西村高等法務研究所

CLOUD Act（クラウド法）研究会

報告書 Ver.2.0

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

Ver.2.0　2023年4月

Ver.1.0　2019年12月

NISHIMURA & ASAHI

西村高等法務研究所
Nishimura Institute of Advanced Legal Studies

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≫
(2023 年 4 月現在)
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　根本　拓
同　角田　龍哉
同　室町　峻哉
同　大和田　華子
同　小川　慶

(2019 年 12 月当時)
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≫
本研究会においては、本報告書 Ver. 1.0 を公表するまでに、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、あくまでも本研究会に参加する西村あさひ法律事務所の弁護士等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。

さらに、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、検討の過程で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上で、2019年12月、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。

その後、国内では越境リモートアクセスについて判断した最決令和3年2月1日刑集75巻2号123頁(以下「**令和3年最高裁決定**」という。)や刑事手続のIT化を巡る議論の進展があり、また国際的にはサイバー犯罪条約第二追加議定書のほか、CLOUD Actに基づく行政協定、EUにおける電子証拠の収集を巡る規制、OECDにおけるガバメントアクセスに関する議論等に関する進展があったことを踏まえ、2023年4月、本報告書をアップデートした。

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 及び電子証拠の取得等に関する包括的な法的枠組みを定めることを目指すEUの電子証拠規則案及び指令案の概要と意義について説明する。このような国際的な動向を踏まえた上で、**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**

[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48参照。

文集(2023 年 4 月時点)。

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国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。

しかし、企業が国内外において保有するデータを取得する捜査手法の制度設計はいまだ発展途上であり、また制度設計にあたっては以下のような多様な論点について検討する必要があるものの、これらの論点が十分に整理されているとは言い難い。

すなわち、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]の権利利益の保障や、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、本報告書において各論点に関する議論を整理した上で、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：

- ✓ 企業におけるデータの蓄積が進んだ昨今において、捜査機関としては、企業とも連携しながら、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。そのための制度として、現行法上、記録命令付差押えが存在し、積極的な活用が期待されるが、課題も存在する。そのような中、現在、法務省の法制審議会・刑事法(情報通信技術関係)部会において、令状手続の電子化・オンライン化や、電磁的記録提供命令の創設に向けた検討が行われており、これらが実現することで、捜査機関と企業の間の円滑な連携を通じたデータの効率的かつ実効性のある取得が更に促進されることが大いに期待される。これらの制度の設計にあたっては、データを保有する企業に対するオンラインでの令状の呈示及びデータの提出におけるセキュリティの確保や、データ主体に対する事前又は事後の通知等の手続の公正性・透明性の担保、

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 4 項)として想定する主体を想定している。

秘密保持の義務付け制度等の拡充、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検討課題があるところ、こうした検討課題について、技術革新・捜査の高度化や国内外の企業の対応方針・対応状況、諸外国・国際的なフォーラムにおける動向も踏まえつつ、捜査機関の捜査能力と関係者の権利保護の双方を強化する方向で、議論を深めていく必要がある(後記**第 4. の 1.**)。

- ✓ また、企業が保有するデータを取得する捜査手法としては、他にも、データが保存されたサーバに捜査機関が自らアクセスしてデータを取得する方法(リモートアクセス)がある。このような捜査手法には、企業に対してデータの提出を求める捜査手法とは異なる有用性がある一方で、今後、データ主体やサーバ管理者である企業の利益や手続保障に配慮する制度設計を更に検討することが望まれる(後記**第 4. の 1.**)。
- ✓ 加えて、取得したデータの公判での利用も見据えた検討も求められる。この点、法務省の法制審議会においては、データが証拠として提出された場合の公判における取り調べ方法等について検討が進んでいるが、更に進んで、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については、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。日本でも、令和 3 年最高裁決定を契機として、越境的なデータの取得に関する手法やその限界についての議論が進展しているが、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.**)。
- ✓ 国際連携の進め方については、サイバー犯罪条約と同第二追加議定書のような、多国間での枠組みを構築するアプローチのほかにも、CLOUD Act が定める行政協定が想定しているように、二国間(又は複数国間)の枠組みを積み重ねていくアプローチも想定できる。日本としては、多国間の枠組み構築に向けた議論にも参画しつつも、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、例えば、企業が保有するデータへの公的機関によるアクセス(ガバメントアクセス)に関するOECDガバメントアクセス宣言(後記**コラム①**)のような国際的に認められた原則や基本的な価値観を共有する有志国間で、そのような二国間(又は複数国間)の枠組み作りを着実に先行させていくことが効果的

であると考えられる。今後、日本国内で電磁的記録提供命令その他の制度整備が進めば(提言 1 参照)、米国をはじめとする有志国との二国間(又は複数国間)の連携を可能とする制度的な下地も整うことになるため、有志国との国際協定の締結のために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　企業におけるガバメントアクセスに対する透明性確保の取組の推進：

- ✓ 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に加えて、ガバメントアクセス要請についての対応状況を集計した透明性レポートの公表や、対応方針の作成・公表など、ガバメント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も重要となる(後記**第 7.**)。
- ✓ このような取組は、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信頼も向上し、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、企業や産業界側においても、ガバメントアクセスに関する透明性の確保に向けた具体的な取組(捜査機関からの情報開示要請への対応方針や対応状況の開示等)についての議論が更に深まり、その実践も増えていくことが期待される(後記**第 7.**)。

第3. 米国及びEUの動向

1. 米国CLOUD Act

(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)やリモートコンピューティングサービス(remote computing services)のプロバイダが保持し、保管し、又は支配するデータに対する米国の政府機関によ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 を利用せず、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、米国の政府機関が、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

---

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、米国内でサービスを提供する事業者も、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)。

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り、法定された考慮要素に基づくコミティ分析によって修正又は取消しをすべきかどうかが判断されることになった[7]。加えて、上記①及び②を満たさない場合であっても、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命令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 Wiretap Act 等の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を採用していることなどが、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

---

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).

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。

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、他国に保存されたデータの捜査を目的とした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た。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、英国と 2019 年 10 月 3 日には行政協定を締結し、2022 年 10 月 3 日には発効に至ったほか、オーストラリアとも 2021 年 12 月 15 日に行政協定を締結した。また、米国は、カナダとも 2022 年 3 月から行政協定の締結に向けた交渉を開始しており、EU とも 2019 年 9 月から電子証拠の収集を巡る取決めの締結に向けた交渉を進めている[16]。なお、米国政府は、米英行政協定の締結にあたり、米国司法省刑事局国際室(Office of International Affairs)[17]に、当該協定による命令を精査等する「CLOUD チーム」を設置した[18]。

2. EU 電子証拠規則案及び指令案の概要

(1) 制定の背景

EU では、警察及び司法当局が、犯罪者やテロリストを調査、起訴し、有罪判決を下すために必要なクラウド上にある電子メールや文書などの電子証拠をより簡易かつ迅速に入手できるようにするため、2018 年 4 月 17 日、欧州委員会より、電子証拠規則案及び指令案の提案がなされた[19]。電子証拠規則案及び指令案はいずれも通常立法手続の下で審議されて

---

14 ACLU, *The Cloud Act Is a Dangerous Piece of Legislation* (Mar. 2018), *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 CLOUD Act に基づく動向は米国司法省のウェブサイトにまとめられている(https://www.justice.gov/criminal-oia/cloud-act-resources)。また、各国独自の背景・法制を踏まえながら、行政協定の締結を巡る国内法への影響などを分析する国が複数現れている(例えばスイス連邦司法省によるレポート(2021 年 9 月 17 日)(https://www.bj.admin.ch/bj/de/home/publiservice/publikationen/berichte-gutachten/2021-09-17.html)や、ニュージーランド法務省の 2012 年情報活動法レビューレポート(2017 年 6 月 27 日)(https://www.lawcom.govt.nz/sites/default/files/projectAvailableFormats/NZLC-R141-Review-of-the-Search-and-Surveillance-Act-2012-final_0.pdf)14.158-14.159 参照)。

17 米国司法省刑事局国際室は、外国に所在する米国人等に対する一定のサピーナについての事前審査等を担当している(米国司法省「CRIMINAL RESOURCE MANUAL」279)。

18 U.S. Department of Justice, *Landmark U.S.-UK Data Access Agreement Enters into Force* (3 Oct. 2022), *available at* https://www.justice.gov/opa/pr/landmark-us-uk-data-access-agreement-enters-force.

19 European Commission, *Security Union: Commission facilitates access to electronic evidence* (Apr. 17, 2018), *available at* https://ec.europa.eu/commission/presscorner/detail/en/IP_18_3343.

おり、2023 年 1 月 20 日、欧州理事会及び欧州議会が合意して修正された電子証拠規則案[20]及び指令案[21]の内容が公表された。以下では、欧州理事会及び欧州議会が合意して修正された電子証拠規則案及び指令案を参照し、説明する。

ネットワークベースのサービスの発展により、犯罪に関連する電子証拠が捜査対象国の外に保管され、又は捜査対象国以外の国に所在するサービスプロバイダによって保管されることが増え、実際に、多数のサービスプロバイダを抱える国に対して司法協力要請が行われることも頻繁に行われている上、要請の件数も増加している。その結果、他国に司法協力を求める方法で電子証拠を取得しようとすると時間がかかる。このような背景から、各加盟国は、自国内の様々な手続等を活用し、サービスプロバイダに任意の直接協力を求めるようになっている。このような傾向は、法的要請に応えようとする法執行機関、司法当局及びサービスプロバイダを、法的不安定性及び潜在的な法の抵触に直面させ得るもので、電子証拠の取得に係る法的枠組みの断片化と評することができる。そのため、電子証拠の提出及び保全に向けた国境を越える司法協力に関して、当該制度の適用範囲に含まれるサービスプロバイダが他の加盟国の当局から発せられる要請に直接応じる義務を含め、電子証拠の特性に応じた一定のルールを定める必要性が生じていた。

そこで、基本的権利の完全な遵守を確保しつつ、既存の EU 法を補完し、電子証拠の分野における法執行機関、司法当局及びサービスプロバイダに適用されるルールを明確化するために、電子証拠規則案及び指令案の提案がなされるに至った[22]。

(2) 電子証拠規則案及び指令案の概要

電子証拠規則案及び指令案が持つ主な意義としては、次の 3 つが挙げられる。

第一に、電子証拠規則案は、EU 域内に対してサービスを提供するサービスプロバイダに対して適用される[23]。電子証拠指令案によって、EU 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、執行管轄権行使の実効性を確保している。

---

20 Council of the European Union, *Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings - Analysis of the final compromise text* (Jan. 20, 2023), *available at* https://data.consilium.europa.eu/doc/document/ST-5448-2023-INIT/EN/pdf.

21 Council of the European Union, *Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings - Analysis of the final compromise text* (Jan. 20, 2023), *available at* https://data.consilium.europa.eu/doc/document/ST-5449-2023-INIT/EN/pdf.

22 電子証拠規則案前文(7)乃至(9)、電子証拠指令案前文(1)乃至(7)。

23 電子証拠規則案 3 条 1 項。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。)等の他の EU 法でも、域内に対するサービス提供を連結の有無の判断要素とする例がある(GDPR 3 条 2 項(a)参照)。

具体的には、電子証拠規則案が定める提出命令及び保全命令は、電子証拠規則案等に拘束される加盟国の司法当局により、EU 域内でサービスを提供するサービスプロバイダによって指定された電子証拠規則案等に拘束される他の加盟国に所在する拠点又は代理人に対して発せられる決定である[24]。「EU 域内でサービスを提供」するという要件を定めることで、当該加盟国と一定の事実上の基準に基づく実質的な関係(substantial connection based on specific factual criteria to the Member State(s))がある[25]サービスプロバイダが対象となるよう制限を加えている。

そして、電子証拠指令案は、EU 域内でサービスを提供する法人格を有するサービスプロバイダが電子証拠規則案等に拘束される加盟国で設立されている場合、当該加盟国に対して、当該サービスプロバイダに、決定及び命令の受領、遵守及び執行に責任を有するものとして、拠点(entity)を指定させるように求める。また、EU 域内でサービスを提供する法人格を有するサービスプロバイダが EU 域内で設立されていない場合であっても、電子証拠規則案等に拘束される加盟国は、自国内でサービスを提供する当該サービスプロバイダに、決定及び命令の受領、遵守及び執行に責任を有するものとして、代理人(法人又は自然人)を指定させるよう求められる[26]。指定される拠点又は代理人は、サービスプロバイダがサービスを提供する加盟国(電子証拠規則案等に拘束される加盟国)に所在し、執行手続の対象になり得る必要がある[27]。このように、EU 域内でサービスを提供するサービスプロバイダは、電子証拠指令案によって、当該サービスプロバイダがサービスを提供する電子証拠規則案等に拘束される加盟国で拠点又は代理人を指定するよう求められることになるため、EU 域内に拠点を有していない場合であっても提出命令又は保全命令を執行することができるような仕組みになっている。

第二に、保全命令と提出命令とでは後者の方が権利侵害の程度が大きいところ、保全命令は全ての刑事犯罪及び 4 か月以上の拘禁刑又は収容命令の執行を対象とするのに対し、提出命令は、被疑者又は被告人の権利を考慮し、一定の刑事手続のために必要かつ相当と言える対象に限定されている[28]。また、データの種類によっても取扱いは異なり、提出命令の対象となるトラフィックデータ(利用者を特定することのみを目的として要求されるデータを除く。)又はコンテンツデータが、サービスプロバイダの所在する加盟国の法律に基づいて免責及び特権によって保護されている場合又は当該加盟国における報道の自由及び他のメディアの表現の自由に関する刑事責任の決定及び制限に関する規則によって保護

---

24 電子証拠規則案 2 条 1 号、2 号。

25 電子証拠規則案 2 条 4 号(電子証拠指令案 2 条 3 号も参照)。

26 さらに、電子証拠規則案等に拘束されない加盟国に設立された EU 域内でサービスを提供するサービスプロバイダについては、電子証拠規則案等に参加している加盟国が、自国内でサービスを提供する当該サービスプロバイダに、決定及び命令の受領、遵守及び執行に責任を有するものとして、代理人(法人又は自然人)を指定させるよう求められる。

27 電子証拠指令案 3 条 1 項、2 項。

28 電子証拠規則案前文(30)、(31)。

されている場合には、発令機関[29]は、提出命令を発令することができない[30]。

「電子証拠」は、加入者データ、トラフィックデータ及びコンテンツデータで構成される[31]ところ、具体的には、以下のとおりデータの種類に応じて提出命令の適用対象が異なる。

---

29 加入者データ及び利用者を特定することのみを目的として要求されるデータの提出命令については、裁判官、裁判所、捜査裁判官、検察官、その他国内法に基づき特定の場合において刑事捜査当局として行動する機関が発令することができる一方、トラフィックデータ(利用者を特定することのみを目的として要求されるデータを除く。)及びコンテンツデータの提出命令については、検察官が発令機関から除かれている(電子証拠規則案 4 条 1 項、2 項)。なお、保全命令については、データの種類を問わず、検察官も発令することができる(電子証拠規則案 4 条 3 項)。

