성균관대학교 법학연구원『성균관법학』 10.17008/skklr.2023.35.1.014
제35권 제1호(2023. 3.)
Sungkyunkwan Law Review Vol.35 No.1 (March 2023) pp. 513 - 541

サイバー犯罪条約の第二追加議定書による サイバー犯罪捜査の変化* **

中村真利子***

【目 次】

* 本稿は、2022年12月10日（土）に成均館大学校で開催された「スマートシティ法制国際共同学術大会」（主催：成均館大学校法学研究院）において発表した報告原稿を加筆・修正したものである。お招きいただいた成均館大学校・李京烈教授、司会の成均館大学校・金奇範教授、討論者の檀国大学校・李定玟教授に感謝申し上げたい。

** なお、本稿は、JSPS科研費21K13208及び中央大学2022年度特定課題研究費の助成を受けたものである。

*** 中央大学国際情報学部准教授・博士（法学）

【要 旨】

サイバー犯罪に関する国際的な取決めである欧州評議会の「サイバー犯罪に関する条約」は、サイバー犯罪の捜査を実効的なものとすることを目指すもので、日本もこの条約を受けて国内法を整備したが、特に国境を越えるデータの押収については課題も多く残されている。そこで、欧州評議会は、データの押収に関する国際協力を強化するため、「協力及び電子的証拠の開示の強化に関するサイバー犯罪に関する条約の第二追加議定書」を新たに策定した。日本も、2022年５月に行われた署名開放式典でこれに署名したことから、本稿では、この第二追加議定書の内容を受け入れることによって、サイバー犯罪捜査が今後どのように変わり得るか検討した。関連して、新しい国際協力の枠組みとして注目されているアメリカ合衆国のCLOUD法（Clarifying Lawful Overseas Use of Data Act）と、2022年10月に施行されるに至ったイギリスとの行政協定も紹介し、このような二国間での行政協定の可能性についても論じた。

Ⅰ　はじめに

サイバー犯罪に関する国際的な取決めである欧州評議会の「サイバー犯罪に関する条約」（以下、「サイバー犯罪条約」という。）は、サイバー犯罪の捜査を実効的なものとするため、締約国に対して、自国の当局によるデータの提出命令を行う権限を付与するための国内法の整備を求めるとともに（サイバー犯罪条約18条）、「蔵置されたコンピュータ・データに対する国境を越えるアクセス」についても定めている（サイバー犯罪条約32条）。

日本は、これらを受けて、2011年の改正により記録命令付差押え（刑訴法218条１項）及びリモートアクセス捜査（刑訴法218条２項）を導入した。もっとも、記録命令付差押えについては、記録命令の対象は国内のプロバイダであることはもちろんのこと、そのプロバイダのサーバが国外にある場合に、国外に蔵置されているデータを捜査機関に開示することが国家主権との関係でどのように考えられるか、必ずしも明らかではない。また、リモートアクセス捜査は、必要なデータが蔵置されているサーバを特定することなく、差押対象物であるコンピュータからサーバにアクセスし、必要なデータを差し押さえることを可能とする捜査手法であるが、サーバが国内にあるとは限らないことから、同様に主権の問題が生じ得る。

少なくともサイバー犯罪条約の締約国に関しては、このような問題についてあらかじめ合意が形成されることが望ましいと思われるところ、欧州評議会は、データの押収に関する国際協力を強化するため、「協力及び電子的証拠の開示の強化に関するサイバー犯罪に関する条約の第二追加議定書」（以下、「第二追加議定書」という。）を新たに策定した。日本も、2022年５月の署名開放式典においてこれに署名したことから、今後、その内容が国会に提出されることになる。そこで、本稿では、現行法に規定のある記録命令付差押え及びリモートアクセス捜査に関して生じ得る問題を概観し、第二追加議定書に対応することによってサイバー犯罪捜査がどのように変わり得るか検討したい。

