)。この点で、電気通信事業法上の通信の秘密に該当する場合の保護は、個人情報保護法によって与えられる保護よりも高いレベルにあるといえる(山本龍彦「インターネット上の個人情報保護」松井茂記ほか『インターネット法』274 頁、295 頁(有斐閣、2015))。

50 その際には、個人情報保護法の個人情報や電気通信事業法上の通信の秘密には該当しない情報であっても、プライバシー侵害の危険性が高いことを理由として要保護性が高いとされる情報(代表例として、消費者が利用する移動体端末から収集される位置情報が挙げられる。総務省『緊急時等における位置情報の取扱いに関する検討会　報告書　位置情報プライバシーレポート』(2014)(http://www.soumu.go.jp/main_content/000434727.pdf))の取扱いにも留意する必要がある。

収集・利用される個人情報についても認めるべきかについて、議論が今後蓄積されることが期待される。

また、捜査を目的として取得された情報について、政府が利用することができる活動の範囲や保存期限についての規律の在り方も検討課題となり得る。例えば、欧州人権裁判所は、英国において一定の犯罪に当たるとの嫌疑で逮捕された被疑者から採取した指紋等について、当該被疑者がその後有罪とされたか否かにかかわらず半永久的に保管する旨を定めた 1984 年警察及び刑事証拠法は欧州人権条約 8 条に違反すると判断し[51]、これを受けて英国では、2010 年犯罪及び保安法によって、有罪とされなかった被疑者に関する指紋等の保管期限を設定する等の法改正が行われた。

さらに、中長期的には、捜査を目的としたデータの取得時における規律と、取得後におけるデータの利用・保存に関する規律を連続的に捉えた上で、両者の規律のバランスを検討していくことも有益であると考えられる[52]。

今後、こうしたデータの利用・保存にまつわる国家としてのセキュリティ体制の整備という観点からも、体制・法制度の整備に向けた検討を深める必要がある[53]。

2. 捜査機関が取得したデータの公判利用

捜査機関が必要なデータを取得できたとして、その公判における利用を巡る課題もある。

裁判所としては、公判に顕出されたデータの収集や選別、加工が恣意性を伴わないものであって、データの真正性や正確性が具体的な実施方法・実施者との関係で担保されていることを確認する手段が必要となる[54]。情報技術の解析に関する規則 2 条 1 項においても、「情報技術の解析の対象が、公判審理において証明力を保持し得るように処置しておかなければならない」旨が定められている。

そこで、捜査機関としては、取得したデータをその解析過程も含めて証拠化し、解析結

---

51 S. and Marper v. The United Kingdom, 2008-V Eur. Ct. H.R. 167., *available at* https://www.echr.coe.int/Documents/Reports_Recueil_2008-V.pdf、末井誠史「DNA 型データベースをめぐる論点」国立国会図書館調査及び立法考査局レファレンス 2011 年 3 月号 5 頁、6-12 頁(2011)。

52 緑大輔「監視型捜査における情報取得時の法的規律」法律時報 87 巻 5 号 65 頁、69 頁(2015)、山本龍彦「警察による情報の収集・保存と憲法」『プライバシーの権利を考える』67 頁、76-84 頁(信山社、2017)、山本龍彦「監視捜査における情報取得行為の意味」『プライバシーの権利を考える』89 頁、93-98 頁(信山社、2017)。

53 宍戸常寿ほか「情報法制の現在と未来」論究ジュリスト 20 巻 179 頁(2017)[宍戸常寿]。

54 最決平成 12 年 7 月 17 日刑集 54 巻 6 号 550 頁は、DNA 型鑑定について、前提となっている①科学的理論の正確性と②その実施の方法の科学的信頼性を根拠にその証拠能力を肯定したが、かかる判断枠組みは科学的証拠に限らず専門証拠一般に妥当し、データの解析についても同様に妥当すると考えられる(成瀬剛「科学的証拠の許容性(五・完)」法学協会雑誌 130 巻 5 号 1064-1065 頁(2013)、吉峯耕平ほか「デジタル・フォレンジックの原理・実際と証拠評価のあり方」季刊刑事弁護 77 号 109-129 頁(2014))。

果報告書を公判に提出することが考えられる。この解析結果報告書には、解析を実施した場所、対象となる記録媒体の型番や製品番号、記録媒体や各ファイル等のハッシュ値[55]、解析時のメモに基づく解析手順、解析環境、解析ツールの名称及びバージョン等を記載することが想定される。

もっとも、裁判所にとっては、捜査過程の記録の確認や日本の捜査担当者に対する証人尋問を行っても、それが適切なものであったかどうかの判断の基準がないため、なお証拠能力や証明力の評価が容易でないおそれがある。そこで、関係者のコンセンサスの下、デジタル・フォレンジック技術に関する標準を定立し、技術の進歩に合わせて更新していくことが望ましいと考えられる[56]。

例えば、捜査の対象となったサーバからダウンロードしたファイルが、当該サーバ上のファイルと同一であることの担保が必要である[57]。また、事業者側としては、捜査機関からの要請に応じて、過度な負担とならない範囲で、捜査の対象となるアカウントやファイルへのアクセスを停止したり、削除されたファイルを復元したり、変更前のバージョンのファイルを保存したりする機能を備えておくことが有益であると考えられる。

3. 暗号化データに関する課題

暗号化されたデータの取得に伴う課題については、復号を強制される主体が被疑者である場合と被疑者以外の第三者である場合とで問題の所在が異なるため、以下では各々の場面に分けて検討する。

(1) 被疑者との関係

捜査機関が、被疑者に対して、暗号化されたデータのパスワードの開示や、復号を強制することが自己に不利益な供述を強要されない権利(自己負罪拒否特権、憲法 38 条 1 項)の

---

55 ファイルに対して一定の計算手順により求められた、規則性のない固定長の値のことを指し、標準的には SHA1 や SHA256 が用いられる。

56 デジタル・フォレンジックによる解析の正確性等に関する解説としては、特定非営利活動法人デジタル・フォレンジック研究会「証拠保全ガイドライン 第 7 版」(2018 年 7 月 20 日)(https://digitalforensic.jp/wp-content/uploads/2018/07/guideline_7th.pdf)や羽室英太郎＝國浦淳編著『デジタル・フォレンジック概論』(東京法令出版、2015)がある。

57 捜査対象のサーバ上でハッシュ値を確認することができれば、このハッシュ値と、対象サーバからダウンロードしたファイルに対して計算したハッシュ値とを照合することで、同一性を確認することができる。しかし、現時点ではこのような機能を実装したサーバは見当たらない。そこで、対象サーバにサイズの異なる複数のファイルをアップロードし、当該ファイルをダウンロードしてファイル毎にそれぞれ計算したハッシュ値を照合した結果、全て一致した場合には、当該対象サーバはダウンロードによってファイルが変更されないことを確認するという方法も検討できる。

侵害となるのかが問題となる[58]。

この点については、いくつかの米国の裁判例がある。例えば、自己負罪拒否特権の侵害に当たるか否かの判断に当たり、その要請の内容が、ある個人の思考の内容を外部に強制的に表現させるかどうかという点に焦点を当てた裁判例や[59]、その要請に応じること自体に供述的側面があるかどうかに焦点を当てた裁判例がある[60]。

また、英国においては、捜査権限規制法(Regulation of Investigatory Powers Act 2000 (以下「**RIPA**」という。))において、パスワードを開示する必要性、比例性及び補充性が認められる場面においては、一定の司法審査を受けることを前提に、被疑者に対し、捜査機関が、パスワードの開示を強制できることが法定されている(RIPA 49 条 1 項乃至 3 項、50 条 1 項、別紙 2)[61]。

今後、日本においても米国・英国における取扱い等を参考に、被疑者に対するパスワードの開示や復号の要求と自己負罪拒否特権の関係についての議論を深めることが考えられる[62]。

(2) 被疑者以外の第三者との関係

被疑者以外の第三者で、パスワードの開示や復号を強制され得る主体としては、大きく分けて①被疑者に係る暗号化データを保存・保管している事業者、②暗号化解除技術を持つ専門業者が想定される。

例えば米国では、全令状法(All Writs Act)に基づき、不合理な負担を課さない限りにおいて、被疑者と直接関係のない者に対しても復号の支援を要請することが可能と解されてい

---

58 実務上は、指紋認証システムや顔認証システムに基づくロックを解除するために、被疑者の顔や指紋情報が必要となる場合には、被疑者に対する身体検査令状(刑事訴訟法 218 条 1 項)の発付を請求することで対応している場合があるようである。

59 United States v. Doe, 670 F.3d 1335 (11th Cir. 2012), 湯淺墾道「暗号化とアメリカ憲法――iPhone 問題を手がかりに」情報ネットワークローレビュー15 巻 96-101 頁(2017)。