30 電子証拠規則案 5 条 7 項。

31 電子証拠規則案 2 条 6 号。

データの種類	データの内容	提出命令の適用対象
利用者を特定することのみを目的として要求されるデータ	特定の犯罪捜査において利用者を特定することのみを目的として法執行機関から要請された場合、IP アドレス、必要に応じて関連するソースポート及びタイムスタンプ(日時)又は当該識別情報と技術的に同等のもの及び関連情報 [32]	・ 全ての刑事犯罪 ・ 4 か月以上の拘禁刑又は収容命令の執行 [33]
加入者データ	サービスの利用申込に関してサービスプロバイダに保有される、(a)氏名、生年月日、郵便若しくは地理的住所、請求及び支払に係るデータ、電話番号又はメールアドレスなど加入者又は利用者を識別するデータ、並びに、(b)(i)最初の登録又は起動時点で、加入者若しくは利用者が使用した、又は加入者若しくは利用者に提供された技術データ及び関連技術手段又はインターフェースを特定するデータ並びに(ii)サービス利用の検証に関連するデータを含む、サービスの種類及びその提供期間に関するデータ(ただし、パスワード又は利用者が提供し、若しくは利用者の要請により作成されたパスワードの代わりに使用されるその他の認証手段を除く。)[34]	
トラフィックデータ(利用者を特定することのみを目的として要求されるデータを除く。)	(a)メッセージ又は他の種類の交信の送信元及び送信先、端末機器の位置、日付、時刻、期間、容量、経路、形式、使用されたプロトコル及び圧縮の種類等のサービスプロバイダによって提供されるサービスの提供に関するデータで、当該サービスに関する状況又は追加情報を提供するのに役立ち、サービスプロバイダの情報システムによって生成又は処理されるデータ(電子通信メタデータを含む。)、並びに、(b)利用日時、サービスへのログイン・ログオフ等、サービスに対する利用者のアクセスセッションの開始及び終了に関するデータ(ただし、加入者データは、トラフィックデータから除かれる。)[35]。	・ 発令国において長期 3 年以上の拘禁刑により処罰される刑事犯罪 ・ 情報システムによって全部又は一部が実行された場合における、キャッシュレス決済に関する犯罪、児童への性的虐待に関する犯罪及び情報システムに関する犯罪 ・ テロ犯罪 ・ 上記犯罪に対する 4 か月以上の拘禁刑又は収容命令の執行 [36]
コンテンツデータ	テキスト、音声、動画、画像、音等のデジタル形式のデータのうち、加入者データ又はトラフィックデータ以外のもの [37]	

このような適用対象の相違は、加入者データ及び利用者を特定することのみを目的として要求されるデータよりも、トラフィックデータ(利用者を特定することのみを目的として要求されるデータを除く。)及びコンテンツデータの証拠としての価値は高いものの、機微性が高いデータであり、命令による侵害の程度も大きいことから、より厳格な基準を設け

32 電子証拠規則案 2 条 8 号。

33 電子証拠規則案 5 条 3 項。

34 電子証拠規則案 2 条 7 号。

35 電子証拠規則案 2 条 9 号。

36 電子証拠規則案 5 条 4 項。

37 電子証拠規則案 2 条 10 号。

る意図に基づくものである。長期 3 年以上の拘禁刑という閾値は、(加盟国間での刑罰のバランスも踏まえた)犯罪捜査の効率性と権利保護及び比例原則とのバランスを確保する観点から選択された [38]。提出命令には一定の拒否事由が認められており、提出命令の名宛人やサービスプロバイダ、さらにはデータ主体の権利保護を担保していると言える。拒否事由には、具体的かつ客観的な証拠に基づき、提出命令の執行が EU 基本条約 6 条及び EU 基本権憲章に規定された基本的権利の明らかな侵害を生じさせると信じるに足りる相当な証拠が存在する場合、提出命令の執行が一事不再理(*ne bis in idem*)の原則に反する場合などが含まれている [39]。

第三に、発令機関は、データ主体に対し、不当に遅滞することなく、データの提出について通知することが求められており [40]、透明性を確保する仕組みが組み込まれている [41]。当該通知がなされる場合、提出命令に対する救済を求める各国法上の適用可能性についての情報も適時に提供し、救済が効果的に行使され得る状況が確保される必要がある [42]。もっとも、提出命令又は保全命令の発令機関は、公的若しくは法的な捜査、手続等の妨害防止、犯罪の発見、捜査、訴追等若しくは刑事罰の執行の妨害防止、他者の権利及び自由の保護などの観点から、データ主体への通知を遅滞、制限又は省略することができる [43]。

＝＝

コラム①：OECD におけるガバメントアクセスに関する議論

本報告書が検討の対象とする問題状況に関連する国際的枠組みとして、民間が保有する個人データに対する政府によるアクセスといういわゆる「ガバメントアクセス」の規律に関する議論が、経済協力開発機構(OECD)等の国際フォーラムにおいて進められている。

かかる議論の背景には、そのようなガバメントアクセスは、犯罪等の防止による国民の

---

38 電子証拠規則案前文(31)。

39 電子証拠規則案 10a 条 1 項、前文(42a)乃至(42f)。

40 電子証拠規則案 11 条 1 項。

41 類似の仕組みは、2022 年 11 月 16 日から施行が開始された EU のデジタルサービス法にも見られる。すなわち、仲介サービス提供者が、司法機関又は行政機関から当該サービスの受領者に関する情報提供命令を受領した場合、当該受領者に対して、遅くとも当該命令が履行される時点等までに、当該命令の理由や是正措置に関する情報を含む情報を提供する義務を負う(10 条 5 項)。

42 電子証拠規則案 11 条 1 項、4 項、17 条 3 項。

43 電子証拠規則案 11 条 2 項。犯罪の予防、捜査、検挙、訴追又は刑事罰の執行を目的とする権限のある機関による個人データの処理に係る個人の保護及び当該データの自由な移動に関する 2016 年 4 月 27 日付欧州議会及び理事会指令(*Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA available at* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016L0680-20160504)13 条 3 項。

安全の確保や国家安全保障のために必要性が認められる一方で、それが民主的価値や法の支配に矛盾し、無制限、不合理、恣意的又は比例性を欠く場合には、プライバシー等の人権を侵害し、またデータの流通の障害となって世界経済に悪影響を与えることになるとの問題意識がある[44]。

2022 年 12 月 14 日、OECD のデジタル経済政策委員会の閣僚会合において、民間部門が保有する個人データに対するガバメントアクセスに関する宣言(Declaration on Government Access to Personal Data Held by Private Sector Entities：以下「**OECD ガバメントアクセス宣言**」という。)[45]が採択され、ガバメントアクセスに関する 7 つの原則が示された。

かかる宣言は、その適用対象となる「ガバメントアクセス」を、各国政府が、各国の法的枠組みに従って各国領域内で法執行及び国家安全保障の目的を追求しようとする場合に、民間部門が保有又は管理する個人データにアクセス及び処理することであると定義した上で、その中には、各国政府が、民間部門又はデータが自国の領域内に存在しない場合に、当該民間部門に対してデータ提供を義務付ける権限を各国法の下で有する場合も含むとしている。このように、OECD ガバメントアクセス宣言は、捜査目的での越境的なデータの取得という本報告書が重点を置く問題状況の規律もその射程に含むものであることを明示しており、着目に値する。

同宣言が示したガバメントアクセスに関する 7 原則とその概要は以下のとおりである。

---

44 後記 OECD ガバメントアクセス宣言参照。

45 OECD, *OECD/LEGAL/0487*, (Dec. 14, 2022), *available at* https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0487#translations.

OECD ガバメントアクセス宣言における 7 原則

1. 法的根拠 (Legal basis)
ガバメントアクセスは各国の法的枠組みに根拠づけられ、規制される。かかる法的枠組みは、政府を拘束し、法の支配の下にある民主的に設立された機関によって運用され、濫用のリスクから個人を十分に保護するために目的、条件、制限及びセーフガードを定める。

2. 正当な目的 (Legitimate aims)
ガバメントアクセスは特定された正当な目的のためにのみ行われ、当該目的に照らして過剰な態様とならない。ガバメントアクセスは、批判を抑圧したり、民族、ジェンダー等の特性のみに基づいて個人に不利益を与えたりする目的で行われない。

3. 承認 (Approvals)
ガバメントアクセスが基準、規則及び手続に従って実施されることを確保するために事前承認要件が定められる。これらは、アクセスの結果として生じるプライバシー等の人権への干渉の程度に見合ったものであり、より深刻な干渉についてはより厳格な承認要件が設けられる。

4. データの取扱い (Data handling)
取得された個人データの処理は権限を付与された者のみが行い、かかる処理は、プライバシー、セキュリティー、秘密性及び完全性を維持するための措置の実施を含む要件に従う。データの喪失や不正アクセスを防止するための内部統制が実施される。

5. 透明性 (Transparency)
ガバメントアクセスに関する一般的な法的枠組みが明確で容易にアクセスできる。政府による法的要件の遵守に関して監督機関が行う公開の報告や、政府の記録へのアクセスを要求するための手続を含むガバメントアクセスに関する透明性を提供するメカニズムが存在する。

6. 監督 (Oversight)
ガバメントアクセスの法適合性を確保するための効果的で公平な監督のメカニズムがある。監督システムは、関連する情報の入手、調査の実施、法的枠組みの違反への対処等の権限を持つ組織の活動を含む。

7. 救済 (Redress)
国家安全保障と法執行活動の機密保持の必要性を考慮しつつ(これには、自分のデータに対するアクセスの有無等の個人への通知の制限が含まれ得る。)、法的枠組みに対する違反を特定し、是正するための効果的な司法的・非司法的救済を個人に対して提供する。

このように、OECD ガバメントアクセス宣言は、ガバメントアクセスについての包括的な原則を示すものとなっている。かかる宣言は、それが米国、EU 各国及び日本を含む OECD 加盟国により遵守されるものであることにも鑑みれば、今後、民間部門が国内外に保有する個人データを政府が捜査目的で取得しようとする行為も含め、ガバメントアクセスに関する具体的な国内的・国際的なルールが検討される上での基礎を提供するものといえる(一例として、後記**第 6.** で議論するような外国政府との間での行政協定の締結を検討する際に参照することも考えられるように思われる。)。

また、日本を含め、OECD ガバメントアクセス宣言を遵守することになる国においては、前記データの捜査目的での取得を規律する既存の法制度(例えば、日本の刑事訴訟法の規律)について、当該宣言との整合性を具体的に検討し、不整合ないし不十分な部分があれば早急にこれを手当てすることが求められると考えられる。

＝＝

＝＝

コラム②：インターネットと管轄政策ネットワーク(I&JPN)の取組

インターネットと管轄政策ネットワーク(Internet & Jurisdiction Policy Network。以下「I&JPN」という。)は、2012 年にフランス・パリで設立された非営利団体であり、主に国境を越えたインターネットと国家管轄権に関する問題に対処すべく、法的な相互運用性を高め、サイバー空間における国家管轄相互の緊張を緩和するための取組を行っている。具体的には、①データと管轄、②コンテンツと管轄及び③ドメインと管轄という 3 つの問題についてのプログラムを立ち上げ、それぞれについて、マルチステークホルダーから成るコンタクトグループにおける検討や、各種の提言等を行っている。

2021 年 3 月に、I&JPN は、上記①から③のプログラムによる取組の成果物として、各課題についての政策的なフレームワークや対処に向けた手段を示す「ツールキット(Toolkit)」シリーズを公表した[46]。このうち、データと管轄のコンタクトグループにおける検討の成果である「電子証拠に対する越境的なアクセス」のツールキット[47]は、電子証拠に対する越境的なアクセスについて構築されるべき制度の主要な構成要素(core components)及びそれぞれの構成要素に係る基準(regime standard)を提示している。

＝＝

46 Internet & Jurisdiction Policy network, *News: Download the I&JPN Toolkits* (March 2021) *available at* https://www.internetjurisdiction.net/news/toolkits.

47 Internet & Jurisdiction Policy network, *Toolkit: Cross-Border Access to Electronic Evidence* (March 2021), *available at* https://www.internetjurisdiction.net/uploads/pdfs/Internet-Jurisdiction-Policy-Network-21-103-Toolkit-Cross-border-Access-to-Electronic-Evidence-2021.pdf.

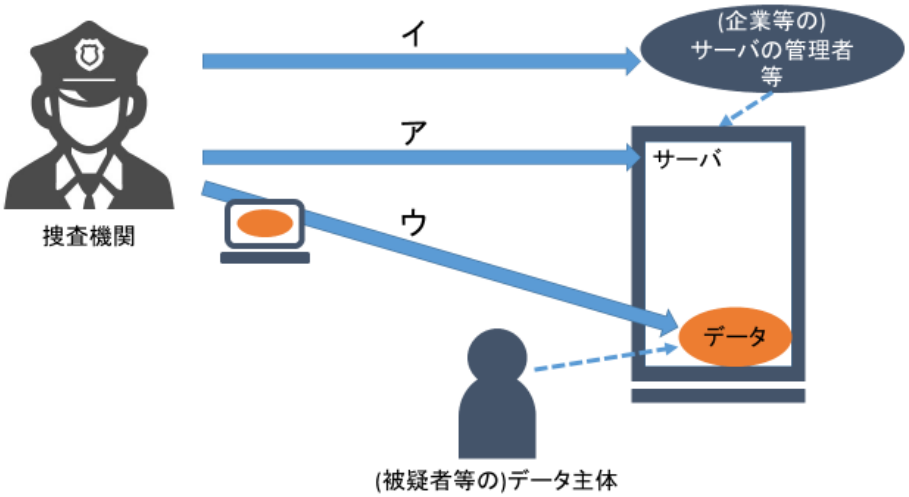
第4. 企業が保有するデータの取得及び利用に関する日本の法令上の検討課題

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[48]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[49]。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 3 つの方法に整理することができる(**図**参照)。



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

---

48 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。

49 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.)。

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、当該サーバ自体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を利用することができる(同法 218 条 1 項、99 条の 2)。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[50]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。もっとも、記録命令付差押えには、次のような欠点もある。まず、記録命令付差押えを行うために、捜査機関は、被処分者であるサーバの管理者等の所在地まで赴き、令状を呈示した上で、記録媒体にデータを記録させ、当該記録媒体を物理的に差し押さえる必要がある。また、記録命令付差押えは令状に基づく強制処分ではあるものの、その実効性を確保するための強制手段が法定されておらず、被処分者たるサーバの管理者等が任意に協力しない場合には、データを取得することができない。

そのような中、2022 年 3 月、法務省に設置された刑事手続における情報通信技術の活用に関する検討会は、取りまとめ報告書を公表し、捜査機関が、犯罪の捜査をするために必要があるときは、裁判官の発する令状により、データを保管する者に対し、必要なデータをオンラインで提供させること(記録命令付差押えの「差押え」の部分を除いて「記録命令」の

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

部分に限ること。)をできるようにする制度を提言した[51]。これを受け、2022 年 7 月に法務省の法制審議会に設置された刑事法(情報通信技術関係)部会では、当該制度(以下「**電磁的記録提供命令**」という。)の創設に向けた検討が行われている[52]。

一方、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データの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(以下、このような捜査手法を一般的に「**リモートアクセス**」と呼ぶ。)。

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)からデータを当該電子計算機又は他の記録媒体に複写し、当該電子計算機又は当該他の記録媒体を差押える方法が存在する(同法 99 条 2 項、218 条 2 項。以下、これらの規定に基づくリモートアクセスを「**刑訴法上のリモートアクセス**」という。)。ただし、刑訴法上の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ければ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、更に以下の手法が提案されている。まず、一度クライアント端末を差し押さえた後に、改めて刑訴法上の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[53]。