また、アメリカ合衆国でも、自国のプロバイダに対してデータの提出を

求める開示命令に関して、そのデータが国外のサーバに蔵置されている場合に、開示命令の効力が及ぶかが問題となった事件をきっかけとして、2018年に、このような場合も開示命令の対象となることを明らかにするCLOUD法（Clarifying Lawful Overseas Use of Data Act）が制定された。注目されるのは、自国のプロバイダが、行政協定を締結した外国に対して一定の情報を開示することを認める規定が置かれていることである。2019年にはイギリス、2021年にはオーストラリアとの間で行政協定が締結されており、このような枠組みは、数年かかることもあるといわれる国際捜査共助に代わる新たな国際協力の形として期待される。そこで、このような行政協定の可能性についても検討する。

Ⅱ 国境を越えるデータの押収と課題

サイバー犯罪条約は、2001年11月に採択、署名され、2004年７月に批准国の条件を満たして効力が発生した。日本もこれに署名し、2004年４月に国会で承認されたが、2012年７月の受託書寄託、公布及び告示を経て、日本について効力が発生したのは同年11月のことであった。この間、国内法の整備が進められ、2011年の改正（2012年６月施行）によって、記録命令付差押え（刑訴法218条１項）及びリモートアクセス捜査（刑訴法218条２項）が導入された。これらの新しい捜査手法によって、サイバー犯罪の捜査において重要な証拠となるデータの押収が効率化、迅速化されることになったが、対象のデータが他国のサーバに蔵置されている場合に、当該他国の主権との関係をどのように考えるかについて、刑事訴訟法、国際法の観点から様々な議論がなされている。そこで、本章では、記録命令付差押え及びリモートアクセス捜査の導入経緯とその概要を確認するとともに、それぞれの課題について検討する。

１ 記録命令付差押え

サイバー犯罪条約は、締約国に対して、自国の当局がデータの提出命令を行う権限を付与するための国内法の整備を求めている（サイバー犯罪条約18条）。具体的には、①「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蔵置されたものを提出するよう命令すること」、②「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」が、その権限の内容である。このうち①を担保するためのものが記録命令付差押え（刑訴法218条１項）である。

記録命令付差押えとは、「電磁的記録を保管する者その他電磁的記録を利用する権限を有する者に命じて必要な電磁的記録を記録媒体に記録させ、又は印刷させた上、当該記録媒体を差し押さえること」をいう（刑訴法99条の２）。必要なデータが保管されている記録媒体を特定することが困難な場合や、その操作に専門的な知識・技術を要する場合に、処分を受ける者に対して、必要なデータのコピーやプリントアウトを命じることができるというものである。被処分者はこれに応じる義務を負うものの、義務違反に対する罰則はないことから、プロバイダといった、令状があれば協力的であると考えられる被処分者が想定されているが、必要なデータが保管されているサーバを管理しているプロバイダさえ判明すれば良いという点では、簡便なデータの押収方法といえる。

もっとも、プロバイダが管理するサーバが国外にある場合に、物理的な捜査と同様、国家主権との関係で、このような記録命令付差押えが制限されることになるかが問題となる。この点、サイバー犯罪条約18条で掲げられている前述の①の対象となる者の範囲は「自国の領域内に所在する者」である。「保有し又は管理している」というのは、データが保管されている記録媒体を自国の領域内で物理的に保有している場合だけではなく、自国の領域内から正当な権限に基づいてデータの提出を自由に管理できる状況にある場合も含まれると注釈されており[1]、提出命令の対象となるデータが他国にある場合も想定されている。

立法担当者によると、「記録命令付差押えが我が国に所在する者に対し

1) Council of Europe, Explanatory Report to the Convention on Cybercrime, https://rm.coe.int/16800cce5b, last accessed 2022/11/25 (hereinafter “Explanatory Report (1)”) at 29 (paragraph 173).