60 Fisher v. United States, 425 U.S. 391 (1976), United States v. Doe, 465 U.S. 605 (1984), United States v. Hubbell, 530 U.S. 27 (2000), 笹倉宏紀「自己負罪拒否特権」法学教室 265 号 103 頁、107-109 頁(2002)。

61 これは、英国法上の自己負罪拒否特権は、対象となる情報が対象者の意思から独立していない、その内心に関わるものについては及ぶが、パスワードはそのような内心に関するものではないという考え方に基づくとされている。ただし、英国の裁判例でも、パスワードを知っていること自体が不利益事実に当たる場合には、自己負罪拒否特権の保護が及ぶと考える余地が示されている(丸橋昌太郎「暗号解除に関する規律について―イギリスにおける暗号解除法制を参考に」『日髙義博先生古稀祝賀論文集　下巻』393 頁、403-404 頁(成文堂、2018))。

62 例えば、パスワードそれ自体が自己負罪となる情報ではないことを理由として、現在の判例の立場では、パスワードの開示強制は自己負罪拒否特権の侵害とならない可能性が高いと指摘する見解が見当たる(松井茂記『インターネットの憲法学　新版』372 頁(岩波書店、2014))。

る[63]。2016 年には同法に基づき、FBI が Apple 社に対し iPhone のロック機能を解除することの支援を求め、争いになった事案があった。

また、英国においては、被疑者の場合と同様、RIPA に基づき、被疑者以外の第三者に対しても、当局へのパスワードの開示や復号を強制し得る(同法 49 条 1 項、50 条 1 項)。

さらに、オーストラリアにおいては、2018 年 12 月に成立した電気通信その他の法令の改正法(援助及びアクセス提供法)(Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018)によって、当局が事業者に対して、その保有する暗号化されたデータにアクセスするためのバックドアを設けることを、命令により義務付けることができるようになった(同法 317 条 E(1)、317 条 L)[64]。

このように、現状では、被疑者以外の第三者に対するパスワードの開示や復号の強制であったり、その協力要請の可否について国際的に多様な動向が見られる。日本でも、諸外国の動向も注視しながら、企業と連携した上で、検討を深めていく必要がある。ただし、企業に予めバックドアを設置させることについては、人権保障[65]、(バックドアの設置を求められていない企業との関係での)企業の競争力の低下、バックドアが悪用されることによる情報漏洩等のリスクといった観点からの問題が生じ得るため、慎重に検討せざるを得ない。なお、CLOUD Act は暗号の解除について義務付けを要請するものではなく[66]、行政協定では、プロバイダによる暗号解除を強制したり、これを制限する義務を課したりすることはできないとしている[67]。

第5. 国外に保存されたデータの捜査を目的とした取得を巡る検討課題

捜査対象となるデータが国外に所在するサーバに保存されている場合、及びデータを管理等する事業者が国外事業者であったり国外で活動していたりする場合には、捜査を目的としたデータの取得それ自体を巡る検討課題に加えて、更に国際法上の評価等に関連した検討課題も生じてくる。

---

63 United States v. New York Tel. Co., 434 U.S. 159 (1977).

64 Parliament of AUSTRARIA, *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* (https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6195).)

65 例えば、通信の秘密やプライバシー権の保護との関係性が問題となり得る。なお、復号キーの公開が表現の自由の問題をも生じさせると指摘するものとしては、松井茂記『インターネットの憲法学 新版』379 頁(岩波書店、2014)。

66 U.S. Department of Justice, *Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act*, 5-6 (2019), available at https://www.justice.gov/opa/press-release/file/1153446/download.

67 CLOUD Act Sec.105(a), 18 USC§ 2523(b)(3).これと同趣旨と思われる規定が、「デジタル貿易に関する日本国とアメリカ合衆国との間の協定」にも定められている(21 条 3 項)。

1. サーバの所在国の同意を得ない場合

まず、捜査対象となるデータが保存されているサーバの所在国の同意を得ない場合には、当該データの捜査を目的とした取得が、国際法上適法な国家管轄権の行使か否かという問題が生じる。

(1) 管轄権の概念と問題の所在の整理

ア 管轄権の概念と行使基準

日本の捜査機関が、捜査を目的として国外のサーバに保存されているデータを取得する場合、刑事訴訟法の地理的適用範囲自体は国外も含んでいると解される一方[68]、他国の主権ないし管轄権を侵害するのではないかという問題が生じ得る[69]。

国家が人や財産等の事象に対して、自国の国内法を制定、適用、又は執行するためには、当該事象に対して国家管轄権を有している必要がある[70]。この国家管轄権は、①国内法令を制定して、一定の事象と活動をその適用の対象とし、合法性の有無を認定する立法管轄権、②司法機関及び行政機関が逮捕、捜索、強制調査、押収、抑留等の手段により国内法を執行する執行管轄権、及び③司法機関及び行政裁判所がその裁判管轄の範囲を定め、国内法令を適用して具体的な事案の審理と判決の執行を行う司法管轄権の 3 つに分類される[71]。

そして、国家がある事象に対してこれらの管轄権を有するかどうかは、属地主義、属人主義等の国際法上の確立された基準に照らして判断されるのが原則である[72]。この他、各関係国と対象事項との間の「実質的かつ真正の連関」[73]が存在する場合も国家管轄権の行使根拠となるとの考え方がある。

管轄権の行使については、原則として、領域内に所在する者や領域内で行われた行為に

---

68 日本の刑事訴訟法の地理的適用範囲について、日本の刑事訴訟法は日本の領域内のみならず領域外にも適用があるが、外国の主権が及ぶ範囲では国際法上の制限を受けるとする外国主権制限説が通説である(山内由光「国外における捜査活動」松尾浩也・岩瀬徹編『実例刑事訴訟法Ⅰ』5 頁、10-12 頁(青林書院、2012 年))。

69 Council of Europe Cybercrime Convention Committee (T-CY), *Transborder access and jurisdiction: What are the options?*, Doc no T-CY (2012)3, 6 (2012).

70 山本草二『国際法〔新版〕』231 頁(有斐閣、1994)。

71 酒井啓亘ほか『国際法』85 頁(有斐閣、2011)、小寺彰「国家管轄権の域外適用の概念分類」山本草二古稀『国家管轄権 国際法と国内法』343 頁、343-344 頁(勁草書房、1998)、小寺彰ほか編『講義国際法〔第二版〕』163 頁(有斐閣、2010)。

72 酒井啓亘ほか『国際法』86 頁(有斐閣、2011)。

73 山本草二『国際法〔新版〕』234 頁(有斐閣、1994)。

対して、領域国が当該対象者・行為と最も緊密な連関を持つため、属地主義[74]が認容されてきた。

しかし、第二次世界大戦後に、国境を越えた経済活動の拡大に伴い、各国の公法的規制が域外適用される事例が発生している。顕著なものとして、米国による反トラスト法の域外適用を巡る司法摩擦が挙げられる。1945 年の連邦裁判所アルコア事件判決[75]は、外国人が他国で行ったカルテル行為であっても、その悪影響が米国に及び、かつ、それが意図されている場合は米国反トラスト法が適用されるといういわゆる効果理論を認容し、その後も同理論に基づく反トラスト法の域外適用が多数なされるに至った。これら米国の国内裁判手続に付随して、文書提出命令、米国外での事情聴取等、米国当局による執行も行われている。しかし、これに反発した欧州各国は、自国企業、個人に対して外国当局への情報開示を禁止する「対抗法(blocking statute)」を制定し、米国当局による米国外での証拠収集がかえって妨げられることとなった[76]。

その後、競争法についての効果理論は一定の国際的なプラクティスとして定着しているが、米国の対外関係法第 4 リステイトメント(2018 年)では、管轄権の行使のより一般的な基準として、国家と対象事項との「真正な連結(genuine connection)」が示されるに至っており、かかる連結の要素としては従来一応の管轄権の根拠とされてきた属地、属人、効果主義等が列挙されている[77]。

米国のみならず、現在の一般国際法の下では、正当な国家管轄権の行使のためには、国家と管轄権の行使対象(企業等)との間に「正当な連結点」が認められる必要があることには争いがないものと考えられる。ただし、何を「正当な連結点」と考えるかについては、各国の具体的な実行を見る必要がある。この点について、各国法では、企業が自国の管轄権に服すること、企業の利用者が自国領域に相当数存在すること、企業が自国を狙ってサービ

74 山本草二『国際法〔新版〕』239 頁(有斐閣、1994)。

75 U.S. v. Aluminum Co. of America, 148 F.2d 416 (1945).

76 米国による反トラスト法の域外適用及び各国による対抗立法の制定については、石井由梨佳『越境犯罪の国際的規制』137-160 頁(2017)を参照。

77 Restatement (Fourth) of the Foreign Relations Law of the United States§407-413(AM. LAW INST. 2018).

スを提供していること等を基準に管轄権の範囲を画定している例がある[78]。

イ　サイバー空間と主権

サイバー空間と主権との関係性について、サイバー活動に関する国際法規則を整理したタリンマニュアル 2.0[79]では、次のとおり規定している。すなわち、タリンマニュアル 2.0