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)。このような捜査手法については、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

51　刑事手続における情報通信技術の活用に関する検討会「『刑事手続における情報通信技術の活用に関する検討会』取りまとめ報告書」13 頁(2022 年 3 月)(https://www.moj.go.jp/content/001368581.pdf)。

52　法制審議会刑事法(情報通信技術関係)部会・第 7 回会議配布資料 11「検討のためのたたき台(諮問事項「一」関係)」(https://www.moj.go.jp/content/001389630.pdf)の第 1-3 1(2)参照。

53　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)。

モートアクセスは認められないのではないかといった検討課題があり得るが、学説上はこの捜査手法を肯定する見解がある[54]。

さらに、データが保存されたサーバにアクセスする権限を有する者から有効な任意の承諾を得て、任意捜査としてリモートアクセスを行うという方法も行われている(令和 3 年最高裁決定参照。)[55]。

(2) 捜査機関と企業との連携

前記(1)のとおり、企業が保有するデータに対する捜査目的による現行法上の取得手法には、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[56]。

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である記録命令付差押えには基本

54　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』114-115 頁(立花書房、2019)。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(以下「**平成 29 年 GPS 最高裁判決**」という。)も参照。

55　もっとも、現代人が保有するデータは膨大なものとなることがあり、高度なプライバシー情報も多数含まれていることから、当該データに係るプライバシーは住居内のプライバシーに匹敵する状況となっている。そうすると、アクセス権限を有する者の任意の承諾を得てリモートアクセスを行うことは、居住者の任意の承諾を得て住居の捜索を行うことに等しいと言い得るところ、憲法 35 条は「住居」に準ずる私的領域に「侵入」されることのない権利を保障していること(平成 29 年 GPS 最高裁判決参照)、そして居住者の任意の承諾を得た住居の捜索が犯罪捜査規範 108 条によって禁止されていることに照らせば、任意捜査としてリモートアクセスを実施する場合にも、プライバシーへの配慮は慎重に確保される必要がある。
また、被処分者のプライバシーに配慮しながら任意捜査としてのリモートアクセスを実施しようとしても、なおその承諾の任意性が否定されることはあり得ることに鑑みれば(令和 3 年最高裁決定の原判決である大阪高判平成 30 年 9 月 11 日刑集 75 巻 2 号 220 頁等参照。)、任意捜査であれば当然に捜査の安定性が確保されるというわけではない可能性がある。
これらの点を踏まえれば、リモートアクセスとの関係で、任意捜査以外のより適切な捜査手法の設計に向けた検討は引き続き求められていると言い得るように思われる(なお、データが国外のサーバに保存されている場合や、その可能性が否定できない場合において考慮すべき事項については、後記**第 5. の 1. (2)イ**参照。)。

56　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)も参照。

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・電磁的記録提供命令の更なる活用

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更に活用していくことが望まれる。

前記**(1) ウ**のとおり、刑訴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、捜査対象となるデータが、クライアント端末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削除されずに保存されている場合がある[57]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[58]。

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、捜査関係事項照会書ではなく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

57　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。

58　ただし、近年、国外に所在するサーバへのアクセスに関する国内外の議論が進展しており(後記**第 5. の 1. (2) イ**参照。)、記録命令付差押えのような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捜査手法とリモートアクセスのようなデータが保存されたサーバに捜査機関自らアクセスしてデータを取得する捜査手法を、状況に応じて適切に選択することが重要になる(後記**エ**参照。)。

ていくことが検討されるべきであろう[59] [60]。

さらに、前記**(1)イ**のとおり、現在、法制審議会では、捜査機関が、裁判官の発する令状により、データを保管する者に対し、必要なデータをオンラインで提供させるための電磁的記録提供命令の創設に向けた検討が行われており、今後、その活用も期待される。

ウ　記録命令付差押え・電磁的記録提供命令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[61]。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、企業側の対応が困難になり得るほか、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あらかじ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[62]。また、同様の問題は、現在法制化に向けた検討が進んでいる電磁的記録提供命令の場合にも妥当すると考えられる。

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、記録命令付差押え又は電磁的記録提供命令の対象となるデータの特定の在り方を模索していくことが期待される。

さらに、記録命令付差押えや電磁的記録提供命令の運用にあたっては、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。現在、法制審議会においては、令状の請求・発付・執行に関しても、電子化に向けた検討が行われている(後記**(3)ア**参照)が、こうした事項について検討するにあたっては、データを実際に提出することになる企業とも連携し、その在り方を模索していくことが重要であると考えられる。

59　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, 138 S. Ct. 2206, 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。

60　このような方向性は、ガバメントアクセスに関して事前承認や監督のメカニズムを設けるべきであるとする OECD ガバメントアクセス宣言(前記**コラム①**参照)とも整合する。

61　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。

62　このような問題があるため、捜査機関は捜査対象となるデータを保有する企業との間で、事前に協議を実施して令状請求を行っている。

エ　データが保存されたサーバに捜査機関自らアクセスしてデータを取得する捜査手法における留意点

前記**(1)ウ**のとおり、刑訴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いものであるとは言い難い。一方で、サーバに対する検証として行われる場合や任意捜査として行われる場合も含め、リモートアクセスそれ自体は、(i)捜査機関がサーバやサーバ管理者等の所在地に赴かずにデータを入手することを可能とするものであること[63]、(ii)エンドツーエンドの暗号化により、サーバ管理者等の事業者側では目的のデータを復号できないような場合にユーザーのクライアント端末を通じて復号されたデータを取得し得ること[64]、そして(iii)企業によるデータの任意での提出が期待できない場合にもデータを取得し得ること[65]等から、少なくとも現行刑事訴訟法の下においては、捜査機関にとって有用な捜査手法となっていることは否定し難い。

もっとも、リモートアクセスは、記録命令付差押えや電磁的記録提供命令のようなサーバ管理者等にデータの提出を求める捜査手法と異なり、サーバを管理する企業の与り知らないところで対象データを取得するものであることから、企業に対する手続保障の問題が生じ得る。そのため、企業との関係でも通知等の公正性担保の手段を講じることが望ましい(後記**(3)イ**参照)。

(3) 今後の制度設計に関する検討課題

企業が保有するデータの取得手法を巡る今後の検討課題としては、以下のようなものが考えられる。

ア　令状手続の電子化及びデータ提出のオンライン化

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図るためには、令状手続の電子化についての検討が重要になる。また、本研究会における国内外の企業への

63　仮に電磁的記録提供命令の制度が創設された場合、捜査機関はサーバ管理者等の所在地に赴かずにデータの提出を求めることができるため、このメリットは相対的に小さくなるものと思われる。

64　ただし、被処分者が被疑者である場合に、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は、自己負罪拒否特権(憲法 38 条 1 項)との関係で問題が生じる可能性がある(後記 **3. (1)** 参照)。

65　法制審議会では、電磁的記録提供命令について、処分者に対する間接強制等の実効性担保の方策を設けることが検討されている(法制審議会刑事法(情報通信技術関係)部会・第 7 回会議配布資料 11「検討のためのたたき台(諮問事項「一」関係)」(https://www.moj.go.jp/content/001389630.pdf)の第 1－3 2(4)参照)ため、電磁的記録提供命令の制度が創設された場合には、このメリットは相対的に小さくなる可能性がある。

ヒアリングによれば、データ提出についてもオンライン化が実現すれば、捜査機関に対してより協力しやすくなるとの意見が多かった。

この点、法制審議会・刑事法(情報通信技術関係)部会では、刑事手続における情報通信技術の活用に関する検討会の取りまとめ報告書における提言[66]を踏まえ、令状手続の電子化に向けた検討が行われている[67]。また、電磁的記録提供命令の制度が創設されれば、遠隔地に所在する事業者が、オンラインで呈示された令状に対して、遠隔地からオンラインでデータを提出することができるようになる。

令状手続の電子化及びデータ提出のオンライン化を実現するためには、オンラインでの令状の呈示やデータ提出におけるセキュリティ確保をいかにして図るかが課題となる[68]。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「コンプライアンス WAN」[69]を構築している例が参考になる。また、一部の企業は、自ら法執行機関とのコミュニケーションのため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、公開されたオープンな環境ではなくクローズドな環境を構築することでセキュリティを確保している[70]。

さらに、電磁的記録提供命令の制度が創設されることにより、遠隔地に所在する事業者に対してオンラインで令状を呈示し、オンラインでデータの提出を受けることができるようになった場合、これまでは物理的に不可能であった日本国外に所在する事業者に対するデータの提出命令が技術的には可能となる。国際法上、他国に所在するサーバ管理者に対して管轄権を行使し得るかについては慎重な検討を要する(後記**第 5. の 1. (2) ア**参照)が、将来的に、他の締約国に所在する者との直接協力について規定したサイバー犯罪条約第二追加議定書(後記**第 5. の 2. (2) ウ**参照)が批准されたり、CLOUD Act に基づく行政協定のような二国間での枠組みが構築されたりすることで(後記**第 6. の 1.** 参照)、管轄権の行使が許

---

66 刑事手続における情報通信技術の活用に関する検討会「『刑事手続における情報通信技術の活用に関する検討会』取りまとめ報告書」9-12 頁(2022 年 3 月)(https://www.moj.go.jp/content/001368581.pdf)。

67 法制審議会刑事法(情報通信技術関係)部会・第 7 回会議配布資料 11「検討のためのたたき台(諮問事項「一」関係)」(https://www.moj.go.jp/content/001389630.pdf)の第 1-2 参照。

68 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/bureau/cyber/pdf/h27_honpen.pdf)参照。

69 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 26 日)(https://www.fsa.go.jp/sesc/news/c_2009/2009/20090126.html)。

70 諸外国における例として、例えば、米国では、通信業者が用意した安全なポータルサイトを介したデータの押収が一般的に行われている。また、フランスでは、「国際司法傍受プラットフォーム」を介したデータの請求及び取得が行われている(刑事手続における情報通信技術の活用に関する検討会・第 9 回会議資料 33「諸外国における情報通信技術の活用に関する法制・運用の概要【暫定版・更新版】」(https://www.moj.go.jp/keiji1/keiji07_00022.html)参照)。さらに、スイスにおいても、法執行機関とプロバイダ間でデータをやり取りするプラットフォーム(Post and Telecommunications Surveillance Service)(https://opendata.swiss/en/organization/dienst-ueberwachung-post-und-fernmeldeverkehr-uepf)が存在し、スイスの法執行機関はプロバイダに対して手数料を支払ってこれを利用している。

容される範囲が拡大し得ると考えられる。そのため、今後、日本国外に所在する事業者に対して電磁的記録提供命令を行うために必要な立法・制度整備についても検討が必要になると考えられる[71]。

イ　通知等の手続の公正性担保の手段

日本の刑事訴訟法は、令状を用いた捜査手続の公正性担保を図る仕組みとして、被処分者に対する令状の呈示を義務付けている(同法 222 条 1 項、110 条)。もっとも、企業が保有するデータの捜査を目的とする取得においては、少なくとも、(被疑者等の)データ主体と(企業等の)サーバの管理者等が利害関係者として存在しており(前記**(1)**の図参照)、単純に被処分者との関係で手続の公正性を担保するだけでは不十分な可能性がある。そこで以下では、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捜査手法の場合と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のそれぞれについて、手続の公正性担保にあたって考慮すべき事項を整理する。

(ア) 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捜査手法の場合

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場面では、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。そこで、被処分者(サーバの管理者等)に対する令状呈示のみならず、データ主体の利益にも配慮した手続の公正性を担保するための手段について、検討する必要がある。

捜査機関のサーバ管理者等に対するデータ提出要求については、サーバ管理者等が、当該要請の有効性の精査等によって、サーバ管理者等自身の利益だけでなく、データ主体の利益も踏まえて、適切に対処する役割を果たし得る。しかし、データ主体自身が、当該データ提出の求めがあったこと、又はその求めに応じてデータ提出が行われたことを認知していなければ、データ主体自身は、異議を述べ、被った権利利益に対する侵害に対する救済を受ける機会を逸することになる。したがって、データ主体の権利利益を保護する観点からは、データ主体に対して適時かつ適切な情報提供が行われる仕組みが重要な検討課題となる。例えば、EU の電子証拠規則案(前記**第 3. の 2. (2)**参照)は、証拠の提出又は保全に係る発令機関が、提出対象となるデータの主体に対し、そのデータ提出について、不当に遅滞することなく通知することを法的に義務付けている[72]。また、I&JPN が公表した「電

71　関連して、日本国外に所在する事業者が日本の法令に基づき日本国内に設置・指定する代表者や代理人を通じて、当該事業者に対して電磁的記録提供命令を行うことの可否についても論点になり得る(後記**第 5. の 1. (2)ア**参照)。

72　電子証拠規則案 11 条 1 項。また、同規則案は、発令機関がデータ主体に対し通知を行う場合において、当該データ主体が、後記の加盟国の国内法に基づく救済を求めることのできるという情報が適時に提供される必要があり、この情報は、当該救済が実効的に行使されることを確保するものでなければならないとも定めている(電子証拠規則案 17 条 3 項)。

子証拠に対する越境的なアクセス」のツールキット(前記**コラム②**参照)も、デフォルトルールとして、データの提出に係る要求又は命令を発出する国に対し、データ主体(user)に対する通知の法的義務を課すべきであるとする[73]。

一方で、捜査の過程でデータ主体に対してデータの提出に関する通知を行うと、特にデータ主体が被疑者やその関係者である場合、捜査の密行性又は実効性が損なわれる可能性がある[74]。この点に配慮して、例えば、EU の電子証拠規則案は、発令機関が、捜査に対する支障の回避、国家安全保障の確保等の目的のために必要かつ相当な限度で、データの提出に関する通知を遅らせ、制限し、又は省略することができるとも定めている[75]。I&JPN の「電子証拠に対する越境的なアクセス」のツールキットも、情報の開示により実施中の捜査が徒労に終わる危険がある場合には、一定の期間において、データ主体への通知を遅らせ、又はデータの提出に係る要求又は命令を秘匿する[76]ことがあり得ると述べる[77]。また、OECD ガバメントアクセス宣言(前記**コラム①**参照)も、透明性や救済の確保の観点から個人の情報提供を受ける利益の重要性を指摘する一方で、国家安全保障及び法執行活動の機密保持の必要性とのバランスも図られなければいけないとしている。

このような他の国・地域や国際フォーラムでの議論を踏まえると、日本国内でも、今後、データ主体の権利利益に配慮した手続の公正性を担保する措置として、データ主体に対して、どのようなタイミングで、どのような内容の通知を行うのかという点や、実際にデータの提出命令を受け取るサーバ管理者等に対して、どのような対応を求めるべきかと

---

73 Internet & Jurisdiction Policy network, *Toolkit: Cross-Border Access to Electronic Evidence* (March 2021), *available at* https://www.internetjurisdiction.net/uploads/pdfs/Internet-Jurisdiction-Policy-Network-21-103-Toolkit-Cross-border-Access-to-Electronic-Evidence-2021.pdf, p.19.