て行われ、その者が対象となる電磁的記録を保管又は利用する権限を有する限り、当該電磁的記録が外国に所在するサーバ等の記録媒体に記録されている場合であっても、記録行為自体は、その命令を受けた者によって行われるものであり、これにより記録された他の記録媒体を捜査機関が差し押さえたとしても、外国の主権を侵すものとは考えられない。」とのことである[2]。ただし、捜査機関の命令に基づいて行われる以上、主権侵害の可能性は否定できないことから、サイバー犯罪条約18条は、対象となるデータが他国にある場合にも提出命令が可能であることを締約国が合意したものであるとも考えられる[3]。もっとも、このように解すると、サイバー犯罪条約の締約国以外との関係では、なお記録命令付差押えと国家主権について考える必要があると思われる。

2 リモートアクセス捜査

サイバー犯罪条約はまた、「蔵置されたコンピュータ・データに対する国境を越えるアクセス」についても定めている（サイバー犯罪条約32条）。具体的には、①「公に利用可能な蔵置されたコンピュータ・データにアクセスすること（当該データが地理的に所在する場所のいかんを問わない。）。」、②「自国の領域内にあるコンピュータ・システムを通じて、他の締約国に所在する蔵置されたコンピュータ・データにアクセスし又はこれを受領すること。ただし、コンピュータ・システムを通じて当該データを自国に開示する正当な権限を有する者の合法的なかつ任意の同意が得られる場合に限る。」のいずれかに当たる場合に、他の締約国の許可なく越境アクセスできるとされている。

これを国内法において具体化したものがリモートアクセス捜査（刑訴法218条２項）である。これは、差し押さえるべき物が電子計算機である場合に、「当該電子計算機に電気通信回線で接続している記録媒体であつて、当該電子計算機で作成若しくは変更をした電磁的記録又は当該電子計

2) 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1049頁、1068頁（注６）（2012年）。

3) 川出敏裕「コンピュータ・ネットワークと越境捜査」酒巻匡ほか編『井上正仁先生古稀祝賀論文集』（有斐閣、2019年）414頁。

算機で変更若しくは消去をすることができることとされている電磁的記録を保管するために使用されていると認めるに足りる状況にあるものから、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こと」をいう。

必要なデータが蔵置されているサーバ等の記録媒体を特定して差し押さえるというのではなく、差押対象物であるコンピュータにネットワークで接続しているサーバ等の記録媒体にリモートアクセスし、そのコンピュータで作成・変更したデータや、そのコンピュータから変更・消去できるようなデータを、そのコンピュータやCD-R等の記録媒体にコピーした上で、これを差し押さえることができるようになった。リモートアクセス捜査によれば、わざわざサーバを物理的に特定し、捜査機関がその場所に行って差し押さえる必要がないことから、非常に利便性の高い捜査手法といえる。

もっとも、サイバー犯罪条約32条においては、前述の①及び②以外の場合については規定されるに至っていないこともあり[4]、利用者の同意が得られない場合に、国境を越えてリモートアクセス捜査を行うことができるかが問題となる。東京高判平成28年12月７日高刑集69巻２号５頁[5]は、サーバが国外にある可能性がある場合について、「捜査機関としては、国際捜査共助等の捜査方法を取るべきであったともいえる」としており、これは、立法担当者の「一般には、電磁的記録を複写すべき記録媒体が他国の領域内にあることが判明した場合において、［サイバー犯罪］条約第32条によりアクセス等をすることが許されている場合に該当しないときは、当該他国の主権との関係で問題を生じる可能性もあることから、この処分を行うことは差し控え、当該他国の同意を取り付けるか、捜査共助を要請することが望ましいのではないかと考えられる」[6]との見解とも一致する

4)　Explanatory Report (1) at 53 (paragraph 293).

5)　この判決の紹介・解説として、山内由光・研修832号13頁（2017年）、宇藤崇・法学教室445号152頁（2017年）、四方光・刑事法ジャーナル58号143頁（2018年）、笹倉宏紀・平成29年度重要判例解説182頁（2018年）、星周一郎「サイバー空間の犯罪捜査と国境・覚書き」警察学論集73巻４号71頁（2020年）がある。