78　例えば、CLOUD Act では、米国の管轄権に服するサービスプロバイダが管轄権行使の対象とされ、当該プロバイダが管理、支配又は保有する国内外に保存されたデータの開示命令が許容されているところ、米国の管轄権に服するかどうかの判断要素としては、米国内に事業所があるかどうか、米国外に所在する企業であり米国に向けてサービスを提供している場合には、当該サービスプロバイダのサービス提供行為の性質、量、質(例えば、ウェブサイトに米国向けのコンテンツがあるか否か)といった要素が挙げられる(U.S. Department of Justice, *Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act*, 8 (Apr. 2019), *available at* https://www.justice.gov/opa/press-release/file/1153446/download)。また、EU 電子証拠に関する指令案及び規則案 3 条では、EU 非加盟国のサービスプロバイダであって EU 域内向けにサービスを提供する者に、提供先の EU 加盟国における代理人指定を義務付け、その代理人に対して域内外のデータ開示命令等の措置をとることが提案されている。そこでは、EU 法は域内に対するサービス提供を連結の有無の判断要素としており、域内に拠点を有さないサービスプロバイダに対して代理人の設置を義務付けることによって、実効的な管轄権の行使を確保していると言える(European Commission, *Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings* COM/2018/226 final - 2018/0107 (COD), *available at* https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1524129181403&uri=COM:2018:226:FIN)。さらに、韓国の電気通信事業法 2 条の 2 では「この法律は、国外で行われた行為であっても、国内市場や利用者に影響を与える場合には、適用する。」と定める域外適用規定が存在する。具体的には、同法 87 条では、国内に事業所を置いていない事業者が、電気通信回線設備を用いた電気通信役務等の基幹通信役務を韓国国外から国内へ提供する場合に、同じく基幹通信役務を提供する国内の基幹通信事業者との間で、基幹通信役務の越境提供に関する「協定」を締結しなければならないとした上で、かかる「協定」に基づく基幹通信役務の越境提供について、一定の国内規定の遵守を求めている。そして、同法 87 条が同法 83 条を準用することで、韓国の捜査機関が、電気通信事業利用者の氏名、住民登録番号、アドレス、電話番号、ID、利用開始日等の提出を命令した場合、国内に事業所を置いていない事業者もこれに従う義務が規定されている(電気通信事業法(法律第 16019 号、2018 年 12 月 24 日最終改正), *available at* http://www.law.go.kr/lsInfoP.do?lsiSeq=206000&efYd=20190625#J2:2(韓国語のみ))。なお、韓国情報通信網法 32 条の 5 では、韓国に情報通信サービスを提供し、一定の売上高を有する、国内に住所又は営業所がない情報通信サービス提供者等に対し国内代理人の指定を義務付け、さらに、同法 64 条にて、同法律に違反する行為、または利用者の安全性と信頼性の確保を著しく損なう事件・事故が発生した場合等に、当該国内代理人に対して資料提出を義務付けている(情報通信網利用促進及び情報保護等についての法律(法律第 16021 号、2018 年 12 月 24 日最終改正), *available at* http://www.law.go.kr/lsInfoP.do?lsiSeq=206009&efYd=20190625#0000(韓国語のみ)；韓国に対して情報通信サービスを提供しているか否かの判断基準については、韓国放送通信委員会「国内代理人の指定制度ガイドライン」(2019 年 3 月)を参照されたい(*available at* https://kcc.go.kr/download.do?fileSeq=48880))。ただし、こうした代理人設置の義務付けについては、別途、サービス貿易や電子商取引に関する国際協定整合性の観点からも検討を要することには留意が必要である。

79　タリンマニュアル 1.0 は、2013 年に International Group of Experts at the invitation of the NATO サイバー防衛協力センター(NATO Cooperative Cyber Defense Centre of Excellence)が公表したサイバー攻撃に関する国際法規則を整理した文書であり、サイバー攻撃の武力攻撃該当性やサイバー攻撃と自衛権との関係について論じている。また、2017 年に公表されたタリンマニュアル 2.0 は、武力攻撃に至らないレベルのサイバー活動について、諸分野の国際法的観点からの評価を論じた文書である。

は、国家は自国領域内に所在する IT インフラ(ケーブル、ルーター、サーバ、及びパソコン等)及び IT インフラへのオペレーションに対して主権を享受することを確認しつつ [80]、国家によるサイバー活動について、①ターゲット国の領域的主権の侵害の程度及び②本質的な政府機能の妨害又は侵害があったかを基準に、主権の侵害の有無を議論している。例えば、主権侵害が生じる例として、ある国家の政府職員が他国領域内に物理的に存在する間にサイバー行動をとった場合や、遠隔サイバー行動によりサイバー・インフラの物理的損害や機能の喪失が生じた場合等を挙げている [81]。

(2) 国外に保存されたデータの捜査を目的として取得する手法と国際法上の評価

前記**(1)イ**のとおり、国家は、自国領域内に所在する IT インフラ及び IT インフラへのオペレーションに対して主権を享受する。そのため、国外に保存されたデータの取得を行う場面では、当該データが保存されている他国の主権ないし管轄権を侵害する違法な管轄権の行使に当たらないかが問題となる。

まず、ある国家が、他国の領域内において、主権的行為を行うことは、他国の同意がない限り、領域主権を侵害するものとして、国際法上禁止されている。そのため、国外に保存されたデータを捜査を目的として取得する場面において、他国の領域に捜査機関が立ち入って捜査を行うことは、他国の領域内において執行管轄権を行使するものとして主権侵害行為に当たり、国際法上許容されない。

一方、捜査機関が、ネットワークを通じて、国外に所在するサーバに保存されているデータを取得する場合は、他国の領域に捜査機関が立ち入って捜査を行うことはないが、他国の主権をなお侵害する可能性があるので、かかる捜査を行うことについての国際法上の評価が問題となる。

ア　サーバの管理者等にデータの提出を求める方法

サーバの管理者等にデータの提出を求める捜査手法には、①国内の企業に対して、国外のサーバに保存されているデータの提出を命ずる捜査手法(前記**第 4. の 1. (1)** で説明した日

---

80 Michael N. Schmitt, TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS, 11 (2d ed. 2017). サイバー空間は、しばしば「グローバル・ドメイン」又は「第 5 のドメイン」と表現され、物理的特性のない、仮想的であり、公海や宇宙空間と同様、「万民共有物」(*res communis omnium*)であると主張されることもある。しかし、タリンマニュアルでは、サイバー行動は、国家が主権的権限を行使する領域において行われ、及び国家が主権的権限を行使する物に対して行われ、又は、国家が主権的権限を行使する人若しくは組織によって行われることにより、サイバー空間にも国家主権が及ぶことが確認されている(ibid, 12)。

81 Michael N. Schmitt, TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS, 17-18 (2d ed. 2017).

本の記録命令付差押え等)[82]、又は②国外にいるサーバ管理者等に直接データの提出を命じる捜査手法があり、それぞれ国際法上、次のように評価される。

まず①について、国際法の属地主義に基づくと、データ又はその記録媒体の提出命令の対象者であるサーバの管理者が領域内に所在する場合、当該国家はかかる対象者に対して当然に執行管轄権を有する。また、国外のサーバに保存されているデータについては、他国領域に捜査機関が立ち入り、捜査を行うような執行管轄権に基づく強制措置とは異なり、実際のデータ又はその記録媒体の提出行為が国内で行われ、国外に所在するサーバへのアクセスは命令を受けた国内にいるサーバの管理者等が行うのであれば、国際法上許容されると考えるべきである[83]。

一方、②ある国の捜査機関が、他国に所在するサーバ管理者に対して直接データ提出を

---

82 日本では、前記**第 4 の 1. (1)**のとおり、日本国内の企業に対して、国外に保存されているデータの提出を命ずることを可能にする制度として、記録命令付差押えが存在する。この制度の立法担当者は、日本国外のサーバにアクセスをし、取得したデータを記録する行為自体は、私人である命令を受けた者(サーバの管理者等)が行うものであるから、当該サーバの所在する相手国の主権侵害にはならないとの見解を示していた(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 55 頁、74 頁(2012))。