74 この問題に対処した国内での先例として、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。

75 電子証拠規則案 11 条 2 項、犯罪の予防、捜査、検挙、訴追又は刑事罰の執行を目的とする権限のある機関による個人データの処理に係る個人の保護及び当該データの自由な移動に関する 2016 年 4 月 27 日付欧州議会及び理事会指令(*Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA available at* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016L0680-20160504)13 条 3 項。

76 「電子証拠に対する越境的なアクセス」のツールキットは、データ取得にかかる要求又は命令を秘匿する方法については明記していないが、考えられる方法として、例えば、データ主体への通知内容を制限し、その目的や背景を明かさないといった方法が考えられる。

77 Internet & Jurisdiction Policy network, *Toolkit: Cross-Border Access to Electronic Evidence* (March 2021), *available at* https://www.internetjurisdiction.net/uploads/pdfs/Internet-Jurisdiction-Policy-Network-21-103-Toolkit-Cross-border-Access-to-Electronic-Evidence-2021.pdf, p.19 (前記**コラム②**参照).

いう点を念頭に、データ主体の権利利益の保護等に関する制度設計を検討していく必要があると考えられる。一方で、そのような制度の具体化を検討するに際しては、上記の他の国・地域や国際フォーラムでの議論も参照しながら、データ主体の権利利益の保護と捜査の実効性のバランスをいかに図るかについての具体的な検討が求められる[78]。その検討にあたっては、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。)において、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)が設けられているといった、関連する既存の国内法の仕組みも参照されるべきと考えられる[79]。

さらに、データの提出に関する異議申立ての機会を付与するための通知に加えて、そのような異議申立て及び救済の仕組みの検討も重要になると考えられる。このような仕組みの対象としては、実際にデータの提出命令を受け取るサーバ管理者等のほか[80]、データ主体自身も想定される。この点、前記の EU の電子証拠規則案及び I&JPN の「電子証拠に対する越境的なアクセス」のツールキットは、データ主体が異議を申し立て、救済を受けるための仕組みの必要性に触れ、また、救済の手段については、既存の法制度又は運用も活用

78 例えば、手続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(平成 29 年 GPS 最高裁判決参照)、企業が保有するデータの取得全てについて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ように思われる。

79 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)。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。

80 刑事訴訟法上、捜査機関による記録命令付差押えの処分に対しては、準抗告をすることができる(刑事訴訟法 430 条 1 項、2 項)ところ、法制審議会においては、電磁的記録提供命令による提供に関しても準抗告の対象とする方向で議論が進んでおり(法制審議会刑事法(情報通信技術関係)部会・第 7 回会議配布資料 11「検討のためのたたき台(諮問事項「一」関係)」(https://www.moj.go.jp/content/001389630.pdf)の第 1－3 1(3)参照)、サーバ管理者等がこうした準抗告をデータの提出後だけでなく、データの提出前に用いることも想定される。米国では、SCA 上、プロバイダは、開示を求められるデータがその性質上異常に多い場合又はプロバイダに対する過度な負担となる場合に、裁判所に対してデータ開示命令の修正又は取消しを申し立てることができる(18 U.S. Code § 2703(d))ほか、CLOUD Act によって、プロバイダが、データ主体が米国市民ではなく、当該命令が行政協定を締結した外国政府の法令に違反する場合における修正又は取消しの申立手続が設けられた(18 U.S. Code § 2703(h)。前記**第 3. の 1. (2)** 参照)。このように、他国においても、データの提出命令を受け取ったサーバ管理者等がデータの提出前に開示命令に対して異議を申し立てる手続が法定されている例が見当たる。

し得る旨の方向性を示している[81]。

(イ) 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

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、上記(ア)のデータ主体の利益への配慮や手続保障の問題[82]に加えて、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。

日本の捜査実務上、リモートアクセスは、刑事訴訟法 218 条 2 項に基づいて行われる場合(刑訴法上のリモートアクセス)、サーバに対する検証として行われる場合及び任意捜査として行われている場合とがある(前記 **1. (1) ウ**参照)ところ、いずれにおいてもサーバ管理者等に対する令状呈示や通知は行われていない。これに対して、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)、かかる処分は直接の被処分者だけでなくサーバの管理者等にも通知される[83]。

現行刑事訴訟法上、リモートアクセスは、差し押さえるべき端末やサーバといった「物」に対する捜査として実施されているが、中長期的には、電磁的記録提供命令のように、データの取得それ自体を目的としたリモートアクセスのための手続を新たに創設した上で、上記ドイツの法制も参考に、サーバ管理者等との関係でも手続保障に配慮する制度設計を行うことも検討課題になり得る。

---

81 EU の電子証拠規則案は、提出命令により自己のデータの提出を求められた全ての者(any persons whose data were sought via a European Production Order。European Production Order について、前記**第 3. の 2. (2)**参照。)が、提出命令に対して実効的な救済を受ける権利(right to effective remedies)を有するとした上で(17 条 1 項)、かかる権利が加盟国の国内法に基づき裁判所で行使されなければならないこと、及びかかる権利には、当該措置の必要性及び比例性の観点も含めてその適法性に異議を唱える可能性が含まれなければならないことを規定している(17 条 2 項)。また、同規則案は、救済の手続においては、国内における類似の事案で適用される期間やその他の条件が適用されなければならないと規定している(17 条 4 項)。
I&JPN の「電子証拠に対する越境的なアクセス」のツールキットも、データ主体が自己のデータの提出又は利用に関し異議を申し立てる有意義な機会を確保すべきとした上で、その手続は、政府がデータを利用しようとする場面に適用可能なあらゆる刑事手続、データ保護当局の運用又はその他利用可能な国内法及び民事上の救済手段を通じて提供され得ると述べている(Internet & Jurisdiction Policy network, *Toolkit: Cross-Border Access to Electronic Evidence* (March 2021), *available at* https://www.internetjurisdiction.net/uploads/pdfs/Internet-Jurisdiction-Policy-Network-21-103-Toolkit-Cross-border-Access-to-Electronic-Evidence-2021.pdf, p.19.)。

82 刑訴法上のリモートアクセスの場合は、当該端末の所持者に対してリモートアクセスを行うサーバ等の範囲を記載した令状(刑事訴訟法 219 条 2 項)を呈示した上でリモートアクセスを行う必要があるが、端末の所持者とリモートアクセスにより取得されるデータのデータ主体は(一致することが多いとは考えられるものの)必ずしも一致するわけではないため、データ主体の利益への配慮や手続保障の問題が生じ得る。また、サーバに対する検証としてリモートアクセスを行う場合には、端末の差押えという手順なしにリモートアクセスを行うことができるため、データ主体に対して令状を呈示することなく実施することも可能であり、運用次第で同様の問題が生じ得ると考えられる。

83 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)。

ウ　企業に対する秘密保持の義務付け制度の拡充

前記**イ**に関連して、捜査機関がサーバの管理者等[84]に対してデータの提出に係る要求又は命令を行った場合に、捜査手続の密行性又は実効性の確保の観点からは、サーバの管理者等の企業に対して当該要求又は命令に関する秘密保持を義務付けることの検討も必要になると考えられる。

この点に配慮した刑事訴訟法上の制度として、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)が既に存在する。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[85]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。

一方で、この問題に関して、EUの電子証拠規則案は、プロバイダが、欧州提出命令認定書(European Production Order Certificate: EPOC)若しくは欧州保全命令認定書(European Preservation Order Certificate: EPOC-PR)[86]又は提出若しくは保全されたデータの機密性、秘密性及び完全性を確保するために必要な、最先端の運営上及び技術上の措置を講じなければならない旨を規定する[87]。また、米国のSCA(前記**第3.の1.(1)**参照)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データ主体への通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[88]。

エ　捜査機関が取得したデータの利用、保存等に対する規律

データを取得する捜査手法の活用が進むと、捜査機関に大量のデータが蓄積されることになるため、捜査機関によるその利用、保存等に対する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、2008年に、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関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

84　ここでいう「サーバの管理者等」は、データ主体と同一の者でない限り、データ主体を含まない。

85　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)。

86　電子証拠の保全を命じる欧州保全命令(European Preservation Order。電子証拠規則案2条2号。)はEPOC-PRを通じて、電子証拠の提出を命じる欧州提出命令(European Production Order。電子証拠規則案2条1号。)はEPOCを通じて、それぞれ送信される(電子証拠規則案8条1項)。

87　電子証拠規則案11条3項。

88　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))。

違反すると判断し[89]、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。また、OECD ガバメントアクセス宣言(前記**コラム①**参照)は、政府によるアクセスを通じて取得された個人データについて、この取扱いがプライバシー、セキュリティー、秘密性及び完全性を維持するための措置の実施を含む法的要件の下で行われること、法的に許容された期間に限り保持されること等を定める法的枠組みや、不正なデータの使用、改変等を探知、防止等する内部統制システムの構築の必要性を示唆している[90]。

日本においては、捜査機関が保有するデータの利用、保存等に対しては個人情報保護法(旧行政機関個人情報保護法)による規律が一定程度及ぶほか[91]、被疑者写真の管理及び運用に関する規則や指掌紋取扱規則、DNA 型記録取扱規則といった国家公安委員会規則が、被疑者写真や指掌紋、DNA 型記録といった情報の管理及び運用に関する事項を定め、これらの情報を「保管する必要がなくなったとき」等にこれを抹消しなければならないと定めている[92]。捜査機関によるデータの利用、保存等は、こうした法律や規則による制約の下で行われている[93]。一方で、裁判例上、上記各規則が定める「保管する必要がなくなったとき」がどのような場合を指すかは明らかでなく、運用次第では、これらの規則に基づいて情報が抹消されるべき場合はほぼ存在し得なくなる可能性もあるとの指摘がなされたこともある[94]。

さらに、捜査機関に違法又は不適切にデータを利用、保存等されているデータ主体等に、どのような救済手段を提供するかという観点からの検討も求められ得る。この点、個人情報保護法は、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 76 条 1 項)、訂正請求権(同法 90 条 1 項)及び利用停止請求権(同法 98 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等には適用されない(同法 124 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)。他方で、名古屋地裁令和 4 年 1 月 18 日判決[95]は、無罪判決が確定した原告が、国に対して、人格権に基づく妨害排除請求として、捜査機関に取得された原告の指紋、DNA 型及び顔写真の各データ並びに原告所有の携帯電話のデータの

---

89 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)。

90 OECD, *OECD/LEGAL/0487*, (Dec. 14, 2022), Principle IV. (Data handling).

91 個人情報保護法第 5 章参照。

92 被疑者写真の管理及び運用に関する規則 5 条、指掌紋取扱規則 5 条 3 項、DNA 型記録取扱規則 7 条。

93 名古屋地判令 5 年 2 月 17 日 LEX/DB25594817 参照。

94 名古屋地判令 4 年 1 月 18 日判例時報 2522 号 62 頁、第 3 5(3)イ参照。ただし、「保管する必要がなくなったとき」について、一律のルールを規定するのは難しいとの指摘もなされ得るであろう。

95 解説として、國田武二郎・小山剛「刑事弁護レポート　名古屋地判令 4・1・18　平成 30 年(ワ)第 3020 号　LEX/DB25591643　国家賠償等請求事件　無罪確定した男性から採取した指紋、顔写真及び DNA 型データの抹消命令」『季刊刑事弁護』(通巻 113 号)100-104 頁等。

抹消を請求した事案において、指紋、DNA 型及び顔写真の各データに係る抹消請求を認容した。近時の国際的な議論に目を向ければ、OECD ガバメントアクセス宣言は、個人データの不適切なアクセス又は保持に対する救済手段に、かかるデータの削除や違法なデータの処理の停止が含まれ得ることを示している[96]。

こうした国内の動向や前記の国際的な議論を踏まえて、今後、捜査機関が取得したデータの利用、保存等に関する規律や、違法又は不適切なデータの利用、保存等に対するデータ主体等の救済の在り方について、更に議論が深まることが期待される[97]。このような制度設計にあたっては、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視点も有益であると考えられる[98]。

オ　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、例えば以下のような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

96　OECD, *OECD/LEGAL/0487*, (Dec. 14, 2022), Principle VII. (Redress).

97　法制審議会刑事法(情報通信技術関係)部会・第 7 回会議議事録(https://www.moj.go.jp/content/001394233.pdf) 27-29 頁、池田委員及び久保委員発言も参照。かかる規律の検討は、こうしたデータの利用、保存等に関す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重要性が認められる(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)参照)。

98　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)。

為(刑法 35 条、以下「**法令行為**」という。)等の違法性阻却事由が認められる場合[99]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[100]17 条 8 項及びその解説[101]3-7-3 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[102]。

現在、電磁的記録提供命令という新たな捜査手続の創設に向けた検討が進んでいるが、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、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。さらに、2023 年 6 月 16 日に施行予定である改正法(以下「**改正電気通信事業法**」といい、改正電気通信事業法に伴い改正された電気通信事業法

---

99 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)。

100 個人情報保護委員会・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(令和 4 年 3 月 31 日個人情報保護委員会・総務省告示第 4 号)」(2022 年 3 月)(https://www.soumu.go.jp/main_content/000805614.pdf)。

101 個人情報保護委員会・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(令和 4 年 3 月 31 日個人情報保護委員会・総務省告示第 4 号)の解説」(2022 年 3 月)(https://www.soumu.go.jp/main_content/000805807.pdf)。

102 個人情報保護委員会・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(令和 4 年 3 月 31 日個人情報保護委員会・総務省告示第 4 号)の解説」3-7-1(1)(2022 年 3 月)(https://www.soumu.go.jp/main_content/000805614.pdf)。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))。

施行規則を「**改正電気通信事業法施行規則**」という。)が [103]、「利用者の利益に及ぼす影響が大きい電気通信役務」[104]を提供する電気通信事業者を指定し(以下「**指定電気通信事業者**」という。)[105]、指定電気通信事業者による「特定利用者情報」[106]の適正な取扱いについて規定しており、捜査機関によるデータの取得に関する議論は、こうした新たな規律との関係も含めて整理する必要があると考えられる [107]。

(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(外国に所在する)第三者に提供することが禁止されている(同法 27 条 1 項、28 条)。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 [108]。

---

103 電気通信事業法の一部を改正する法律(令和 4 年法律第 70 号)(https://www.sangiin.go.jp/japanese/joho1/kousei/gian/208/pdf/s0802080482080.pdf)。

104 改正電気通信事業法施行規則 22 条の 2 の 20 参照(https://public-comment.e-gov.go.jp/servlet/PcmFileDownload?seqNo=0000246511)。要約すると、無料の電気通信役務の場合は利用者数が 1,000 万人以上である電気通信役務が、有料の電気通信役務の場合は利用者数が 500 万人以上である電気通信役務が、それぞれ「利用者の利益に及ぼす影響が大きい電気通信役務」に該当する。

105 改正電気通信事業法 27 条の 5 参照。

106 通信の秘密に該当する情報に加え、利用者を識別できる情報のうち、特定の利用者を識別することができる情報を電子計算機を用いて検索することができるように体系的に構成した情報の集合物等(データベース等)を構成する情報を構成する情報は、「特定利用者情報」に該当する(改正電気通信事業法 27 条の 5、改正電気通信事業法施行規則 22 条の 2 の 21)。
改正電気通信事業法における「利用者」には、電気通信事業者又は同法 164 条 1 項 3 号に掲げる電気通信事業を営む者との間に電気通信役務の提供を受ける契約を締結する者に加え、継続的に電気通信役務を利用するための識別符号を付与された者が含まれる(同法 2 条 7 号イ、改正電気通信事業法施行規則 2 条の 2 参照)。