6)　杉山=吉田・前掲注２、1095頁。

ように思われる。

しかし、サーバが他国に設置されていること、あるいはどこの国にあるのかさえわからないことは珍しいことではない。また、同意を得るべき利用者は被疑者であることも多く、リモートアクセス捜査を認めることによって自己に不利益なデータが押収されてしまう可能性があることから、同意が得られないことも十分に考えられる。国内のプロバイダが管理するサーバであっても、必ずしも国内にあるとは限らない以上、サーバが外国にある可能性があるというにとどまる場合にまで国際捜査共助によるべきということになると、実質的にリモートアクセス捜査の道が閉ざされてしまうことにもなりかねない。そこで、少なくとも、利用者が普段からIDやパスワードのほかは特に制限なくアクセスできる領域についてのみリモートアクセス捜査が行われる場合、国家主権の問題は生じないとの考え方も示されている[7]。このような場合、具体的な嫌疑を前提とした捜索差押許可状の発付を受けてリモートアクセス捜査を実施することから、利用者の権利・利益に関しては司法審査を経ているといえ、特に他国やそのプロバイダに何かを要求したり、その国民を含む利用者を常に監視したりするような態様は考えにくいからである。

また、国内の証拠法の問題として、相手国が越境リモートアクセス捜査を認識し、これを国際法上違法であると評価する場合はさておき、サーバが他国に設置されている可能性があるというにとどまる場合には、国内の刑事裁判において適用される証拠法には影響を与えないとの見解もある[8]。判例は、違法に収集された証拠について、その証拠能力を否定する違法収集証拠排除法則を採用しているものの、証拠排除の基準としては、

---

7) 例えば、川出敏裕「サイバー犯罪の捜査」警察学論集71巻9号157頁、174頁（2018年）、四方・前掲注5、148頁-150頁、中野目善則「サイバー犯罪の捜査と捜査権の及ぶ範囲―プライヴァシーの理解の在り方、法解釈の在り方、他国へのアクセスの及ぶ範囲等の観点からの検討」警察政策22巻130頁、134頁-142頁、147頁-154頁（2020年）、星・前掲注5、81頁-86頁。

8) 裁判例としては、大阪高判平成30年9月11日高刑速（平30）344頁がある。この判決の紹介・解説として、栗田理史・研修849号25頁（2019年）、指宿信・新判例解説Watch24号187頁（2019年）、宇藤崇・法学教室462号157頁（2019年）、中島宏・法学セミナー768号130頁（2019年）、深野友裕・警察学論集72巻4号151頁（2019年）、星・前掲注5がある。

「証拠物の押収等の手続に、憲法35条及びこれを受けた刑訴法218条１項等の所期する令状主義の精神を没却するような重大な違法があり、これを証拠として許容することが、将来における違法な捜査の抑制の見地からして相当でないと認められる場合においては、その証拠能力は否定される」との立場をとっている[9]。

最高裁判所が初めてリモートアクセス捜査に関して判断した最（二小）決令和３年２月１日刑集75巻２号123頁[10]では、対象となるサーバが国外にある可能性があったことから、関係者の同意を得てリモートアクセス捜査が実施されたものの、この同意について任意性があるとはいえないと判断された。そうすると、サイバー犯罪条約32条で掲げられている前述の②の範囲（「合法的なかつ任意の同意」という部分）を超えることになるが、最高裁判所は、「電磁的記録を保管した記録媒体が同条約の締約国に所在し、同記録を開示する正当な権限を有する者の合法的かつ任意の同意がある場合に、国際捜査共助によることなく同記録媒体へのリモートアクセス及び同記録の複写を行うことは許されると解すべきである。」と指摘するのみで、重大な違法を認めなかった。

法廷意見では国家主権への言及はないものの、法廷意見に参加した三浦守裁判官の補足意見は、「本件においては、……リモートアクセスの対象である記録媒体は、日本国外にあるか、その蓋然性が否定できないものであって、〔サイバー犯罪〕条約の締約国に所在するか否かが明らかではないが、このような場合、その手続により収集した証拠の証拠能力については、〔法廷意見〕の説示をも踏まえ、権限を有する者の任意の承諾の有