これに対して、捜査機関の命令で記録行為が行われる以上、日本国外へのデータアクセスを含む記録行為も捜査機関の行為の一環であるとして、主権侵害がないとする見解に疑問を呈する見方も存在する(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』409 頁、414 頁(有斐閣、2019))。また、米国 CLOUD Act 制定の発端ともされる Microsoft 事件において、かかる捜査手法は、データにアクセスすることのできるサーバの利用権限者に対して管轄権を有していることのみをもって、データの保存場所に関係なく、関心のあるデータをあらゆる国家が取得できる事態を招くので問題である旨の Microsoft の主張に、サーバ設置国であるアイルランドを含む多くの国が同意したとされる(Currie, Robert J., *Cross-Border Evidence Gathering in Transnational Criminal Investigation: Is the Microsoft Ireland Case the "Next Frontier"?,* 54 CANADIAN YEARBOOK OF INTERNATIONAL LAW 63, 87-89 (2017))。

83 国外に保存されたデータの提出命令を、当該データ所在国の同意を得ずに、国内の事業者に対して出すことの可否については、これを否定的に捉える学説もあるものの(Bert-Jaap Koops & Morag Goodwin, Cyberspace, *the Cloud and Cross-Border Criminal Investigation: The Limits and Possibilities of International Law,* Tilburg: Tilburg Institute for Law, Technology and Society, 61-62(2014))、肯定的に捉える学説も多い(域外適用の一般的な議論に関して明示的に肯定する説として、Mann, Frederick Alexander, *The Doctrine of International Jurisdiction Revisited after Twenty Years,* 186 Recueil des Cours 9, 47-49 (1984)。またこの点に関する国家実行は統一的ではないとする見解としては Currie, Robert J., *Cross-Border Evidence Gathering in Transnational Criminal Investigation: Is the Microsoft Ireland Case the "Next Frontier"?,* 54 CANADIAN YEARBOOK OF INTERNATIONAL LAW 63, 83 (2017)を参照)。また、前記脚注 78 に記載のとおり、EU や韓国等、各国の実践において、国内に代理人や拠点を設置し、当該代理人や拠点に国外に保存されたデータの取得・提出を命令する動向がみられる。実際に、日本以外でも、必ずしも MLAT を通じず、サーバの国内の利用権限者に対して、国外に所在するサーバに保存されたデータ(又はその記録媒体)の提出を求める捜査手法を実際に行っている国家や、かかる要請に応じる会社も多数ある模様である(Currie, Robert J., *Cross-Border Evidence Gathering in Transnational Criminal Investigation: Is the Microsoft Ireland Case the "Next Frontier"?,* 54 CANADIAN YEARBOOK OF INTERNATIONAL LAW 63, 91-93 (2017))。さらに、ベルギー国外に保存されたデータに対する提出命令を許容したベルギー破棄院の裁判例もある(*Yahoo!,* Hof van Cassatie van België, 1 December 2015, Nr. P.13.2082.N. (http://jure.juridat.just.fgov.be/pdfapp/download_blob?idpdf=N-20151201-1;非公式英訳 http://journals.sas.ac.uk/deeslr/article/viewFile/2310/2261))。加えて、サイバー犯罪条約 18 条が定めるデータの提出命令の対象に関しても、データが国外に保存されている場合が含まれる可能性は排除されていない(後記**第 5 の 2. (2)ア**参照)。

要求する場合は、他国に所在するサーバ管理者が、捜査機関が所在する国内の顧客に対して積極的にサービスを提供する等、捜査機関の所在国と他国に所在するサーバ管理者等との間に「正当な連結点」がある場合、捜査機関所在国の立法管轄権は及ぶと評価されるものの、執行管轄権については別途国際法上慎重な評価が必要となると思われる。国外のサーバ管理者等に直接データの提出を命じる捜査手法については、国家間の合意形成により、相手国の主権を侵害する捜査方法ではないことを確立していくことが重要である。

イ　捜査機関自らデータが保存された国外に所在するサーバにアクセスしてデータを取得する方法

日本のリモートアクセスのような、捜査機関が国外に所在するサーバに直接アクセスすることでデータを取得しようとする捜査手法は、国際法上、どのように評価されるか。

前述のとおり、他国領域内において、ある国が主権を行使することは、「国際慣習又は条約から導き出される許容的な規則による」場合を除き、領域主権の侵害に当たる[84]。

リモートアクセスは、刑事訴訟法等に従い別途取得したクレデンシャル情報(各ユーザーの ID 及びパスワード等)を用いて、ネットワークプロトコルに従い、自国領域内からデータにアクセスする捜査手法である。データが保存されているサーバの所在地が特定できておらず、それが国外に所在する可能性があったとしても、他国領域に物理的に捜査機関が立ち入るものではないため、「他国領域内」における執行管轄権に基づく強制措置に当たらないとする立場もあるが、国際法上、議論は分かれている[85] [86]。

84　S.S. Lotus (Fr. v. Turk.), 1927 P.C.I.J. (ser. A) No. 10 at 18-19 (Sep. 7).

85　Currie, Robert J., *Cross-Border Evidence Gathering in Transnational Criminal Investigation: Is the Microsoft Ireland Case the "Next Frontier"?*, 54 CANADIAN YEARBOOK OF INTERNATIONAL LAW 63, 76-80 (2017); また、国外に保存されているデータへのリモートアクセスを許容する旨の判断を下した国外の裁判例もある。例えば、韓国の捜査機関により、国外に所在するデータ・ストレージ媒体へのリモートアクセスを許容した事例(韓国大法院判決 2017 年 11 月 29 日(2017 年 9747)(原文 https://www.scourt.go.kr/sjudge/1512108215099_150335.pdf; 英訳 http://library.scourt.go.kr/SCLIB_data/decision/20_2017Do9747.htm))や、ノルウェーの捜査機関が、国内に所在する企業の端末から、国外に保存されているデータをダウンロードしたことを許容した事例がある(Tidal Music AS v. The public prosecution authority, 28 March 2019, HR-2019-610-A, (case no. 19-010640STR-HRET)(英訳 https://www.domstol.no/globalassets/upload/hret/decisions-in-english-translation/hr-2019-610-a.pdf))。

86　なお、近時では、単に企業がサーバの所在地を開示しないケースに留まらず、利用者がダークウェブ等を用いることにより、あえて意図的にサーバの所在を秘匿するケースも広まっている。この点について、そもそもこのようなサーバ所在地が判明しないケースでも、リモートアクセスのための令状を発付できるかという課題が指摘されている。これに対しては、当該サーバが国内にあることが必ずしも確認できなくとも令状は発付できるとの見解や、外国の同意があることは令状発付の要件とすべきではないとの見解が示されている(河村博ほか編『概説　サイバー犯罪――法令解説と捜査・公判の実際』157 頁[大原義宏](青林書院、2018)、笹倉宏紀「クラウド捜査」芝原邦爾ほか『経済刑法――実務と理論』571 頁(商事法務、2017)、杉山治樹「国外における捜査活動の限界」平野龍一＝松尾浩也『新実例刑事訴訟法　I』55-56 頁(青林書院、1998))。実際に米国には、データの所在地が技術的手段によって秘密にされている場合等には、越境的なリモートアクセスを認める令状の発付を認める連邦刑事訴訟規則 41 条が存在する。

それゆえ、後記 2. (2) で紹介するサイバー犯罪条約第二追加議定書案では、捜査機関が国外に所在するサーバにアクセスすることでデータを取得しようとする捜査手法の必要性に鑑みて、従来の領域主権の考え方に限定されない、国際法上の正当性を付与する試みがなされている[87]。なお、サイバー犯罪条約 32 条は、国外に所在するサーバに保存されたデータにアクセスできる場合を規定するが、その適用を受けるためには、サイバー犯罪条約に加盟すること、すなわちサーバ所在国の同意を取得すること及びデータ主体の同意があることが原則として前提とされており、サーバ所在国の同意が得られない場合の捜査の根拠にすることはできない。

一方、日本国内においても、リモートアクセスに関して、未だ定見があるわけではなく、さらに議論を深めていくべきである。

まず、日本のリモートアクセスの立法担当者は、国外に所在するサーバへのアクセスが当該他国の主権を侵害するか否かについて、国際的に統一した見解があるわけではないとしつつも、サーバが国外に所在することが明らかである場合には、当該サーバに対してリモートアクセスを行うことは控え、捜査共助によることが望ましいとの考えを示していた[88]。

このような考え方については、日本の刑事裁判例においても問題となってきているが、国外に所在するサーバにデータが保存されている可能性がある場合に、リモートアクセスではなく、MLAT に依拠することがどの程度必要かつ望ましいものと評価するかについては、これまで定まった判断が提示されていない。むしろそのような場合にリモートアクセスを実施することは、一概に否定されるべきではないとの見方も示されるようになってい

87 米国においては、MLAT 等の別途の国際的な手続きが存在したとしても、それが外国への管轄権の行使を抑制する一要素となるわけではないとの見解が採られてきたとの指摘が見当たる(石井由梨佳『越境犯罪の国際的規制』88-104、175-197 頁(2017))。