107 改正電気通信事業法で定める特定利用者情報に関する規律と行政協定との関係については、後記**第 6. の 2. (2) ア**を参照。

108 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)」3-1-5(2022 年 9 月最新改正)(https://www.ppc.go.jp/files/pdf/230401_guidelines01.pdf)及び宇賀克也『新・個人情報保護法の逐条解説』250 頁(有斐閣、2021)。なお、一般財団法人情報法制研究所(JILIS)が 2020 年 4 月に公表した「捜査関係事項照会対応ガイドライン」(2020 年 4 月 1 日第 1 版作成)(https://www.jilis.org/proposal/data/sousa_guideline/sousa_guideline_v1.pdf)は、「『法令に基づく場合』とは、法令に基づき、適法になされた捜査関係事項照会に対して、必要かつ相当な範囲で個人情報の提供等を行った場合を意味するものと考えられる」から、「仮に捜査関係事項照会がなされた場合であっても、例えば、捜査との関連性がない情報等を捜査機関に報告することは、『法令に基づく場合』に該当せず、本人の同意を得ることが必要となる」との考え方が示されている。

現在、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として、電磁的記録命令の制度の創設に向けた検討が進んでいるが、これについても、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や条件を定め、法定の手続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、個人データの中でも、データの類型・性質や、(データの提供に関する事前・事後の本人の関与や司法機関等による審査の仕組み等を踏まえた)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。この点について、例えば、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は、電気通信事業者が、捜査機関からの要請により位置情報の取得を求められた場合においては、裁判官の発する令状に従うときに限り、当該位置情報を取得することができると規定している[109]。さらに、そうした令状の発付がある場合、あらかじめ利用者の同意を得ていることで、取得した位置情報を他人(捜査機関)へ提供することも認められるとしている[110] [111]。関連して、EU 電子証拠規則案が、データの種類に応じて提出命令の適用対象に差異を設けている点も参考となり得る(前記**第 3. の 2. (2)** 参照)。

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、これを公判において利用するにあたっては、以下のような課題もある。

(1) データの取り調べ方式

法制審議会・刑事法(情報通信技術)部会では、刑事手続における情報通信技術の活用に

---

109 個人情報保護委員会・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(令和 4 年 3 月 31 日個人情報保護委員会・総務省告示第 4 号)」41 条 4 項(2022 年 3 月)(https://www.soumu.go.jp/main_content/000805614.pdf)並びに個人情報保護委員会・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(令和 4 年 3 月 31 日個人情報保護委員会・総務省告示第 4 号)の解説」5-4-1 及び 5-4-4(2022 年 3 月)(https://www.soumu.go.jp/main_content/000805807.pdf)。

110 個人情報保護委員会・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(令和 4 年 3 月 31 日個人情報保護委員会・総務省告示第 4 号)」41 条 2 項(2022 年 3 月)(https://www.soumu.go.jp/main_content/000805614.pdf)及び個人情報保護委員会・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(令和 4 年 3 月 31 日個人情報保護委員会・総務省告示第 4 号)の解説」5-4-2(2022 年 3 月)(https://www.soumu.go.jp/main_content/000805807.pdf)。

111 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解説は、電気通信事業法上の通信の秘密に該当しない位置情報であっても、その取得又は利用は、利用者の同意を得る場合又は違法性阻却事由がある場合に限り行うことが「強く求められる」と規定している(5-4-1 及び 5-4-2 参照)。

関する検討会の取りまとめ報告書における提言[112]を踏まえ、電子的方法により作成・管理される証拠書類の公判廷における取り調べ方法について、データに記録された情報の種類や性質等に応じた取り調べの方式について検討がなされている[113]。具体的には、文字の言語的情報が証拠となるときは「朗読」すること、視覚的情報が証拠となるときは「表示」すること、そして聴覚的情報が証拠となるときは「再生」することといった仕組みが検討されている[114]。

この点、特に文字ではない情報の「表示」や「再生」にあたっては、これに用いられるハードウェア(スクリーン、再生機器等)やソフトウェア(画像や動画再生ソフトウェア等)の性能が、裁判官の心証形成に大きく影響し得ることに留意する必要がある。この問題は、必ずしもデータを証拠とする場合に固有の問題ではなく、これまでも映像を記録したDVDや音声を記録したテープ等を証拠とする場合にも存在していた問題であったが、今後、捜査機関が取得したデータの公判利用が一般的になれば、この問題がより頻繁に生じる可能性もあるため、議論が進展することが望まれる。

(2) データの真正性や正確性の確認方法

公判に顕出されたデータの真正性や正確性に疑義がある場合に、当該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、裁判所が確認する手段についても検討する必要がある[115]。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。

具体的には、捜査機関としては、証拠として提出しようとするデータの真正性や正確性に疑義が生じ得る場合に、その解析過程も含めて証拠化し、解析結果報告書として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

---

112 刑事手続における情報通信技術の活用に関する検討会「『刑事手続における情報通信技術の活用に関する検討会』取りまとめ報告書」18-19頁(2022年3月)(https://www.moj.go.jp/content/001368581.pdf)。

113 他にも、プロパティ情報等のメタデータを取り調べの対象とするかといった点についても検討がなされている。

114 法制審議会刑事法(情報通信技術関係)部会・第7回会議配布資料11「検討のためのたたき台(諮問事項「一」関係)」(https://www.moj.go.jp/content/001389630.pdf)の第1－5 1参照。

115 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))。

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[116]、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。

また、デジタルデータは改変が可能かつ容易であり、システムの動作に伴い書き換えられることもあることから、データの解析の前提として、その収集段階において同一性を確保した保全を行うことが必要である。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を担保すること等が必要である[117]。事業者側としても、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。さらに、捜査機関が作成する供述録取書等の証拠についても、電子署名やタイムスタンプ等の活用により保全を行うことが望まれる[118]。

もっとも、裁判所にとっては、捜査過程の記録の確認や捜査担当者に対する証人尋問を行っても、データの解析過程や保全方法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、提出されたデータや解析結果報告書の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[119]。また、今後、裁判所自身が提出されたデータや解析結果報告書の証拠能力や証明力を評価できるだけの能力、体制を拡充していくことが重要になると考えられる。

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。

---

116 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。

117 捜査対象のクラウドサービスを提供する事業者のサーバ上において、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ごと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。

118 法制審議会刑事法(情報通信技術関係)部会・第 4 回会議議事録(https://www.moj.go.jp/content/001386019.pdf) 6 頁、久保委員発言参照。

119 デジタル・フォレンジックによる保全・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 9 版」(2023 年 2 月 20 日)(https://digitalforensic.jp/wp-content/uploads/2023/02/shokohoznGL9.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。

(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)の侵害となるのかが問題となる[120]。

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あたり、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[121]、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[122]。

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)[123]。

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[124]。

---

120 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。

121 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)。

122 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)、酒巻匡「アメリカにおける自己負罪拒否特権の一断面――文書提出命令との関係について――」廣瀬健二＝多田辰也編『田宮裕博士追悼論集　下巻』447 頁、457 頁(信山社、2003 年)。

123 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))。

124 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))。他方で、法制審議会・刑事法(情報通信技術)部会でも、本人が拒否する場合に暗号資産の秘密鍵を強制的に明らかにさせることは自己負罪拒否特権の侵害になるのではないかとの問題提起がなされている(法制審議会刑事法(情報通信技術関係)部会・第 6 回会議議事録(https://www.moj.go.jp/content/001391536.pdf) 34 頁、久保委員発言参照。)。

(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る[125]。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) Act 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)[126]。

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、企業にあらかじめバックドアを設置させることについては、人権保障[127]、(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[128]、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[129]。そのため、高度に暗号化されたデータが第三者のサービスにアップロードされ、その復号鍵は利用者側でのみ保持するような場合には、そもそも当該

---

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

126 Australian Government, *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018, available at* https://www.legislation.gov.au/Details/C2018A00148.

127 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)。

128 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 (Apr. 2019), *available at* https://www.justice.gov/opa/press-release/file/1153446/download.

129 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)。

第三者が当該データを保持、保管又は支配していると言えるかが問題となる一方で、当該第三者が利用者の詳細を把握していないようなケースも想定される[130]。こうしたケースへの対処の在り方についても、今後議論が深まることが期待される。

[130] Justin Hemmings et al, *Defining the Scope of 'Possession, Custody, or Control" for Privacy Issues and the CLOUD Act*, pp. 654-667.

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。

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[131]、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[132]。

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[133]。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並びに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[134]。

---

131 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・岩瀬徹徹『実例刑事訴訟法 I 』5 頁、10-12 頁(青林書院、2012 年)、吉戒純一「判解」ジュリスト 1562 号 98 頁、100 頁(2021))。

132 Council of Europe Cybercrime Convention Committee (T-CY), *Transborder access and jurisdiction: What are the options?*, Doc no T-CY (2012)3, 6 (2012) *available at* https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e79e8.

133 山本草二『国際法〔新版〕』231 頁(有斐閣、1994)、岩沢雄司『国際法』174 頁(東京大学出版会、2020)。

134 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)、岩沢雄司『国際法』174-175 頁(東京大学出版会、2020)。

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[135]。このほか、各関係国と対象事項との間の「実質的かつ真正の連関」[136]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[137]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[138]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[139]。

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[140]。

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

---

135 酒井啓亘ほか『国際法』86 頁(有斐閣、2011)、岩沢雄司『国際法』175-183 頁(東京大学出版会、2020)。

136 山本草二『国際法〔新版〕』234 頁(有斐閣、1994)。

137 山本草二『国際法〔新版〕』239 頁(有斐閣、1994)。

138 United States v. Aluminum Co. of America, 148 F.2d 416 (1945).

139 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(有斐閣、2017)を参照。

140 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[141]。

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[142]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 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、パソコン等)

141　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否かや、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、前記**第 3. の 1. (2)**のとおり、EU の電子証拠規則案及び指令案では、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で管轄権行使の実効性を確保していると言える。
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、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。

142　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。

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[143]、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を挙げている[144]。

(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あたり、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

---

143 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)。

144 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)[145]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、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、属地主義に基づき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[146]。

この点に関連して、日本の会社法は、日本において継続して取引をしようとする外国会社に対して、日本における代表者を定め(会社法 817 条 1 項)、外国会社の登記をしなけれ

---

145 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ため問題である旨の 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))。

146 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 141 に記載のとおり、EU、韓国など、各国の実践において、国内に代理人や拠点を設置することを求め、当該代理人や拠点に対して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. (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 **2.(2)ア**参照)。

ばならないこととしている(会社法 818 条 1 項)。また、日本の電気通信事業法は、電気通信事業法の適用のある外国法人等[147]に対して、電気通信事業の登録の申請又は届出を行う際に国内における代表者又は国内における代理人を定めて総務大臣に提出することを義務付けている(電気通信事業法 10 条 1 項 2 号、16 条 1 項 2 号)。こうした代表者や代理人を通じて、日本国外の事業者に対して、国外に保存されたデータの提出を義務付ける枠組みを構築すべきか(あるいは他の枠組みを用いることが適当か)については、まさに本報告書で示すような検討課題を踏まえた検討を要すると思われる。

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など、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。

他国領域内における管轄権の行使は、当該領域国の主権権能の簒奪と見做される場合には、領域主権の侵害に当たる[148]。ただし、国際慣習又は条約でそれを許容する規則がある場合を除く。

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、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

147　総務省は、2021 年 2 月 12 日に電気通信事業法の地理的適用範囲に関する従前の解釈を変更して、外国法人等が「日本国内において電気通信役務を提供する電気通信事業を営む場合」又は「外国から日本国内にある者に対して電気通信役務を提供する電気通信事業を営む場合」には、外国法人等に対しても電気通信事業法が適用されるとの考え方を示した(総務省「外国法人等が電気通信事業を営む場合における電気通信事業法の適用に関する考え方」(2021 年 2 月 12 日)(https://www.soumu.go.jp/main_content/000739291.pdf))。

148　S.S. Lotus (France v. Turkey), 1927 P.C.I.J. (ser. A) No. 10 at 18-19 (Sep. 7); Michael Akehurst, “Jurisdiction in International Law,” 46 BRITISH YEAR BOOK OF INTERNATIONAL LAW,146, 147 (1972).

いとする立場もあるが、国際法上、議論は分かれている[149] [150]。

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の検討段階では、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、当該捜査手法に対して、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たが、結局、定められた時間枠内で合意することはできないとして、交渉の対象にならなかった(後記 **2. (2) イ参照**)。

一方、日本国内においても、国外に所在するサーバへのリモートアクセスに関して、近年、議論の進展がみられる。

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、国際捜査共助によることが望ましいとの考えを示していた

---

149 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)。
一部の国では、国内の法令上、国外に保存されているデータへのリモートアクセスを明示的に許容している例がある。例えば、ベルギーの刑事訴訟法上、一定の場合に国外に保存されたデータの複製を認めている(Code d'Instruction Criminelle, Art. 88 ter)。また、英国では、明文の規定はないものの、Police and Criminal Evidence Act 1984 の Sections 19-20 により、国外に保存されているデータへのリモートアクセスができると解されている。European Judicial Cybercrime Network, "Country information on direct access to e-evidence" (https://www.eurojust.europa.eu/judicial-cooperation/practitioner-networks/european-judicial-cybercrime-network)も参照。
さらに、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(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))、デンマークの捜査機関による SNS アカウントへのアクセスを許容した事例(U 2012.2614 H, Højesteret, 12.05.2012)(非公式英訳 https://sas-space.sas.ac.uk/5563/1/2038-2939-1-SM.pdf)がある。

150 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＝松尾浩也編『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。

[151]。これに対して、学説上は、サーバ所在地が判明しない場合にまで国際捜査共助に依ることを求めることは、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った[152]。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あった[153]。

そのような中、令和 3 年最高裁決定は、①「電磁的記録を保管した記録媒体が[サイバー犯罪]条約の締約国に所在し」、②「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」と判断した。もっとも、令和 3 年最高裁決定は、リモートアクセスによって収集された証拠が違法収集証拠として排除されるか否かを判断する前提として、その収集手続に「重大な違法」があるか否かを判断したにすぎないとされ[154]、リモートアクセスの適法性・違法性の判断基準を明確に示したものではないと思われる。

令和 3 年最高裁決定は、上記①及び②の要件をいずれも満たすリモートアクセスは適法であると明言する一方、上記①又は②のいずれかの要件を満たさないリモートアクセスの適法性については明言していない。もっとも、令和 3 年最高裁決定において問題となったリモートアクセスは、上記①の要件を満たさなかった(電磁的記録を保管した記録媒体の所在は不明であった)にも関わらず、「警察官が、国際共助によらずに 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相当であるということはできず」と説示されており、最高裁は、上記①の要件を満たさない場合であっても、上記②の要件を満たしさえすれば適法にリモートアクセスを行い得るとの前提に立っている可能性がある[155]。また、令和 3 年最高裁決定は、被処分者による任意の承諾が否定されないリモートアクセス(「手続<イ>」)により収集された証拠の証拠能力を、極めて簡潔な理由付けにより肯定しており、任意処分として実施されるリモートアクセスの場合には、刑事