9)　最（一小）判昭和53年９月７日刑集32巻６号1672頁。

10)　この決定の紹介・解説として、前田雅英・WLJ判例コラム227号（2021年）、田中優企・法学教室490号149頁（2021年）、四方光・法学教室491号75頁（2021年）、星周一郎・刑事法ジャーナル69号264頁（2021年）、吉戒純一・ジュリスト1562号98頁（2021年）、川出敏裕・論究ジュリスト37号121頁（2021年）、指宿信・Law & Technology 92号40頁（2021年）、同・Law & Technology 93号32頁（2021年）、岩崎正・新判例解説Watch 29号225頁（2021年）、大橋充直・捜査研究848号56頁（2021年）、中野目善則・令和３年度重要判例解説147頁（2022年）、水谷恭史=関口和徳・季刊刑事弁護109号140頁（2022年）、横山裕一・日本大学法科大学院法務研究19号95頁（2022年）がある。国際法の観点から紹介・解説するものとしては、例えば、竹内真理・令和３年度重要判例解説249頁（2022年）参照。

無、その他当該手続に関して認められる諸般の事情を考慮して、これを判断すべきものと解される。」と付言している。したがって、たとえ主権侵害の可能性があったとしても、少なくとも、サーバが国外にある可能性があるというにとどまる場合には、そのことだけでは、リモートアクセス捜査によって入手されたデータの証拠能力を否定すべきほどの重大な違法はないと考えることもできそうである[11]。

主権の問題が国内の刑事裁判に直接影響を与えるとは考えにくい上、捜査機関が、リモートアクセス捜査を許可する令状に基づいて他国のサーバにアクセスする場合や、相手方の同意を得てリモートアクセス捜査をしようとする場合、「令状主義の精神を没却するような重大な違法」を排除の基準とし、捜査機関の態度や抑止効を総合的に考慮する判例の立場からは、証拠排除という結論につながる可能性は低いようにも思われる。もっとも、相手国がこのような越境リモートアクセス捜査を認識し、これを国際法上違法であると評価する場合には、違法収集証拠排除法則にいう重大な違法が認められる可能性のほか[12]、主権侵害の原状回復措置としてのデータの破棄の結果、これを証拠として利用できなくなる可能性[13]や、違法収集証拠排除法則とは別の「手続的正義」の観点から証拠能力が否定される可能性[14]も指摘されている。

Ⅲ 第二追加議定書の概要[15]と展望

サイバー犯罪条約は、締約国に対してデータの捜索・押収手続の整備を求めるものであり、その締約国に限られるとはいえ、サイバー犯罪対策に

11) 笹倉・前掲注5、183頁、山内・前掲注5、21頁-22頁、川出・前掲注7、174頁、深野・前掲注8、163頁、早乙女宜宏「リモートアクセスによる差押えに伴う問題点の一考察」日本大学法科大学院法務研究16号67頁、67頁-68頁（2019年）。

12) 川出・前掲注3、430頁。

13) 芝原邦爾ほか編『経済刑法―実務と理論』（商事法務、2017年）572頁〔笹倉宏紀〕。

14) 指宿・前掲注8、189頁-190頁。

15) 本稿における第二追加議定書の和訳は、2022年5月12日付けで外務省から公開されている和文（仮訳文）による。外務省「『協力及び電子的証拠の開示の強化に関するサイバー犯罪に関する条約の第二追加議定書』への署名」（仮訳文）、https://www.mofa.go.jp/mofaj/files/100342968.pdf、2022年11月25日最終閲覧。

関する国際協力を推し進めることになった。もっとも、合意が形成しやすい部分について優先的に取りまとめられたため、前章でみたように、特に国境を越えるデータの押収に関して限界があることは否めないところである。このようななか、欧州評議会は、データの押収に関する国際協力をさらに強化するために第二追加議定書を策定し、これが2021年11月に採択され、2022年５月に署名開放式典が行われた。日本も21か国の代表とともに署名し、今後、その内容に応じた国内法の整備が進められることになると思われる。そこで、本章では、第二追加議定書のうちデータの押収に関する部分を概観し、従来のサイバー犯罪捜査がどのように効率化、迅速化され得るのか考えてみることとしたい。