88 第 177 回国会衆議院法務委員会会議録 14 号(平成 23 年 5 月 27 日)10 頁[江田五月法務大臣答弁]、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 100-101 頁(2012)。

る[89]。

また、日本の学説上は、サーバ所在地が判明しない場合にまで MLAT に依ることを求めると、捜査機関に不可能を強いることになりかねないため、そのような場合には直ちにリモートアクセスができると解されるべきであり、仮に執行後にサーバが国外に所在すると判明したとしても、執行が遡って違法になることはないとの指摘がある[90]。また、国外に所在するサーバへのアクセスは、他国の領域に物理的に立ち入る場合とは区別するべきであるとして、主権侵害と解すること自体に疑問を呈する見解も存在する[91]。

(3) 各国法令間の抵触の調整

国外に所在するサーバに保存されたデータを捜査の目的で取得する場面では、前記(1)及び(2)で論じた主権ないし管轄権侵害の問題に加えて、個人の権利を保護する手続的なセーフガード(各国のデータ保護法令、個人情報保護法等)に抵触することを理由に、国際法上の制約を受けないかという問題も生じ得る。例えば、EU では早々に、CLOUD Act に基づく開示命令に応じて個人データを米国に移転することは、EU データ一般保護規則(EU/2016/679、The EU General Data Protection Regulation、以下「GDPR」という。)の越境移転規制(48 条)に抵触するとの見解が示されるとともに、EU 議会からは CLOUD Act が定める手続き等が GDPR に適っていないとして、EU・米国間のプライバシーシールドの停止が勧

---

89 横浜地判平成 28 年 3 月 17 日 LEX/SB25542385 は、「サーバコンピュータが外国にある可能性が高く、捜査機関もそのことを認識していたのであるから、この処分を行うことは基本的に避けるべきであったといえる」と指摘し、リモートアクセスの利用に慎重な考慮を促すかのような判示をするも、その控訴審である東京高判平成 28 年 12 月 7 日高刑集 69 巻 2 号 5 頁は、「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」との判断を示した。その後の大阪高判平成 30 年 9 月 11 日 LEX/DB25449705(上告中)は、「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(注：サイバー犯罪)条約 32 条によりアクセス等をする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」と指摘するに止まり、さらに、東京高判平成 31 年 1 月 15 日 L07420003(上告中)も、「上記の場合にリモートアクセスを行うためには、国際捜査共助を要請するのが望ましいとしても、これを行わずにリモートアクセスを行ったことにより、外交上の問題を生じ得ることはともかく、わが国の刑訴法の解釈上，捜査の違法性の判断に直ちに影響を及ぼすものではないというべきである」と述べた。なお、同東京高判は、証拠能力について、リモートアクセスが捜査共助の要請なく行われたことは、「証拠能力を判断するに当たって考慮すべき事項とはいえない」とまで判示している。最高裁の判断が待たれる。

90 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』428-429 頁(有斐閣、2019)。

91 山内由光「検証許可状に基づき押収済みのパソコンから海外メールサーバに接続した捜査に重大な違法があるとして証拠が排除された事例」研修 832 号 13 頁、22-25 頁(誌友会事務局研修編集部、2017)。

告されたこともあった [92]。さらに、欧州データ保護監督官(EPDS)及び欧州データ保護会議(EPDB)が欧州議会の市民的自由・司法・内務委員会(LIBE Committee)に宛てた共同返答書簡は、GDPR 48 条に抵触することを指摘するとともに、EU・米国間において電子証拠へのアクセスに関する包括的な協定を締結することの重要性を強調している [93]。

しかし、自国でいかなる法律を制定するかについては、立法管轄権の範囲内であれば基本的にはその国が裁量を有する。また、協定を締結した国家間の法律が抵触した場合の調整方法については、確立した国際法上の規則があるとは言い難い [94]。

米国では国内法による処理として、各国の利益考慮に基づくコミティを活用している。実際に CLOUD Act においても、前記**第 3. の 2.** のとおり、一定の要件を満たす場合には、データの開示命令を受けたプロバイダが米国裁判所に当該命令の修正又は取消を申し立てることができる旨を定めているが、米国裁判所はかかる申立ての判断を行う際にコミティを考慮する旨を定めている [95]。一般法上のコミティに関しては、コミティの判断の外延には曖昧さが残り、予測可能性の観点から問題がないか、自国に有利な判断がなされないかについて課題があるが、CLOUD Act においてはコミティ判断の考慮要素が定められており、一定の対処が試みられている。

さらに、CLOUD Act では、行政協定の締結により、個別法の抵触を調整することが想定されているが、この点については、後記**第 6.** において詳述する。

2. サーバ所在国の同意を得る場合やその他の方法の検討状況

次に、サーバ所在国の同意を得て国外に保存されたデータを取得する場合には、国家管轄権の抵触の問題は生じないところ、国際的に、サーバ所在国の同意を得るための枠組み作りが進んでいる。また、サーバ所在国の同意を得ずに適法に執行管轄権を行使する方法についても、国際的な枠組みの検討が進められている。

(1) 刑事相互共助条約(MLAT)

捜査機関が他国に所在する被疑者又は証拠の捜査を行うには、当該被疑者又は証拠の所

---

92 European Parliament, “Adequacy of the protection afforded by the EU-US Privacy Shield European Parliament resolution of 5 July 2018 on the adequacy of the protection afforded by the EU-US Privacy Shield”, 2018/2645(RSP), *available at* http://www.europarl.europa.eu/doceo/document/TA-8-2018-0315_EN.pdf.

93 EPDB-EDPS Joint Response to the LIBE Committee on the impact of the US Cloud Act on the European legal framework for personal data protection, *available at* https://edpb.europa.eu/our-work-tools/our-documents/letters/epdb-edps-joint-response-libe-committee-impact-us-cloud-act_en.

94 酒井啓亘ほか『国際法』86 頁(有斐閣、2011)。

95 CLOUD Act Sec.103(b), 18 U.S.C. 2703(h).

在国に外交ルートを通じて共助を要請することが考えられる。また、MLAT を締結している相手国との間では、外交ルートを経由することなく、直接、自国の関係機関(日本の法務省等)から相手国の当局(米国の司法省等)に共助を要請することも可能である[96]。

この MLAT を通じた手続きは、外交ルートを通じた要請よりは簡略ではあるものの、一般的には 6 ヶ月から 24 ヶ月(平均的には 10 ヶ月)程度の時間を要しているのが実情であり[97]、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る[98]。さらに、どの国にデータが保存されているか捜査機関にとって不明である場合(Loss of Location)には、MLAT では対応できないのが実情である[99]。

(2) サイバー犯罪条約

サイバー犯罪条約は、2001 年に採択された、コンピュータ・システムに対する違法なアクセス等一定の行為の犯罪化、コンピュータ・データの迅速な保全等に係る刑事手続の整備、犯罪人引渡し等に関する国際協力等につき規定する条約である。

サイバー犯罪条約では、国境を越えた捜査目的でのデータの取得に関する一定の規律が整備された[100]。

ア　データ提出命令(18 条)

まず、自国の領域内に所在する者に対してデータ提出を要求することに関して、サイバー犯罪条約 18 条は、次の 2 つの事項を行う権限を加盟国の捜査機関に与えるため、必要

96　例えば、刑事に関する共助に関する日本国とアメリカ合衆国との間の条約 2 条 2 項及び 3 項。

97　Council of Europe Cybercrime Convention Committee (T-CY) Cloud Evidence Group, *Criminal justice access to data in the cloud: Recommendations*, 9 (2016); Sieber, Ulrich, and Carl-Wendelin Neubert, *Transnational Criminal Investigations in Cyberspace: Challenges to National Sovereignty*, 20 MAX PLANCK YEARBOOK OF UNITED NATIONS LAW 241, 308 (2017); Schwartz, Paul., *Legal Access to The Global Cloud*, 118 COLUM. L. REV. 1681, 1721-1722 (2018).

98　指宿信「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」Law & technology82 号 47 頁(2019)。

99　UNODC, *Comprehensive Study on Cybercrime*, 217-218(2013), *available at* https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf; Sieber, Ulrich, and Carl-Wendelin Neubert, *Transnational Criminal Investigations in Cyberspace: Challenges to National Sovereignty*, 20 MAX PLANCK YEARBOOK OF UNITED NATIONS LAW 241, 308 (2017); Schwartz, Paul,Legal Access to The Global Cloud, 118 COLUM. L. REV. 1681, 1721-1722 (2018).

100　Currie, Robert J., *Cross-Border Evidence Gathering in Transnational Criminal Investigation: Is the Microsoft Ireland Case the "Next Frontier"?*, 54 CANADIAN YEARBOOK OF INTERNATIONAL LAW 63, 77-78 (2017).