---

151 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)。

152 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)。

153 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)。

154 吉戒純一「判解」ジュリスト 1562 号 98 頁、104 頁(2021)。

155 成瀬剛「判批」ジュリスト 1577 号 160 頁、163 頁(2022)。

訴訟法上の問題が少ないとの前提に立っている可能性がある[156]。

そして、このような令和 3 年最高裁決定の傾向も踏まえてか、法務省刑事局国際刑事企画官(当時)が令和 3 年最高裁決定後の 2022 年 11 月に個人の見解として公表した論稿においては、「当該電磁的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を得てリモートアクセスを行うことは〔サーバの所在地国を問わず〕許容される」とする一方で、令状に基づく強制処分としてのリモートアクセスについては、「国際捜査共助を要請しなければならない場合か否か、そしてどの国に対して要請すべきかを判別することが困難な場合」において許容されるとの見解が示されている[157]。かかる見解は、日本の捜査機関が日本に所在する者を通じて国外に所在するサーバにリモートアクセスする際の基本的な指針になるものと思われる。

もっとも、令和 3 年最高裁決定の原判決である大阪高判平成 30 年 9 月 11 日刑集 75 巻 2 号 220 頁等で示されているように、裁判所は任意の承諾の有無を厳格に判断する傾向があることから、アクセス権限を有する者による承諾の取得を優先し、これに全面的に依拠する捜査を行うことは、捜査の迅速性や安定性の観点からは必ずしも望ましくない可能性がある。また、リモートアクセスにおいては、データ主体のみならず、データが保存されているサーバ管理者等の利益にも配慮すべきである(前記**第 4.の 1.(3)イ(イ)**参照)ところ、アクセス権限を有する者の承諾に基づく任意捜査としてのリモートアクセスでは、サーバ管理者等の利益に十分に配慮できない可能性がある[158]。そのため、中長期的には、むしろ、令状審査を経ることで適正手続を担保した越境リモートアクセスが国際法上も許容されることを正面から認める方向で、国際的な合意を形成することを目指していくことも考えられる[159] [160]。

---

156 三浦裁判官の補足意見も、問題となったリモートアクセスにより収集された証拠能力について、「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」(強調加筆)と述べており、任意処分として実施されるリモートアクセスの場合には問題が少ないことを示唆している可能性がある。

157 北嶋良蔵「越境リモートアクセスについて」警察学論集 75 巻 11 号 114 頁、134-138 頁(2022)。

158 さらに、前記脚注 55 に記載のとおり、企業のサーバに保存されたデータには高度なプライバシー情報も多数含まれており、住居内のプライバシーに匹敵する状況となっていることからすると、アクセス権限を有する者との関係でも、より手続保障を充実化させることが望ましい可能性もある。

159 外務省国際法局審議官(当時)が 2022 年 5 月に個人の見解として公表した論稿においては、「すぐに国際的な合意を形成することは困難かもしれないが、中長期的な視野に立てば、…正当なアクセス権限を有する者が国内に所在し、捜査当局が犯罪捜査のために必要な場合に令状をもってその者が正当な権限を有するデータにアクセスして参照・複写するだけであれば、…基本的に違法な主権侵害とならない可能性が高い、という考え方は、国内における犯罪捜査の必要性と他国の領域主権への配慮とのバランスのとり方として一定の合理性があると思われる」(強調加筆)との見解が示されている(御巫智洋「インターネットの利用に関する国際的なルールにおいて領域主権が果たす機能」国際法外交雑誌 121 巻第 1 号 1 頁、14 頁(2022))。

160 このような方向性は、ガバメントアクセスに関して事前承認や監督のメカニズムを設けるべきであるとする OECD ガバメントアクセス宣言(前記**コラム①**参照)とも整合する。

(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、GDPR 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告された[161]。そして 2020 年 7 月 16 日、米欧プライバシーシールドを無効とする欧州司法裁判所の判決が下されたことを受け、米国は、2022 年 10 月 7 日、当該判決が提起した懸念の全てに対応したとされる、米国大統領令及び司法長官が定める規則に基づく新しい米欧データプライバシーフレームワーク(EU-U.S. Data Privacy Framework。以下「**DPF**」という。)を公表した[162]。DPF は、米国側からの命令の対象となり得るデータは必要かつ相当な範囲に限定されること、EU 市民は、米国側の要請に関して、米国の情報機関の「市民の自由保護官」(Civil Liberties Protection Officer。以下「**CLPO**」という。)に対して不服を申し立てることができ、CLPO はその調査結果を司法長官に提出して適切な措置を求める(司法長官は外国情報監視裁判所に連携する)こと、その上で、EU 市民は、CLPO の決定を米国のデータ保護審査裁判所(Data Protection Review Court。米国政府外の 3 名の裁判官から構成される。)に上訴でき、同裁判所は必要な調査やデータの削除命令を下すことができることなどが明確化されており、今後 EU による十分性認定に向けた検

---

161 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.さらに、欧州データ保護監督官(EDPS)及び欧州データ保護会議(EDPB)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、CLOUD Act に基づく個人データの米国への移転が 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(EDPB, *EDPB-EDPS Joint Response to the LIBE Committee on the impact of the US Cloud Act on the European legal framework for personal data protection*, (12 July, 2019), *available at* https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-edps-joint-response-libe-committee-impact-us-cloud-act_en).

162 The White House, *FACT SHEET: President Biden Signs Executive Order to Implement the European Union-U.S. Data Privacy Framework*, (October 7, 2022), *available at* https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/07/fact-sheet-president-biden-signs-executive-order-to-implement-the-european-union-u-s-data-privacy-framework/.これを受けて、欧州委員会は、2022 年 12 月 13 日に、DPF に対する十分性認定の採択に向けたプロセスを開始し、決定文のドラフトを公表しており(European Commission, *Data protection: Commission starts process to adopt adequacy decision for safe data flows with the US* (13 December 2022), *available at* https://ec.europa.eu/commission/presscorner/detail/en/ip_22_7631)、2023 年夏頃の認定を目指しているとされている。この他に、米国商務省は、2023 年 1 月 11 日、DPF に関する Q&A を公表している(https://www.privacyshield.gov/article?id=EU-U-S-Privacy-Shield-Program-Update)。

討が進む見込みである[163]。今後、他国との関係でも同様の問題が生じる可能性もあろう[164]。

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、ある国によるデータ提出命令等が、各国内法令と抵触した場合の調整方法等については、依然として不明確な状況であり、確立した国際法上の規則があるとは言い難い[165]。

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 1.(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し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[166]。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。

また、EU の電子証拠規則案においても、第三国の適用法令との抵触を理由に、提出命令に対して異義を申し立てることができる制度が設けられている。提出命令の名宛人が、提出命令を遵守することにより第三国の適用法令に抵触すると考える場合には、発令機関及び法執行機関に異義を申し立てることができ、通知を受けた発令機関は提出命令を維持するか否か、改めて検討する。検討の結果、発令機関としては提出命令を維持すべきであるとの結論に至った場合には、当該加盟国の管轄裁判所に審査を求める必要があり、最終的には、当該管轄裁判所の判断に従うこととなる。なお、この場合、管轄裁判所の審査が終了するまでは、提出命令の執行は停止する[167]。

---

163 EDPB, *EDPB welcomes improvements under the EU-U.S. Data Privacy Framework, but concerns remain*, (28 February, 2023), *available at* https://edpb.europa.eu/news/news/2023/edpb-welcomes-improvements-under-eu-us-data-privacy-framework-concerns-remain_en.

164 個人の権利を保護する手続的なセーフガードの有無及び内容も含め、各国のデータ保護法令、個人情報保護法等については、例えば、西村あさひ法律事務所「外国における個人情報の保護に関する制度等の調査結果報告書」(2021 年 11 月)(https://www.ppc.go.jp/files/pdf/offshore_DPA_report_R3_12.pdf)も参照。

165 酒井啓亘ほか『国際法』86 頁(有斐閣、2011)。The European Union and the Council of Europe, *Cooperation between law enforcement and Internet service providers against cybercrime: towards common guidelines,* p. 5 (2020), *available at* https://rm.coe.int/0900001680a091a7 も参照。

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

167 電子証拠規則案 16 条。

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[168]。

この MLAT を通じた手続は、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 か月から 24 か月(平均的には 10 か月)程度の時間を要するのが実情であり[169]、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[170](より迅速な手法としてサイバー犯罪条約第二追加議定書が定める締約国の当局間の協力については後記**(2)ウ(イ)**参照)。さらに、どの国にデータが保存されているかが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[171]。

(2) サイバー犯罪条約・第二追加議定書・「国連サイバー犯罪条約」

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

---

168 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。

169 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).

170 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)。

171 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).

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[172]。

その後、2021 年 11 月 17 日の欧州評議会閣僚委員会において、サイバー犯罪条約の第二追加議定書が採択され、2022 年 5 月 12 日に日本を含めた 22 か国が署名した。同追加議定書は 5 か国の批准で発効するところ、現時点では発効していない。サイバー犯罪条約第二追加議定書は、サービスプロバイダやレジストラとの直接的な協力、加入者情報及びトラフィックデータを入手する効果的な手段、緊急時又は共同捜査における即時協力など、協力の強化や電子証拠の開示のための手法を提供する[173]。

さらに、国連では、2019 年 11 月 18 日、情報通信技術の犯罪目的での利用への対処(“countering the use of information and communications technologies for criminal purposes”)に関する包括的な国際条約を検討すべく、オープンエンドかつアドホックな政府間専門家・地域代表委員会(以下「**アドホック委員会**」という。)を設置することを含む決議案が、国連総会第三委員会で採択され[174]、2019 年 12 月 27 日には、国連総会本会議において当該決議が採択された[175]。これにより、かかる国際条約を議論するためのアドホック委員会が設置された。また、2021 年 5 月 26 日、国連総会本会議で、当該国際条約の交渉条件を示す決議が採択され、アドホック委員会は、2022 年 1 月以降 6 回の会合を経た後、2024 年開催の第 78 回国連総会本会議において条約案を提出することが決定された[176]。アドホック委員会は、2023 年 1 月開催の会合に向けて、「情報通信技術の犯罪目的での利用への対処に関する包括的国際条約」(以下「**国連サイバー犯罪条約**」という。)の前文、国際協力、防止措置、情報交換を含む技術的援助、履行枠組み等に関する規定の草案を公表した[177]。

---

172 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).

173 Council of Europe, *Second Additional Protocol to the Cybercrime Convention on enhanced co-operation and disclosure of electronic evidence (CETS No. 224), available at* https://www.coe.int/en/web/cybercrime/second-additional-protocol.

174 United Nations, *Countering the use of information and communications technologies for criminal purposes : report of the 3rd Committee : General Assembly, 74th session,* A/74/401 (25 Nov. 2019), *available at* https://digitallibrary.un.org/record/3837326?ln=en.

175 United Nations, *Countering the use of information and communications technologies for criminal purposes : resolution / adopted by the General Assembly,* A/RES/74/247, (20 Jan. 2020), *available at* https://digitallibrary.un.org/record/3847855?ln=en.

176 United Nations, *Countering the use of information and communications technologies for criminal purposes : resolution / adopted by the General Assembly,* A/RES/75/282, (1 June 2021), *available at* https://digitallibrary.un.org/record/3928637?ln=en.

177 United Nations, *Consolidated negotiating document on the preamble, the provisions on international cooperation, preventive measures, technical assistance and the mechanism of implementation and the final provisions of a comprehensive international convention on countering the use of information and communications technologies for criminal purposes,* A/AC.291/19, (19 December 2022), *available at* https://www.unodc.org/documents/Cybercrime/AdHocCommittee/5th_session/Documents/2228246E_Advance_Copy.pdf.

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締約国の捜査機関に与えるため、必要な立法その他の措置をとることを締約国に義務付けている[178]。

(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[179]。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、そうした場合にも締約国の捜査機関が自国の領域内に所在する者又は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て提出命令を発することが可能であると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[180]。それゆえ、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は、更に検討が続けられるものと考えられる。

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

---

178 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)。

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

180 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[181]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[182]。

さらに、同条(b)は、同条項に記載された行為以外の捜査、すなわち、データ主体の同意が得られない場合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[183]。この点については、第二追加議定書の検討時間枠内で合意することができないとして交渉の対象にならなかったが[184]、引き続き検討は進められている[185]。

ウ　第二追加議定書

サイバー犯罪条約第二追加議定書では、他の締約国に所在する者や他の締約国の当局との協力を強化する手続が定められ、また、個人情報の保護に関する規定が定められた点に意義があると言える。

(ア) 他の締約国に所在する者との直接協力

サイバー犯罪条約第二追加議定書の 6 条では他の締約国に所在するドメインレジストラ

---

181 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り、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))。

182 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).

183 Council of Europe Cybercrime Convention Committee (T-CY), *Transborder access and jurisdiction: What are the options?*, Doc No T-CY (2012)3, 27 (2012) *available at* https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e79e8.

184 Council of Europe, *Explanatory Report to the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence*, paragraph 24 p. 5 (2022), *available at* https://rm.coe.int/1680a49c9d.

185 Council of Europe Cybercrime Convention Committee (T-CY), *Report on the 27th Plenary of the Cybercrime Convention Committee Strasbourg and online, 29-30 November 2022*, Doc No T-CY (2022)23, p. 4 (2022), *available at* https://rm.coe.int/t-cy-2022-23-plen27-rep-v5/1680a93b1c.

が保有又は管理するドメイン名登録情報の開示要請について定められ、また、7 条では他の締約国に所在するサービスプロバイダが保有又は管理する加入者情報の開示命令について定められた。前者については、多くのサイバー犯罪において、犯罪者が悪意ある不正な目的(例えば、マルウェアの拡散、詐欺)のためにドメインを作成し、利用することによって行われているという背景があることから、当該ドメインを登録した者に関する情報へのアクセスは容疑者の特定のために極めて重要であるとして規定された [186]。また、後者については、加入者情報がサイバー犯罪や電子証拠が必要とされるその他の犯罪の捜査において必要とされる基礎情報であり、他の種類のデータと比較して、開示によるプライバシー等の侵害の程度が低いと言えるため規定された [187]。

サイバー犯罪条約第二追加議定書 6 条及び 7 条は、基本的に同様の構成となっており、まず、1 項において、各締約国は、自国の権限のある当局に対して、他の締約国に所在する者が保有又は管理している情報の開示を要請又は命令する権限を与えるために必要な立法その他の措置をとるべきことを規定している。そして、2 項において、各締約国は、自国の領域内に所在する者が他の締約国の要請又は命令に応じて情報を開示することを認めるために必要な立法及びその他の措置をとるべきことを規定する。ただし、6 条は自国の権限のある当局に、他の締約国の領域内に所在するドメインレジストラに対してドメイン名登録情報の提出を「要請」する権限を認めるにとどまるのに対し、7 条は、自国の権限のある当局に、他の締約国の領域内に所在するサービスプロバイダに対して直接加入者情報の開示を「命令」する権限を認めている上、同条を自国で適用しない権利の留保が認められている(同条 9 項)[188]という相違点もある。なお、7 条を自国で適用しない権利を留保した締約国は、自国の領域内に所在するサービスプロバイダが他の締約国が発する命令に応じて加入者情報を開示するための同条 2 項に基づく措置をとる必要はないものの、相互主義により、他の締約国に所在するサービスプロバイダに対して同条 1 項に基づく加入者情報の開示命令を発することはできないとされている [189]。

そのため、日本としてサイバー犯罪条約第二追加議定書を批准し、必要な立法・制度整備を行えば、他の締約国に所在するドメインレジストラに対して直接ドメイン名登録情報

---

186 Council of Europe, *Explanatory Report to the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence*, paragraph 74 p. 13 (2022), *available at* https://rm.coe.int/1680a49c9d.