1　他の締約国におけるプロバイダ及び団体との直接の協力を強化する手続

第二追加議定書の第２章第２節には、他の締約国におけるプロバイダ及び団体との直接の協力を強化する手続に関する規定が置かれている。具体的には、①他の締約国の領域内に所在するドメイン名の登録サービスを提供する団体に対して、ドメイン名の登録者を特定し、又は当該者と連絡するための情報の要請を発する権限（第二追加議定書６条１項）、及び②他の締約国の領域内に所在するプロバイダに対して、蔵置された加入者情報の開示を得るための命令を直接発する権限（第二追加議定書７条１項）を自国の当局に与えるための立法措置をとるべきことを定めている。これらは、前述のような課題に照らし、電子的証拠に対する時宜に適った越境アクセスの重要性が認識された結果として規定されたものである[16]。反対に、他の締約国から国内の団体又はプロバイダに対してドメイン名の登録情報の要請又は加入者情報の開示命令がなされる場合もあり得るため、これら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が求められることになる（第二追加議定書６条２項、７条２項a）。

①ドメイン名の登録情報の要請（第二追加議定書６条１項）は、ドメイ

16) Council of Europe, Explanatory Report to the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence, https://search.coe.int/cm/pages/result_details.aspx?objectid=0900001680a48e4b, last accessed 2022/11/25 (hereinafter “Explanatory Report (2)”) at paragraph 72.

ン名を入手することが、捜査における最初の一歩として必要不可欠であることが多いことが考慮されたものである。ドメイン名は、マルウェア、ボットネット、フィッシング等の拡散、詐欺（fraud）、児童ポルノ（child abuse materials）の頒布その他の犯罪のためのプラットフォームとして利用されることがある。したがって、ドメイン名の登録者の情報にアクセスすることは、被疑者を特定するために重要となる。このような情報は、ドメイン名の登録サービスを提供する団体が保有しており、例えば、「.com」や「.jp」といったトップレベルドメインの登録管理組織（レジストリ）や、この組織と契約してドメイン名を販売する登録事業者（レジストラ）がこれに当たる。このような情報は個人情報として保護され、アクセスが制限される場合もあることから、ドメイン名の登録者を特定し、又はこれと連絡をとるために必要な情報を入手する効果的かつ効率的な枠組みを提供することを目的として、この規定が制定された[17]。

要請をするにあたっては、情報を求めるドメイン名及び求める情報（例えば、登録者の名前、住所、メールアドレス、電話番号）の詳細な一覧や、情報を開示すべき期限及び方法その他特別な手続上の指示（例えば、登録者又は第三者に対する当該要請の非開示要請）等が提供される（第二追加議定書６条３項）[18]。この要請は、相手方の団体が受け入れる場合には、メールといった電子的な形式によることが認められる（第二追加議定書６条４項）。この方法が最も効率的かつ迅速と思われるからであるが、適当な水準のセキュリティと認証が求められることから、安全なチャネルが利用可能かどうかを確認したり、暗号化といった特別なセキュリティ保護が必要かどうかを判断する必要がある[19]。ドメイン名の登録情報に関しては、開示の「命令」ではなく「要請」をすることになっているが、相手方が協力しない場合には、求める情報を開示しない理由を示すよう要請することもできる（第二追加議定書６条５項）。「命令」ということになれば、締約国がこの規定を適用しない権利を留保することができる旨の規定も設けられることになると推測されることから、比較的弱い「要請」にす

17) Explanatory Report (2) at paragraphs 73-76.

18) Explanatory Report (2) at paragraph 84.

19) Explanatory Report (2) at paragraph 86.

ることで、国際協力の強化を促進しようとしたのではないかと思われる。

②加入者情報の開示命令（第二追加議定書７条１項）は、サイバー犯罪条約18条を補完するものである。従来型の国内における犯罪でさえ、国外のプロバイダが保有している電子的証拠が必要となる場合がある。相互援助（国際捜査共助）のような手続によることは、このような電子的証拠を求める要請の増加から、必ずしも迅速又は効果的な援助を提供するものとはいえない。加入者情報は、電子的証拠が必要となるような犯罪の捜査において最もよく求められる情報であるが、それは、内容にかかわるわけではないとはいえ、加入者の身元、住所等の情報を提供するものであるからである。この規定は、サイバー犯罪条約18条の限界を超えるという趣旨から、他の締約国の領域内にあるプロバイダに対して命令を発することを認める内容となっている[20]。通常、捜査機関が国外においてその権限を行使することは、国家主権の関係で許されないが、現行の記録命令付差押えに相当する捜査手法を、直接、国外のプロバイダを対象としてとることができるようになるということである。