な立法その他の措置をとることを加盟国に義務付けている[101]。

(i) 自国の領域内に所在する者に対し、当該者が保有し又は管理している特定のコンピュータ・データであって、コンピュータ・システム又はコンピュータ・データ記憶媒体の内部に保存されたものを提出するよう命令すること(18 条 1 項 a 号)

(ii) 自国の領域内でサービスを提供するサービスプロバイダに対し、当該サービスプロバイダが保有し又は管理している当該サービスに関連する加入者情報を提出するよう命令すること(18 条 1 項 b 号)

サイバー犯罪条約の注釈書は、同条における「保有し又は管理している」の意味について、①その者が、命令を発した締約国の領土内において関連データを物理的に保有していること、及び②提出されるべきデータを物理的に保有していないものの、命令を発した締約国の領土内から、自由に当該データの提出を管理できる状況にあることを指すとしている[102]。ただし、②に関し、当該データが国外に保存されている場合も含まれているかどうか、すなわち、サイバー犯罪条約は、対象となるコンピュータ・データが国外に保存されている場合をも想定しており、そうした場合にも提出命令が可能であることを締約国が合意したものであると解釈できるかどうかについては争いがある[103]。

それ故、後記**ウ**のとおり、サイバー犯罪条約の第二追加議定書では、データの保存場所が明確でない場合の管轄権の行使基準について、さらに検討が続けられている。

イ　データに対する越境アクセス(32 条(b))

次に、サイバー犯罪条約 32 条(b)は、「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」、つまりデータ主体(サーバの管理者等

---

101 サイバー犯罪条約 18 条 b の「加入者情報」とは「コンピュータ・データという形式又はその他の形式による情報のうち、サービスプロバイダが保有するサービス加入者に関連する情報(通信記録及び通信内容に関連するものを除く。)」を指す(サイバー犯罪条約 18 条 3 項柱書)。

102 Committee of Ministers of the Council of Europe, *Explanatory Report to the Convention on Cybercrime*, 29 (2001), *available at* https://rm.coe.int/16800cce5b

103 この点、米国 Deputy Assistant Attorney General は、サイバー犯罪条約 18 条 1 項 a 号における国家の義務として、CLOUD Act を制定したと説明している(*Deputy Assistant Attorney General Richard W. Downing Delivers Remarks at the Academy of European Law Conference on "Prospects for Transatlantic Cooperation on the Transfer of Electronic Evidence to Promote Public Safety"*, April 5, 2019, *available at* https://www.justice.gov/opa/speech/deputy-assistant-attorney-general-richard-w-downing-delivers-remarks-academy-european-law)、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』414 頁、416 頁脚注 6(有斐閣、2019)。

が契約等により開示権限を有する場合は事業者を含む。)の同意が得られる場合(同条(b))[104]に、他国所在のサーバに保存されたデータにアクセスできるとする。

同条(b)に定められた行為と国家主権ないし執行管轄権との関係性については、他国領域における管轄権の行使を認める例外的な規定であるとの考え方や、同条(b)に定められた行為は、サーバ所在国の管轄事項に「干渉」する行為態様には当たらないといった考え方がある[105]。

さらに、同条(b)は、同条項に記載された行為以外の捜査を禁止又は排除したわけではなく、将来における解決策の発展の余地を残しているとされている[106]。

ウ　第二追加議定書案

欧州評議会のサイバー犯罪条約委員会では、2022 年 12 月の採択を目指し、第二追加議定書案を交渉中である[107]。

この第二追加議定書案では、越境捜査については捜査共助を基本としつつも、プロバイダからの直接協力を補助的に用いることや法的枠組みを明確化してデータ保護を含む安全策を講じるとの方針が示されている[108]。特に、プロバイダからの協力の点につき、クラウドサービスを展開するプロバイダに対する照会が適切に行われるための要件や手続きに関する法的枠組みの整備が必要であると提案されていること、照会に際しては、相手国の個人情報保護や刑事訴訟法上の手続上の権利も十分に保証される必要があると指摘されてい

104　サイバー犯罪条約 32 条(b)の例として、(i)法的権限のあるデータ主体が、SPC により他国に所在するサーバに保存されている、又はデータ主体によって意図的に他国に所在するサーバに保存されている E メールを取得し、これを任意に捜査機関に提供する場合及び(ii)逮捕された被疑者のパソコン又はスマートフォンにメールボックスがある場合に、当該サーバが別の加盟国に保存されていることを捜査機関が確実に認識している場合、被疑者の同意に基づき、捜査機関は当該データを見ることができることが挙げられる(Council of Europe Cybercrime Convention Committee (T-CY)), *T-CY Guidance Note # 3: Transborder Access to Data (Art. 32)* (op. cit. n. 70), 5 (2014))。

105　UNODC, *Comprehensive Study on Cybercrime*, 218 (2013), *available at* https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf, Council of Europe Cybercrime Convention Committee (T-CY), *Transborder access and jurisdiction: What are the options?*, Doc No T-CY (2012)3, 27 (2017).

106　Council of Europe Cybercrime Convention Committee (T-CY), *Transborder access and jurisdiction: What are the options?*, Doc No T-CY (2012)3, 27 (2017).

107　Council of Europe Cybercrime Convention Committee (T-CY), *Preparation of the 2nd Additional Protocol to the Budapest Convention on Cybercrime State of play Note by the Chair for the attention of the 21st Plenary of the T-CY*, 4 (2019), *available at* https://rm.coe.int/t-cy-2019-19-protocol-tor-extension-chair-note-v3/16809577ff

108　指宿信「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」Law & Technology 82 号 54 頁(2019); Council of Europe Cybercrime Convention Committee (T-CY), *Criminal Justice access to data in the cloud: Cooperation with "foreign" service proiders, T-CY (2016)*, 2 (2016).

ることが注目に値する[109]。

また、同条(b)でカバーされない捜査形態、すなわち、データ主体の同意が得られない場合について、サイバー犯罪条約委員会クラウド証拠部会(Council of Europe Cybercrime Convention Committee (T-CY) Cloud Evidence Group)では、捜査機関が合法的に獲得したクレデンシャル情報(ユーザーID やパスワード等)を用いる場合や、差し迫った危険、物理的な危害、証拠隠滅、被疑者の逃亡のおそれがあるといった、緊急若しくはその他の事情がある場合には、他国所在のサーバに保存されたデータへのアクセスを認めること等が検討されている[110]。同部会では、サイバー空間に対して伝統的な属地主義を適用することの限界を踏まえた国外に保存されたデータを取得する捜査に関する管轄権の在り方についても、参考にすべき考え方が提案されている。データの保存場所が次々に変わる場合や、一つのデータが様々な場所に分散して保存されている場合等データの保存場所が明確でない場合には、属地主義に従ってデータが保存されている領域国に執行管轄権があると判断することが妥当でなく、このような場合、データを排他的に処分する権利を有する者と自国との間に正当な連結点(前記 **1. (1)ア**参照)があれば、当該国の捜査機関は、そのデータ又はその媒体に対して執行管轄権を及ぼし得るという考え方も提示されている[111]。

(3) 米英行政協定

CLOUD Act に基づく行政協定は、自国の管轄権が及ぶ企業に対する開示命令が、少なくとも行政協定を締結した 2 国間では相手国の主権を侵害するものではないことを明確化する機能を有するところ、2019 年 10 月 3 日に、米国と英国との間で米英行政協定が締結された(前記**第 3. の 2**)。

同協定に基づき、米英間では、一方当事国の当局から相手国のサービスプロバイダに直接、捜査機関所在国の法令における重大犯罪に関連するデータの提出を求めることができ

---

109 Council of Europe Cybercrime Convention Committee (T-CY) Cloud Evidence Group, *Criminal justice access to data in the cloud: Recommendations*, 44 (2016).

110 Council of Europe Cybercrime Convention Committee (T-CY) Cloud Evidence Group, *Criminal justice access to data in the cloud: Recommendations*, 44-45 (2016); Spoenle, *Cloud computing and cybercrime investigations: territoriality vs. the power of disposal?* discussion paper, Project on Cybercrime, Council of Europe, Strasbourg, 11 (2010), *available at* https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa3df.