187 Council of Europe, *Explanatory Report to the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence*, paragraph 92 p. 17 (2022), *available at* https://rm.coe.int/1680a49c9d.

188 サイバー犯罪条約第二追加議定書の一部を自国で適用しない権利を留保するか否かについては、自国の国内法との関係も重要になる(外国政府等からの情報開示要請・命令と電気通信事業法及び個人情報保護法との関係については、後記**第 6. の 2. (2)** 参照。)。

189 Council of Europe Cybercrime Convention Committee (T-CY), *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence: Explanatory Report,* paragraph 122 (17 November 2021) *available at* https://search.coe.int/cm/pages/result_details.aspx?objectid=0900001680a48e4b#globalcontainer.

の開示を要請したり、他の締約国に所在するサービスプロバイダに対して直接加入者情報の開示を命令したりすることができる(ただし、後者については当該他の締約国が留保していない場合に限られる。)ようになる(前記**第 4. の 1. (3)ア**参照)。

(イ) 他の締約国の当局との協力

サイバー犯罪条約第二追加議定書 8 条 1 項は、各締約国が、自国の権限のある当局に対し、他の締約国への要請の一部として、要請を受ける締約国の領域内に所在するサービスプロバイダに対して、当該サービスプロバイダが保有又は管理する他の締約国内において保存された加入者情報及び通信記録の提出を、当該サービスプロバイダに強制するための命令を発する権限を付与することを認めている。そして、各締約国は、要請を行う締約国が提出した命令を執行するために、必要な立法その他の措置をとることが求められている(同条 2 項)。

この手続は、MLAT を通じた手続(前記**(1)**参照)と比べて、より迅速な加入者情報及び通信記録の開示を可能にする。要請を行う締約国は、要請を受ける締約国に対し、命令並びに補助的な情報及び特別な手続上の指示を提出する必要があり(同条 3 項、4 項)、要請を受ける締約国は、全ての情報の受領日から遅くとも 45 日以内に当該命令をサービスプロバイダに送達するよう妥当な努力を払うことが求められる。そして、要請を受ける締約国は、当該サービスプロバイダに対し、要請された加入者情報については 20 日以内に、通信記録については 45 日以内に提出するよう命じることになる(同条 6 項 a)。

通信記録については同条を自国で適用しない権利の留保が認められているものの(同条 13 項)、日本としてサイバー犯罪条約第二追加議定書を批准し、必要な立法・制度整備を行えば、他の締約国に所在するサービスプロバイダに対して、当該他の締約国を通じて加入者情報及び通信記録の提出を求めることができる(ただし、後者については当該他の締約国が留保していない場合に限られる。)ようになる。なお、通信記録について 8 条を自国で適用しない権利を留保した締約国は、自国の領域内に所在するサービスプロバイダに対して、他の締約国が発する通信記録の提出命令に応じる必要はないものの、相互主義により、他の締約国に所在するサービスプロバイダに対して同条 1 項に基づく通信記録の提出命令を発することはできないとされている[190]。

(ウ) 個人情報の保護に関する規定

サイバー犯罪条約第二追加議定書は、14 条において、個人情報の保護措置に関する詳細

---

190 Council of Europe Cybercrime Convention Committee (T-CY), *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence: Explanatory Report,* paragraph 147 (17 November 2021) *available at* https://search.coe.int/cm/pages/result_details.aspx?objectid=0900001680a48e4b#globalcontainer.

な義務を定めている[191]。

例えば、同条 4 項は、「機微に係る情報」として、人種的若しくは民族的出身、政治的意見、宗教的信条その他の信条若しくは労働組合の構成員であることを明らかにする個人情報、遺伝上の情報、関連する危険性を考慮して機微に係ると認められる生体認証情報又は健康若しくは性生活に関する個人情報を列挙し、締約国における当該情報の処理は、これらの情報の使用による不当かつ有害な影響の危険性、特に違法な差別から保護するための適切な保証措置の下でのみ行うことができるとしている。

また、同条 11 項は、各締約国に対して、一般的な通知の公表により、又は収集された個人情報に係る個人に対する個別の通知により、①処理の法的根拠及び目的、②保有又は審査の期間、③当該個人情報の開示を受ける者又はその分類並びに④利用可能なアクセス、訂正及び救済を通知することを義務付けており、EU の電子証拠規則案と同様に、情報の開示がなされたデータの主体に対する一定の透明性を確保させる制度が導入されている。この点については、日本国内でも、今後、データ主体に対する手続保障と捜査の実効性のバランスを踏まえ、データ主体に対する通知の制度化を検討していく必要があると考えられる(前記**第 4. の 1. (3)イ(ア)**参照)。

エ　「国連サイバー犯罪条約」

2022 年 12 月 19 日に公表された国連サイバー犯罪条約の条文草案には、サイバー犯罪条約及びサイバー犯罪条約第二追加議定書と同様の規定も織り込まれている。

具体的には、刑事相互共助(Mutual legal assistance)として、大要次の 2 つの事項を行う権限を締約国に与えることについて議論が進められている。

(i) 他の締約国の領域内にある[コンピュータ・システム][情報通信技術システム/デバイス]により保存されている[データ][情報]であって、要請する締約国が当該[データ][情報]の捜索若しくは同様のアクセス、押収若しくは同様の取得又は開示に関する相互共助の要請を提出しようとするものについて、当該[データ][情報]の迅速な保存を命令し、又はその他の方法で取得するよう、当該他の締約国に要請すること(68 条 1 項)

(ii) 他の締約国に対し、当該他の締約国の領域内にある[コンピュータ・システム][情報通信技術システム/デバイス]により保存されている[データ][情報](68 条に従って保存されている[データ][情報]を含む。)の捜索若しくは同様のアクセス、押収若しくは同様の取得又は開示することを要請すること(70 条 1 項)

---

191 ただし、移転国及び受領国の双方が個人情報保護のための包括的な枠組みを設定する締約国の間の国際協定であって、一定の要件を満たすものに拘束される場合には、同条の規定に代えて当該国際協定の規定が適用される(同条 1 項 b)。また、上記のような国際協定がない場合には、移転国及び受領国の間で、情報の移転を、他の協定又は取極に基づいて行うことができることを相互に決定することができる(同項 c)。

また、72 条では越境アクセスについて規定されており、締約国は、(留保条件に従って、)他の締約国の承認を受けることなく、次の 2 つの事項を行う権限を締約国に与えることが検討されている。

(i) [データ][情報]が地理的にどこに所在するかを問わず、一般に利用可能な状態で(オープンソースとして)保存された[コンピュータ・データ][電子/デジタル情報]にアクセスすること

(ii) 自国の領域内の[コンピュータ・システム][情報通信技術システム/デバイス]を通じて、他の締約国に所在する保存された[コンピュータ・データ][電子/デジタル情報]にアクセスし、又はこれを受領すること(但し、[データ][情報]にアクセスし、又は受領する締約国が、当該コンピュータ・システムを通じて当該締約国に[データ][情報]を開示する適法な権限を有する者の適法かつ任意の同意を取得する場合に限る。)

2024 年開催の第 78 回国連総会本会議で国連サイバー犯罪条約案が提出される予定であるものの、2023 年 1 月からようやく草案ベースでの議論が開始されたことを踏まえると、交渉の加速化が図られない限り国連サイバー犯罪条約の締結にはまだ時間を要する可能性が高いと考えられるが、国連においても、サイバー犯罪に関し、刑事相互共助や越境アクセスについて議論がなされているという点で、今後の交渉の推移を注視すべきであると考えられる。

(3) 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について、相手国の同意を得ることで、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。

例えば、米英間の行政協定に基づき、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(拘禁刑 3 年以上の刑罰の対象となる犯罪)に関連するデータの提出を求めることができる(同協定 1 条、4 条、5 条)。

具体的には、一方当事国の捜査機関は、当該当事国の国内法に従って、裁判所等の独立した機関の審査を経て、データの開示命令を取得する(この命令は、他方当事国や第三国の要請によって発行することはできない。)(5 条 1 項から 4 項まで)。そして、一方当事国の捜査機関は、当該命令が行政協定を遵守したものであることを確認した上で、(他方当事国の機関等を介することなく)他方当事国のプロバイダに対して直接当該命令を交付することができるが(5 条 5 項及び 6 項)、その際には当該命令が一方当事国の国内法及び行政協定を遵守したものであることの証明書を添付し、また、当該プロバイダに当該命令は行政協定に関するものであること、及び当該捜査機関の連絡先を通知しなければならない(5 条 7 項から 9 項まで)。これに対して、プロバイダは、一方当事国の捜査機関に対して直接データを提供することができる(6 条 1 項)。ただし、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は、当該データを公判等で使用することを拒否できる権利がそれぞれ規定されている(同協定 8 条 4 項)。

また、米豪間の行政協定においてもこれら米英間の行政協定と同様の規定が見当たる。なお、米豪間の行政協定上は、プロバイダの回答方法に関してデータ提出要請国側が定める要件には、当該開示命令や回答の秘密保持を含める旨の規定が見当たる一方で(米豪行政協定 6 条 4 項)、米英行政協定には明示的にその旨の規定が見当たらないものの、プロバイダからデータ提出要請国側への安全なデータ送信のための措置を講じることができる旨の規定は定められていること等を踏まえると、実際には米豪行政協定と同様の取扱いがなされる可能性はある。

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 1. (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 [192]。さらに、日本において令状の請求・発付・執行の電子化が実施され、電磁的記録提供命令も創設されることになれば、日本が米国をはじめとするすでに刑事手続の電子化やデータそれ自体を対象とした捜査活動を実現している諸外国の捜査機関との連携の効果を最大限発揮する制度的な下地も整うこととになる。

そこで、以下では、日本が米国との間で行政協定を締結したとして、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 [193]、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)

---

192 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 (Apr. 2019), *available at* https://www.justice.gov/opa/press-release/file/1153446/download.

193 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。

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[194]。

(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を侵害し、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 4 条、179 条)。そこで、このような開示が、通信の秘密のデータ主体の有効な同意に基づく開示と言えるかや、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[195]、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[196]。このこと

194　同様に、仮に日本と米国政府が行政協定を締結し、日本の捜査機関が日本法に基づき米国企業から直接データの提出を求めるようになった場面においても、適正手続の要請は満たされる必要がある。
従来、国際捜査共助は、それぞれの国で証拠の獲得行為の要件、手続が異なることを当然の前提として成り立っている制度であることから、国際捜査共助によって獲得された証拠の使用が日本において適正手続違反となる範囲は、日本の捜査機関によって証拠が取得された場合と比較して限定されると解されてきた(川出敏裕「国際司法共助によって獲得された証拠の許容性」研修 618 号 3 頁、7 頁(1999)、最決平成 12 年 10 月 31 日刑集 54 巻 8 号 735 頁等)。これに対して、行政協定に基づき日本の捜査機関が米国の企業から直接取得したデータの証拠能力は、国際捜査共助によって米国の捜査機関に依頼して取得されたデータの証拠能力の評価枠組みではなく、日本の捜査機関が国内で取得した証拠能力の評価枠組みに従って判断されることになり得る。このことからすれば、行政協定の締結は、捜査機関による国外に所在するデータの取得との関係でも、日本国憲法及び日本の刑事訴訟法に基づく証拠評価を含む適正手続の保障が及ぶことを明確化する効果を持つものとも言い得る。

195　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。

196　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国外に所在し、かつサーバの管理者等が国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。

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。

さらに、改正電気通信事業法に基づく特定利用者情報の規律について(前記**第 4. の 1. (3) オ(ア)**参照)、CLOUD Act に基づく米国政府の捜査活動の関係で注目すべきは、特定利用者情報の漏えい報告に関するものである。改正電気通信事業法上、指定電気通信事業者は、一定の特定利用者情報の漏えいが生じた場合に、総務大臣へ報告を行うよう義務付けられるところ [197]、対象となる特定利用者情報には、「特定利用者情報の適正な取扱いに影響を及ぼすおそれのある外国の制度に基づき、外国政府に提供を行ったもの」が含まれている [198]。

この点について、改正電気通信事業法に関するガイドラインの解説の改正案は、「特定利用者情報の適正な取扱いに影響を及ぼすおそれのある外国の制度」とは、指定電気通信事業者に対し政府の情報収集活動への協力義務を課すことにより、指定電気通信事業者が保有する特定利用者情報について政府による情報収集が可能となる制度であって、特定利用者情報に係る利用者の権利利益に重大な影響を及ぼす可能性のある制度に限られるとし [199]、そのような制度に基づく特定利用者情報の開示が、漏えい報告の対象になるとの考え方を示している [200]。今後の運用において、米国の法制度に従ったデータの開示が漏えい報告の対象とされることで米国の捜査活動に支障を生じさせることにならないか等については注視する必要がある。

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

197　改正電気通信事業法 28 条 1 項 2 号ロ。

198　改正電気通信事業法施行規則 58 条 1 項 2 号。
「特定利用者情報の適正な取扱いに影響を及ぼすおそれのある外国の制度」という表現については、外国にある第三者による相当措置の継続的な実施を確保するために必要な措置等について定める個人情報保護法施行規則第 18 条 1 項 1 号等における規定ぶりを参考としたものとされている(総務省「電気通信事業法施行規則等の一部を改正する省令案等に対する意見及びそれに対する考え方(審議会への必要的諮問事項以外の事項に係るもの)」(https://public-comment.e-gov.go.jp/servlet/PcmFileDownload?seqNo=0000246510)17 頁)。

199　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(令和 4 年個人情報保護委員会・総務省告示第 4 号)の解説の一部改正の新旧対照表(https://www.soumu.go.jp/main_content/000870399.pdf)78 頁、51 頁。

200　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及びその解説の改正案に対する意見募集」(https://www.soumu.go.jp/menu_news/s-news/01kiban18_01000188.html)。

該データ主体の個人データを(外国に所在する)第三者に提供することが禁止されている(同法 27 条 1 項、28 条)。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[201]。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、データ主体の同意を得ることなくこれに応じた場合、個人情報保護法に抵触するおそれがある。また、仮にデータ主体の同意を得ようとする場合であっても、個人情報保護委員会が公表している「その他本人の権利利益に重大な影響を及ぼす可能性のある制度」[202]に関する情報を踏まえた情報提供をどの程度、どのような形で行うべきかといった点を検討する必要があり得る。

3. 行政協定設計上の留意点

まず、日本では、大平三原則[203]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[204]。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[205]。

(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

---

201 「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)。

202 個人情報保護委員会「外国制度(アメリカ合衆国)」(https://www.ppc.go.jp/enforcement/infoprovision/laws/offshore_report_america/#law)(2023 年 4 月 14 日最終閲覧)。

203 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既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))。

204 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))。

205 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[206]。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)」[207]、「重大な犯罪(serious crime)」[208]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[209]。

(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、従来とおり、MLAT に依ることを求めている[210]。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、米英間の行政協定では、双方の住民[211]を(意図的に)標的にしないことが定められた

---

206 例えば、米英間の行政協定では、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(同協定 8 条 4 項)。このほかにも、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/)。

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

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

209 例えば、米英行政協定では、「重大な犯罪(serious crime)」とは、3 年以上の長期刑が科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)。

210 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.