この命令には、捜査の対象となっている犯罪や求める特定の加入者情報についての詳細な説明等を明記するとともに（第二追加議定書７条３項）、同時に又は別途、加入者情報を返送すべき期限及び方法や特別な手続上の指示（例えば、加入者又は第三者に対する当該命令の非開示要請）等の補足的な情報が添付される（第二追加議定書７条４項）[21]。相手方のプロバイダが受け入れる場合には、この命令及び補足的な情報を電子的な形式で提供することができる（第二追加議定書７条６項）。

プロバイダに対する「命令」ということもあり、締約国は、自国のプロバイダにこれが発せられる場合には、欧州評議会事務局長からの通報を求め、又は特定の状況（例えば、自国の捜査に影響を及ぼすおそれがある場合）においてプロバイダに対して自国の当局と協議するよう要求することができ、一定の場合に、加入者情報を開示しないようプロバイダに指示することが認められている（第二追加議定書７条５項）。一種のセーフガー

20) Explanatory Report (2) at paragraphs 90-95.

21) Explanatory Report (2) at paragraphs 105-106.

ドを設けることができるわけであるが、広範な協力が原則であることから、電子的証拠に対するより効果的かつ迅速な越境アクセスのための手続を提供するため、このような妨害は厳しく制限されることになる[22]。締約国は、第二追加議定書７条の規定を適用しない権利を留保することもできるが（第二追加議定書７条９項a）、この場合、他の締約国のプロバイダに対して命令を発することは許されない[23]。

プロバイダが加入者情報の開示を拒否する場合には、その理由を示すよう要請することができるほか、プロバイダが求められた加入者情報を開示しないと通知する場合、又は命令の受領から30日以内若しくは指定された期限までのいずれか長い方の期間内に命令に応じない場合には、次にみる蔵置されたコンピュータ・データの開示のための当局の間の国際協力を強化する手続に関する規定又は他の形態の相互援助によって、当該命令の執行を求めることになる（第二追加議定書７条７項）。なお、プロバイダに対して加入者情報を開示しないよう指示があった場合であっても、命令の執行を求めることはできるが、同じ内容では応じてもらえない可能性が高いので、あらかじめ相手国の当局に相談することが望ましいとされている[24]。加入者情報に関しては、第二追加議定書８条の規定による開示を求める前に、第二追加議定書７条の命令によるべきことが宣言されることもある（第二追加議定書７条８項）。

2 蔵置されたコンピュータ・データの開示のための当局の間の国際協力を強化する手続

第二追加議定書の第２章第３節には、蔵置されたコンピュータ・データの開示のための当局の間の国際協力を強化する手続に関する規定が置かれている。具体的には、他の締約国に対する要請の一部として、当該他の締約国にあるプロバイダに対して加入者情報又は通信記録を提出するよう強制するための命令を発する権限を自国の当局に与えるとともに（第二追加

22) Explanatory Report (2) at paragraphs 108, 110.

23) Explanatory Report (2) at paragraph 122.

24) Explanatory Report (2) at paragraph 120.

議定書８条１項）、他の締約国からこのような要請を受けた場合に、その命令を執行するために必要な立法措置をとるべきことを定めている（第二追加議定書８条２項）。命令は提出命令やサピーナ（subpoena）といった形式を問わず、法律上、加入者情報又は通信記録の提出を強制する目的で発せられ得るものであれば良く、これが相手国の国内法に則って執行される[25]。自国の命令を相手方に代替執行してもらう形式になることから、第二追加議定書７条の命令によるデータの開示を拒否するプロバイダからも、データの開示を期待することができると思われる。締約国は、通信記録について第二追加議定書８条の規定を適用しない権利を留保することができるが（第二追加議定書８条13項）、この場合、他の締約国に対して命令を発することは許されない[26]。