111 本来であれば、執行管轄権は自国領域内でのみ行使することができ、MLAT においても、捜査機関国は、捜査を実施する国の当局に対して共助要請を行う必要がある。しかし、データの保存場所が明確でない場合にはどの国がデータに対して主権を及ぼし得るのかが特定できないため、多くの国の捜査機関において、所在不明なデータに直接アクセスする等の事例が生じている。この点について、当該データの処分権又は支配権を有する人に対してある国が管轄権を有する場合、すなわち、データの変更、削除、使用を不可能にする等、排他的に処分する権利を有する人とある国が正当な連結点を有する場合には、当該国家が当該個人又は法人のデータに、データ所在国の同意なくしてアクセスすることができるとの見解が示されている(Council of Europe Cybercrime Convention Committee (T-CY) Cloud Evidence Group, *Criminal justice access to data in the cloud: Recommendations*, 44-46 (2016))。

る(同協定 1 条、4 条、5 条)。しかし、英国に関しては、取得されたデータが米国において死刑事件の訴追に用いられる場合、米国に関しては、取得されたデータが英国において米国の表現の自由に懸念を生じさせるような訴追に用いられる場合に、当該データ使用を拒否することができる権利がそれぞれ規定されている(同協定 8 条 4 項)。

第6. 行政協定の締結に関する検討課題

1. 行政協定の機能

前記**第 3. の 2.** のとおり、CLOUD Act では、米国政府と外国政府の間で、プロバイダに対する直接のデータ開示命令の在り方について、行政協定を締結することが想定されている。行政協定は、自国の人的管轄権が及ぶ企業に対する開示命令が、少なくとも行政協定を締結した 2 国間では相手国の主権を侵害するものではないことを明確化する機能を有するが、これに加え、他国と米国との間の潜在的な法の抵触(前記**第 5. の 1. (3) 参照**)を除去する機能を営むことも想定されている[112]。

以下では、具体例として、米国政府が CLOUD Act に基づいて日本の事業者に対してデータの提出を命令する場面において、日本法上、どのような問題が生じ得るかを整理した上で[113]、これを踏まえて、日本が米国との間で行政協定を締結する場合に、どのような点に留意して行政協定を設計すべきかを検討する。

2. 日本の国内法と CLOUD Act に基づく捜査活動の関係

(1) 日本国憲法との関係

CLOUD Act の下では、米国の管轄権が及ぶ日本の企業が、米国政府から米国法上の令状(warrant)等に基づきデータの提出を求められる可能性が生じる。

外国の捜査機関の行為には、日本国憲法は適用されない。そのため、日本の企業が、米国政府から米国法上の令状等に基づきデータの開示を求められたとしても、直ちに日本国憲法上の問題は生じない。

しかし、当該令状等は日本の裁判所による令状審査手続(憲法 35 条)を経たものではない以上、そのような求めに応じて米国政府に対してデータが開示されることをそのまま容認してしまうことが日本政府が負い得る国民の憲法上の権利を保護する義務に抵触しないか

---

112 U.S. Department of Justice, *Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act*, 4-5 (2019), *available at* https://www.justice.gov/opa/press-release/file/1153446/download.

113 なお、日本政府が日本法に基づいて米国の事業者に対してデータの提出を命令する場面において、米国法上、どのような問題が生じ得るかについては、別途の整理が必要となる。

という点や、そのような義務を果たすために日本政府は行政協定の締結等の手法を通じて、CLOUD Act に基づく米国政府からの要請が日本国憲法上の適正手続の要請(憲法 31 条)を満たすようにする必要があるのではないかといった点を検討していく必要がある。

(2) その他の法令との関係

ア　電気通信事業法

米国政府から、日本の事業者が、電気通信事業法上、通信の秘密として保護される情報を含むデータの開示を命令された場合、これに応じることは通信の秘密侵害罪の構成要件に該当し得る(電気通信事業法 179 条)。そこで、このような開示が法令行為(刑法 35 条)や、緊急避難(同法 37 条)といった違法性阻却事由に該当し、電気通信事業法上許容されないかを検討する必要が生じる。

この点について、法令行為にいう「法令」に該当するのは日本の法令に限られると解されるため[114]、当該データの開示を法令行為であることを理由に正当化することはできない。

他方で、緊急避難により保護すべき法益には、外国に所在する個人(日本国籍者ではない者も含み得る)の生命・身体の法益を含まれる場合があると解されている[115]。このことを踏まえると、外国に所在する個人を巡る犯罪に関して、外国政府から開示命令がなされた場合に、緊急避難が成立する余地を認めることも可能であると考えられる。もっとも、実際にどのような範囲で緊急避難が成立するかについては、法益侵害の内容や程度、開示の補充性、法益の均衡といった緊急避難の各成立要件を慎重に検討する必要がある。また、開示に対応する電気通信事業者の予見可能性の観点からの手当ても要すると思われる。

114　宮本英脩『刑法学粋』227 頁(弘文堂、1931)参照、刑法理論研究会『現代刑法学原論〔総論〕第 3 版』228 頁(三省堂、1996)参照。

115　緊急避難の成立要件の一つである「現在の危難」の存否に関連して、外国における日本国籍者ではない個人の生命・身体に対する危険の存在をもって「現在の危難」の存在を肯定し得ることを示唆した裁判例として、福岡高判昭和 40 年 9 月 17 日下刑集 7 巻 9 号 1778 頁や、松江地判平成 10 年 7 月 22 日判時 1653 号 156 頁(ただし、控訴審(広島高判松江支判平成 13 年 10 月 17 日判時 1766 号 152 頁)は、現在の危難の存否について明示的に判断することなく緊急避難の成立を否定した。)が挙げられる(西田典之ほか編『注釈刑法第 1 巻　総論　§§1〜72』480 頁(有斐閣、2010)[深町晋也])。また、児童ポルノに該当する情報のブロッキングについて、当該児童ポルノが保存されているサーバが海外に所在し、かつサーバの管理者等が海外に所在する場合又は不明である場合には、当該児童ポルノの被害児童が日本人か外国人かに関係なく、当該児童ポルノを日本においてブロッキングする行為には緊急避難が成立し違法性が阻却されると論じるものとして、安心ネットづくり促進協議会児童ポルノ作業部会「法的問題検討サブワーキング　報告書」18 頁(2010 年 3 月 30 日公表)(https://www.good-net.jp/investigation/working-group/anti-child-porn_category_112/2010_169-1751_475)が挙げられる。

イ　個人情報保護法

個人情報保護法上、個人情報取扱事業者は、原則としてデータ主体の同意がない限り当人の個人情報を第三者に提供することが禁止されている(同法 23 条 1 項)。その例外として定められている第三者提供の適法性根拠としては、「法令に基づく場合」(同項 1 号)が存在するが、同条にいう「法令」には外国法令が含まれないと解されている [116]。同様に、他の適法性根拠である国等の法令事務の遂行に協力する場合(同 1 項 4 号)についても、「法令」には外国法令は含まれず、また、「国」には外国は含まれないと解されている。そのため、日本の個人情報取扱事業者が、米国政府から個人情報の開示を命令され、これに応じた場合、個人情報保護法に抵触するおそれがある。

3.　行政協定設計上の留意点

まず、日本では、大平三原則 [117]に照らし、CLOUD Act に基づく行政協定は、国会の承認が必要である「条約」に相当すると考えられる [118]。加えて、日本が米国との間で行政協定を締結するための協議を行うとすれば、その設計の在り方として、主に以下の点に留意する必要があると考えられる [119]。

(1)　日米両国の国内法間の調整

前記 2. のとおり、米国政府が、日本の企業に対して CLOUD Act に基づく開示命令を行ったとしても、そのままでは、日本国憲法や他の国内法に整合しないおそれがある。

この点について、CLOUD Act 上、行政協定において、相手国からの開示命令に対する要

116　「衆議院議員松平浩一君提出米クラウド法と個人情報保護法上の対応に関する質問に対する答弁書」(令和元年六月二十五日受領答弁第二二七号)(http://www.shugiin.go.jp/Internet/itdb_shitsumon_pdf_t.nsf/html/shitsumon/pdfT/b198227.pdf/$File/b198227.pdf)。

117　①法律事項を含む国際約束(例えば、当該国際約束の締結によって、新たな立法措置の必要がある場合等)、②財政事項を含む国際約束、及び③政治的に重要な国際約束に関しては、憲法 73 条 3 号により国会の承認が必要であるとする原則。一方、既に国会の承認を経た条約の実施細目を定めた国際約束や規定の法律又は予算の範囲内で実施できる国際約束については、行政府限りの外交処理権の一環(同条 2 号)として締結できる行政取極めにあたり、国会の承認を要しない(国会承認条約に関する大平外相答弁(1974 年 2 月 20 日)、山本草二『国際法〔新版〕』106-109 頁(有斐閣、1994))。

118　一方、米国においては、CLOUD Act に基づく行政協定に対する国会によるチェックの仕組みが定められており、司法長官による行政協定認証の通知から 180 日以内に、国会が不承認の共同決議を行った場合には当該行政協定の効力を生じない旨が定められている(CLOUD Act Sec.105(a), 18 U.S.C. Sec. 2523(d))。