211 英国の捜査機関は米国市民を標的にできない一方で、米国の捜査機関が英国国民や英国市民を標的にできない旨は定められていない(4 条 3 項、1 条 12 項)。これは、米英協定の交渉当時には、英国は EU の一部であったところ、EU 加盟国のいずれの市民であるかによって異なる取扱いを定めることができないとされていたことが意識されているのではないかとの指摘がある(Theodore Christakis, "21 Thoughts and Questions about the UK-US CLOUD Act Agreement", European Law Blog (October 17, 2019))。

(同協定 4 条 3 項)。

加えて、CLOUD Act に基づいて米国政府からの開示命令が出され得る場合に、日本政府ないし日本国民の権利利益の保護が適切に図られるような仕組みを整備しておくことも重要である。例えば、(通常は想定し難いように考えられるものの)仮に、米国の捜査機関が、その刑事捜査のために、デジタル庁が主導して整備を進めている日本の政府機関共通のクラウドサービスの利用環境(ガバメントクラウド)上にある日本政府のデータや日本政府が保有するデータに関して、当該ガバメントクラウドを運営するクラウドサービスプロバイダに対して開示命令を行うことを検討する場面を想定して、日米の捜査機関の間で、そのような開示命令の発出に先立って、その要否等について直接協議・調整できる場を設置しておくことができないかを検討することには一定の意義があるように思われる。また、仮に、米国法令上の諸要件を満たすとしてそのようなデータの開示命令が出される場合でも、当該クラウドサービスプロバイダ側においても当該諸要件が満たされるかを吟味したうえで、国際礼譲を含む当該開示命令の修正・取消し事由の有無を検討し、必要に応じてその旨の主張を行うほか、場合によっては当該プロバイダにおいて外国主権免除法に基づく主権免除の主張を行うこと等を確保しておくことによって、日本政府の権利利益の保護が適切に図られるような仕組みは確保し得るように思われる[212]。

(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等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、日本と米国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

212 デジタル庁の「ガバメントクラウド整備のためのクラウドサービスの提供 -令和 4 年度募集-」の応募要領や調達仕様書のほか、令和 4 年 3 月 25 日衆議院内閣委員会における楠政府参考人答弁(議事録：https://www.shugiin.go.jp/internet/itdb_kaigiroku.nsf/html/kaigiroku/000220820220325012.htm)、及び令和 4 年 11 月 11 日衆議院内閣委員会における二宮政府参考人答弁(議事録：https://www.shugiin.go.jp/internet/itdb_kaigiroku.nsf/html/kaigiroku/000221020221111007.htm)参照。このように、ガバメントクラウド上のデータを巡る米国捜査機関からの開示要請に対して日本の権利利益を保護するために必要な仕組みは、既にデジタル庁が公表するガバメントクラウドの調達仕様に反映されており、今後地方自治体等においてガバメントクラウドの利用が普及していく中でも、有効に機能し得るものと考えられる。そして、米国捜査機関によるガバメントクラウドのサービスプロバイダに対するデータ開示命令は、上記のとおり、そもそもの捜査上の必要性のほか、データ開示命令の米国法令適合性や、国際礼譲による審査、主権免除の可能性等も検討した結果として初めて、現実的な問題になり得るにとどまることからすると、CLOUD Act による国内への影響は、ガバメントクラウドを巡る議論とは直接のかかわりなく、本報告書で示すより幅広い視点から検討されるべきものであると考えられる。

[213]。

(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。実際、既に米国と行政協定を締結した英国[214]やオーストラリア[215]はいずれも、国内法を改正し必要な整備をした上で行政協定を締結している。このような国際的に調整された成果が国内法にも取り込まれていくことで、規制内容が重層・複雑化し、不透明になる状況を避けることもできる。

---

213 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の通知を受けた。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。
その後、前記通知日から 2 年以内に行うとされていた 1 回目の十分性認定のレビューについて、2021 年 10 月 26 日、日欧双方が報告書を公表することを以て当該レビューが完了する旨が公表された。そして、2023 年 4 月 3 日付で十分性の維持が決定され、欧州委員会による報告書(https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=COM:2023:275:FIN)が公表されるとともに、同月 4 日には個人情報保護委員会及び欧州委員会双方から当該レビューが完了した旨が公表された(なお、日本は、2023 年 3 月 22 日、EU 及び英国を日本と同等の水準にあると認められる個人情報保護制度を有している外国とする指定を継続する旨を決定していた)。その際、当初の十分性認定は、捜査機関を含む官民組織や地方組織を一元的に適用対象とする令和 3 年個人情報保護法改正が行われる前に出されたものであったところ、欧州委員会からは、公的機関も個人情報保護法の一元的な適用対象とすることを歓迎する旨が示された(欧州委員会による報告書 2.の記載も参照)。今後、本報告書で提示した様々な論点について、日本の捜査機関による個人情報の取扱いが GDPR 上の要請を満たすものであることを前提とした、更なる議論の進展が期待される。

214 Crime Overseas Production Orders Act 2019 (COPOA).

215 Telecommunications Legislation Amendment (International Production Orders) Act 2021.

第7. 企業における透明性確保の現状と今後の方向性

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、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も重要となる。例えば、OECD ガバメントアクセス宣言(前記**コラム①参照**)においても、民間部門によるガバメントアクセス要請についての集計レポートが、ガバメントアクセスに関する透明性確保に資するものとして位置づけられている。

実際、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、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。

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
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
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
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

他方で、2020 年 4 月、一般財団法人情報法制研究所(JILIS)は、捜査機関から捜査関係事項照会を受けた場合の事業者の対応に必要となる考え方を定めたガイドラインを公表した[216]。また、個々の企業を見ても、日本の捜査機関から情報開示の要請を受領した場合の対応方針を策定し、透明性レポートとは別に公表している例があり、そこでは、以下のような開示方針等が記載されている(なお、以下の表における「企業 A」から「企業 E」は、上記透明性レポートの公表事例の表と対応するものではない。)。

216 一般財団法人情報法制研究所(JILIS)捜査関係事項照会問題研究タスクフォース「捜査関係事項照会対応ガイドライン」(令和 2 年 4 月 11 日第 1 版作成)(https://www.jilis.org/proposal/data/sousa_guideline/sousa_guideline_v1.pdf)
捜査関係事項照会を受けた場合における基本的な考え方として、事業者が、①捜査関係事項照会が形式的に適法になされているか、②捜査機関に提供をする情報が捜査との関連性を有するか、を検討した上で、捜査機関に対し、必要かつ相当な報告を行うものとすることが規定されている(4.1.1 参照)。

社名	開示方針の概要
企業 A	・ 令状に基づく場合 ・ 通信の秘密に該当する情報について、緊急避難が成立すると認められる事案において開示要請を受領した場合 ・ 通信の秘密に該当しない情報について、捜査関係事項照会を受けた場合で、開示が同企業に課される法的義務に抵触しない場合
企業 B	・ 令状に基づく場合 ・ 一部の情報について、開示要請を受領した場合で、開示の必要性及び相当性が認められる場合
企業 C	・ 令状に基づく場合 ・ 開示要請を受領した場合で、合理的な理由がある場合
企業 D	・ (原則として)令状に基づく場合
企業 E	・ 令状に基づく場合 ・ 一部の情報について、捜査関係事項照会を受けた場合で、生命・身体・財産の保護等に対する急迫性・公益性、かつ緊急性が認められる場合

こうした政府機関からの開示要請に対する対応状況や対応方針の公表等については、日本企業においても、徐々に浸透しつつある。今後もこうした取組を推進し、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より一層可能になると考えられる。このような取組は、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に対する信頼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。具体的な取組を検討する際には、透明性レポート又は(国内外の)捜査機関による情報開示要請への対応方針の在り方について、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。

＝＝

コラム③：改正電気通信事業法に基づくガバメントアクセスを巡る透明性の確保[217]

改正電気通信事業法は、指定電気通信事業者に対し、「特定利用者情報」の取扱方針を定め、公表する義務を規定した[218]。当該取扱方針には、取得する特定利用者情報の内容及び

217 日本以外の政府機関等による関与の透明性を広く確保する観点からは、コンテンツモデレーションに対する透明性確保を巡る総務省等における議論のほか、経済安全保障推進法上の特定重要設備の導入等における審査制度や、景品表示法上のステルスマーケティング規制等も、関連性を有する政策動向として留意する必要がある。

218 改正電気通信事業法 27 条の 5、27 条の 8 第 1 項、改正電気通信事業法施行規則 22 条の 2 の 23。

利用目的・方法のほか、安全管理の方法、過去 10 年間に生じた「特定利用者情報」の漏えい事案[219]の時期及び内容の公表等に関する事項を記載することが義務付けられているため、外国の制度に従って外国政府に提供した特定利用者情報に関する情報も公表され得る。このように、日本では、(個人情報保護法上の個人データ(や個人関連情報)の越境移転に対する同意の取得のための情報提供の仕組みも含めて)外国政府による日本に所在する利用者の情報へのアクセス状況に関する透明性を確保する仕組みが導入されつつあるが、今後、本報告書の検討も踏まえ、この仕組みの対象に CLOUD Act に基づく行政協定を用いた開示要請も含まれるのかや、特定利用者情報以外の情報についても同様の仕組みを整備すべきかといった点に関する議論が更に深まることが期待される。

＝＝

219 「特定利用者情報」の漏えいに関する電気通信事業法の改正内容については、前記**第 6.の 2.(2)ア**を参照されたい。

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)、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(日米デジタル貿易協定)といった最新の国際通商ルールにおいても、データの国境を越えた自由な移転という基本原則が具体化されている [220]。加えて、現在も、WTO における電子商取引交渉(Joint Statement Initiative on E-commerce)や、日 EU EPA における「データの自由な流通に関する規定」を同協定に含めることについての交渉といった様々なフォーラムにおいて、国境を越えたデータの移転に関するルールの在り方が協議されている [221]。

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、(個々の事業者においてそうした懸念に配慮した新しいサービスや取組を実施していくことは妨げられるべきものではないものの)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政策が広がることになり、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 [222]。

2. 国際的枠組みを有志国間で構築していくことの意義

I&JPN(前記**コラム②**参照)の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 の電子証拠規則案及び指令案並びに③サ

---

220 このほか、地域的な包括的経済連携協定(RCEP)でも、同基本原則が具体化されている。同協定は一方で、締約国に対して、データの越境移転を制限する措置を講じることについての裁量を CPTPP 等よりも広く認めており、規律のレベルは本文で挙げた各協定よりも低くなっている。また、具体的な内容はまだ明らかとはなっていないが、現在ルール作りに向けた議論がなされているインド太平洋経済枠組み(IPEF)においても、デジタル貿易の前進に向けた取組として、信頼性がありかつ安全な越境データフローを促進・支援することとされている(*MINISTERIAL TEXT FOR TRADE PILLAR OF THE INDO-PACIFIC ECONOMIC FRAMEWORK FOR PROSPERITY: Indo-Pacific Economic Framework for Prosperity (IPEF): Part 1 - Trade*, *available at* https://www.mofa.go.jp/files/100391688.pdf)。

221 以上のデジタル貿易形成に向けた動向については、中川淳司・米谷三以編著『国際経済ルールの戦略的利用を学ぶ』127-142 頁〔小松正明〕(2022)等参照。

222 藤井康次郎「Data Free Flow with Trust 構想とクラウド法－近時の経済連携協定デジタル貿易規律の概観と『クラウド法報告書』の紹介」日本国際経済法学会年報第 29 号 56 頁(2020)。御巫智洋「インターネットの利用に関する国際的なルールにおいて領域主権が果たす機能」国際法外交雑誌 121 巻第 1 号 1 頁、14 頁脚注 38(2022)も同旨。

イバー犯罪条約の追加議定書案の 3 つを提示している[223]。

EU の電子証拠規則案及び指令案は、単独の(ユニラテラルな)法的枠組みにより、立法管轄権が及ぶ範囲のサービスプロバイダに対して提出命令等に応じる義務を課すとともに、当該サービスプロバイダが EU 域内に所在しない場合には、域内に代理人を指定する義務を課すことで執行管轄権行使の実効性を担保しようとするものである。もっとも、域外のサービスプロバイダがその義務に反して域内に代理人を設置しない場合には、執行管轄権を行使できない等の限界はある。

他方で、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、2022 年 5 月に署名されたサイバー犯罪条約第二追加議定書については、早期の批准を目指すべきである。もっとも、第二追加議定書においては、他の締約国に所在するドメインレジストラに対するドメイン名登録情報の開示要請及び他の締約国に所在するサービスプロバイダに対する加入者情報の開示命令までしか認められておらず、これを超えた、他の締約国に所在するサービスプロバイダに対するコンテンツデータの開示命令等について多国間の合意に至るには、相当な時間を要することが予想される。

そこで当面の間は、まさに DFFT の精神に倣い、価値観を共有する有志国間で先行して、CLOUD Act が想定する行政協定のような、二国間(又は複数国間)での枠組みを着実に作っていくことが、迅速性や実現性の観点からは効果的であると考えられる[224]。前記**第 3. の 1. (2)** に記載のとおり、既にこうした枠組みが形成されつつある状況にあるが、複雑化するサイバー犯罪やサイバーセキュリティ上のリスク、地政学的な影響も踏まえると、こ

---

223 Internet & Jurisdiction Policy Network: *Concrete Proposals for Norms, Criteria and Mechanisms: Operational Approaches* (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。

224 このように、多国間の国際的な枠組みであるサイバー犯罪条約第二追加議定書に加えて、CLOUD Act に基づく行政協定のような有志国間での枠組み作りを進めようとする場合、両者の適用関係を整理し、両者の適用がある場面において抵触関係が生じる可能性がないか、生じる可能性がある場合には、どのように調整を行うかについて検討をしておく必要がある。

例えば、サイバー犯罪条約第二追加議定書は、14 条において個人情報の保護措置に関する詳細な義務を定めているため、仮にある国との行政協定において提出要請国の法令に従って個人情報が保護される旨が規定されているにとどまる場合(例えば、米豪行政協定 3 条 4 項はそのような規定振りとなっている。)であっても、当該国がサイバー犯罪条約第二追加議定書の締約国でもある場合には、当該国に所在する者から開示されたドメイン名登録情報(第二追加議定書 6 条)や登録者情報(同 7 条)については、サイバー犯罪条約第二追加議定書 14 条が定める水準の個人情報保護措置を設ける必要がある。そのため、少なくともドメイン名登録情報や登録者情報の提出に関しては、それが行政協定に基づいて行われる場合であっても、サイバー犯罪条約第二追加議定書 14 条に定める水準の個人情報保護措置が適用されるように関連国内法を整備する必要がないかについて検討が必要となる。

他方で、第二追加議定書加盟国の事業者から、行政協定に基づいて非加盟国に対してデータが開示等される場面では、第二追加議定書の適用はないため、上記のような問題は生じない。

のような枠組み作りが進み、国際的に相応に受け入れられたものが作られていくことは、日本のサイバー・経済安全保障戦略の構築・実践に寄与する側面もあるように思われる。

したがって、日本としては、これらの観点からも、CLOUD Act が想定しているような二国間(又は複数国間)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。また、この際に、いかなる国が、価値観を共有する「有志国」として、そのような二国間(又は複数国間)の国際協定を締結する候補となるかの判断にあたっては、OECD ガバメントアクセス宣言(前記**コラム①参照**)のような国際的に認められた原則を共有する国であるか否かという観点から検討することも有益であると考えられる。

以　上