119　州レベルで行政協定上の義務履行の確保が可能かどうかを検討することも必要になり得る。

件を加重することは可能であると解されている[120]。例えば、米国法上、文書提出命令状(subpoena)の取得には、相当な理由(probable cause)を要求する令状(warrant)と異なり、合理的な嫌疑(reasonable suspicion)の存在しか要求されず、捜索差押えの対象の特定性も日本の令状審査に比べれば緩やかであること等を踏まえ、各制度の要件を緻密に検証し、日本の令状審査と同等の要件を求めることが考えられる。また、米国における弁護士・依頼者間秘匿特権のように、どちらか一方の国にしか存在しない制度については、その対応をどのように行うかを行政協定において明確にしておくことが必要である。

(2) CLOUD Act の文言の明確化

CLOUD Act には、「意図的に標的とする(intentionally target)」[121]、「重大な犯罪(serious crime)」[122]等の解釈が必ずしも明確ではない文言が存在するため、それらの文言の解釈を巡ってかえって捜査が滞ることのないよう、その意義を明確化しておくことが重要である[123]。

(3) 日本国民の保護

CLOUD Act は、外国政府が、米国市民をターゲットとする場合には、従来通り、MLAT に依ることを求めている[124]。そこで、日本としても、相互主義の下、米国の捜査が日本国民をターゲットとする場合にも、MLAT に依ることを求めることが考えられる。実際に、米英行政協定では、双方の住民を(意図的に)標的にしないことが定められた(同協定 4 条 3 項)。

---

120 例えば、米英行政協定では、プロバイダによるデータの開示が、データ保護法に整合するものであるべきことを確認している(同協定 2 条等)。また、データの開示命令それ自体についてではないが、同協定では、特に米国における死刑事件及び英国における表現の自由に関する事件において、行政協定に基づき取得したデータを用いる場合には、相手国の承諾を得ることが必要である旨が規定されたようである(同協定 8 条 4 項)。この他にも、アカデミアにおける検討例が現れている(Madhulika Srikumar et al., *India-US data sharing for law enforcement: Blueprint for reforms* (Jan 17, 2019), *available at* https://www.orfonline.org/research/india-us-data-sharing-for-law-enforcement-blueprint-for-reforms-47425/。

121 CLOUD Act Sec.105(a), 18 U.S.C. Sec. 2523(b)(4)(A).

122 CLOUD Act Sec.105(a), 18 U.S.C. Sec. 2523(b)(4)(D)(i).

123 例えば、米英行政協定では、「重大な犯罪(serious crime)」とは、3 年以上の長期刑が課され得る犯罪を意味する旨が規定されている(同協定 1 条 14 項)。

124 U.S. Department of Justice, *Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act*, p.12 (Apr. 2019), *available at* https://www.justice.gov/opa/press-release/file/1153446/download.

(4) 他の国際協定等への影響

日本が米国と行政協定を締結した結果、日米間での捜査目的での越境的なデータの取得が円滑なものとなることが期待される反面、そのようなデータの流通が、日本が締結している他の国際協定に影響しないかも留意しておく必要がある。例えば、EU の GDPR は、EU から日本への越境移転だけでなく、日本から第三国への越境移転に対しても規制をかけることで、データの国際的な流通に統制を及ぼそうとしていることからすると、日本政府と米国政府との間のデータの流通が十分な個人情報の保護水準を保って行われることは重要である[125]。

(5) 国内での実施法・担保法の整備

日本法と CLOUD Act との調整を行うためには、行政協定の締結に加え、特に既存の国内法との抵触が見られる内容については、その実施法・担保法が必要であると考えられる。例えば、CLOUD Act に基づく米国政府からの開示命令に応じることが、電気通信事業法上の通信の秘密を違法に侵害するものではなく、また、個人情報保護法に違反するものではないことを明確化する規定を設けることが必要になる。

第7. 企業における透明性確保の現状と今後の方向性

昨今、国内外のデータ保有企業は、各国の政府機関から受けた、自社が保有している情報への開示要請やコンテンツの削除要請への対応方針や状況等について、透明性レポートの形で公表している。現状では各社ごとにその公表内容にはバリエーションがあるが、政府機関からの要請に対する対応方針のほか、要請の種類別の件数や、そのうち実際に開示した件数の割合、利用者から取得する情報の暗号化に関する技術的保護等を公表している企業がある。以下に、その概要を簡潔に掲載する。

125 日本は、2019 年 1 月 23 日、欧州委員会から、個人データの移転を行うことができるだけの十分な個人データ保護水準を持つ旨の十分性認定を受けた。その際、日本政府は、欧州委員会からの要請に応える形で、刑事捜査や安全保障の観点から行われる、EU 域内から日本に移転した個人データに対する日本の政府機関によるアクセスは、必要かつ相当な範囲に限定され、かつ独立機関による監督を受ける旨の説明を添えていた。

社名	開示項目の概要
企業 A	ユーザーの情報開示・削除要請の対応件数、対応割合、対応方針
企業 B	ユーザーの情報開示・削除要請それぞれの内訳、対応件数、対応割合、対応方針
企業 C	ユーザーの情報開示の対応件数、対応レベル別の件数
企業 D	ユーザーの情報開示・削除要請それぞれの内訳、対応件数、対応割合
企業 E	ユーザーの情報開示・削除要請それぞれの内訳、対応件数、対応割合、対応方針
企業 F	ユーザーの情報開示・削除要請それぞれの内訳、対応件数、対応割合、対応方針

日本企業においては、パブリック・アクセスに対する対応の透明性確保が重要な課題であることの認識は広まりつつも、これまでのところ、こうした透明性レポートを公開している企業は限られているように思われる。

今後、日本企業においても、政府機関からの開示要請に対する対応状況等を取り纏め、公表し、透明性を高めていくことによって、データ主体の保護を図り、市民社会の理解を得ながら、捜査への適切な協力を実現していくことが可能になると考えられる。このような取組みは、データ主体である企業のサービスの利用者に安心感を与える。また、市民社会における企業イメージの向上にもつながり、ひいては、プライバシーに対する権利意識が高まっている社会情勢を反映して、企業の競争力をも高めるものであるといえる。具体的な取組みを検討する際には、透明性レポートの在り方について、より利用者にとって分かり易いものにするにはどうすべきかといった議論も期待される。

第8. 今後の展望

1. 捜査を目的とする越境的なデータの取得と DFFT との関係

デジタル経済を推進していくにあたって、日本政府は、積極的に、日米欧のデータ経済圏構想や、DFFT の実現について発信を行っている。また、環太平洋パートナーシップに関する先進的かつ包括的な協定(CPTPP 協定)や United States–Mexico–Canada Agreement(USMCA＝新 NAFTA)といった最新の国際通商ルールにおいてもデータの自由な移転という基本原則が具体化されている。

しかしながら、国境を超えたデータの移転が活発化することによって、データに対する法執行の実効性への懸念が高まれば、かえって幅広くデータローカライゼーションが許容されるべきということになり、こうした傾向が反転するおそれがある。こうした観点からも、捜査機関が、必要かつ相当な場合に国外のデータに対してアクセスできることを確保していくことの意義が認められる。

2. 国際的枠組みを有志国間で構築していくことの意義

捜査目的での越境的なデータの取得について調査研究を行っているインターネットと管轄政策ネットワークに設置されているデータと管轄ワーキンググループが策定した「オペレーショナル・アプローチ」は、今後広がりを見せ得る捜査目的での越境的なデータの取得に関する国際的な枠組みとして、①CLOUD Act、②EU の電子証拠指令案及び規則案、並びに③サイバー犯罪条約の追加議定書案の 3 つを提示している[126]。

この点について、多国間で国際的な枠組みを構築することができれば、当該枠組みが国際的な捜査協力のための安定的な土台となる。その意味で、先に紹介したサイバー犯罪条約の追加議定書案については、早期の採択を目指すべきである。同時に、迅速性と実現可能性からすれば、まさに DFFT の精神に倣い、価値観を共有できる有志国間で先行して、着実に枠組み作りをしていくことが適切なようにも思われる。したがって、日本としては、このような観点からも、CLOUD Act が想定しているような二国間での国際協定の締結も視野に必要な法的論点の検討を進めていくことが有意義であると思われる。

以　上

126 Internet & Jurisdiction Policy Network, *Concrete Proposals for Operational Norms, Criteria and Mechanisms* (Apr. 23, 2019), available at https://www.internetjurisdiction.net/news/operational-approaches-documents-with-concrete-proposals-for-norms-criteria-and-mechanisms-released. さらに、いわゆる「ガバメントアクセス」の観点からデータの越境移転及びその制限に関する国際的な枠組み作りを検討したものとして、渡辺翔太「ガバメントアクセス(GA)を理由とするデータの越境移転制限―その現状と国際通商法による規律、そして DFFT に対する含意―」(2019 年 12 月)(https://www.rieti.go.jp/jp/publications/summary/19120008.html)もある。