執行を要請する命令には、捜査の対象となっている犯罪や求める特定の加入者情報又は通信記録についての詳細な説明（例えば、加入者情報としては加入者の身元、住所、電話番号、支払い情報、通信記録としては通信の発信元、発信先、経路、日時、期間）等を明記するとともに、捜査されている犯罪に関する法令の規定及び適用のある刑罰、当該プロバイダが通信記録を保有し、又は管理していると信ずる理由、捜査に関連する事実の要約、加入者情報又は通信記録と捜査との関連性、加入者情報又は通信記録の保全を既に求めたかどうか、加入者情報又は通信記録を既に他の手段により求めたかどうか、及び既に求めた場合には、いかなる方法によるものかといった補助的な情報も提供するが、特別な手続上の指示（例えば、加入者に対する当該命令の非開示要請）を実行するよう要請することもできる（第二追加議定書８条３項）[27]。電子的な形式での要請も受け入れられる（第二追加議定書８条５項）。

この執行要請の規定は、サイバー犯罪条約の相互援助に関する規定を補完するメカニズムを構築することを目的としており、提供すべき情報を限定し、データを入手する過程を迅速にすることによって相互援助を合理化するものである[28]。したがって、要請を受けた締約国は、これを遅くとも

25) Explanatory Report (2) at paragraphs 126, 129.

26) Explanatory Report (2) at paragraph 147.

27) Explanatory Report (2) at paragraph 132.

45日以内にプロバイダに送達する合理的な努力をし、プロバイダに対して加入者情報は20日以内、通信記録は45日以内に回答するよう命じるとともに、これらを不当に遅滞することなく要請国に伝達することが求められる（第二追加議定書８条６項）。国外のプロバイダに対して直接命令することを認めるものではないが、要請を受けた締約国がその実施を拒否、延期したり、条件を課したりする場合（第二追加議定書８条８項）を除いて、手続の迅速化が期待される。もっとも、回答命令が発出されるまでの期間に加えて、プロバイダが回答を求められる20日、45日を待つことは、特に捜査の初期段階においては致命的ともなりかねないことから、緊急性のある場合には、その効果は限定的であるようにも思われる。

このような緊急事態に対処するべく、サイバー犯罪条約で指定される速やかな相互援助を確保するための「週７日かつ１日24時間利用可能な連絡部局」（サイバー犯罪条約35条１項）に関して、第二追加議定書では、緊急事態において、通常の相互援助によらずに、他の締約国の領域内にあるプロバイダから蔵置されたデータの迅速な開示を受けるために、自国の連絡部局から当該他の締約国の連絡部局に対して即時の援助を求める要請を発するとともに、このような要請を他の締約国から受けるにあたって必要な立法措置をとることとされている（第二追加議定書９条１項a、２項）。対象は特定の「データ」という広範な文言が用いられているが、これは、緊急事態においては、加入者情報だけではなく、蔵置されたコンテンツやトラフィックデータを通常の相互援助の要請をすることなく入手する重要性が認識されたものである[29]。締約国は、加入者情報の開示のみを求める要請を実施しないことを宣言することができ（第二追加議定書９条１項b）、この場合は、第二追加議定書７条又は８条によることになる[30]。

要請にあたっては、捜査の対象となっている犯罪並びにその法令の規定及び適用のある刑罰、緊急事態が存在し、かつ、要請するデータがそれにどのように関係するかを示す十分な事実、要請するデータについての詳細な説明、特別な手続上の指示（例えば、加入者又は第三者に対する当該要

28) Explanatory Report (2) at paragraph 125.

29) Explanatory Report (2) at paragraph 155.

30) Explanatory Report (2) at paragraph 157.

請の非開示要請）等を明記することになっている（第二追加議定書９条３項）[31]。電子的な形式での要請も受け入れられるほか、口頭での要請が受け入れられることもある（第二追加議定書９条４項）。

この規定は、緊急事態において、他の締約国の領域にあるプロバイダが保有する蔵置されたデータを迅速に入手する能力を向上させる必要性が意識されたものである。緊急事態とは、テロ攻撃の直後、病院システムを損なわせるようなランサムウェア攻撃、誘拐事件において被害者家族に身代金を要求するために用いられたメールアカウントを捜査する場合等が想定されている[32]。このような場合において、事前に通常の相互援助要請の準備をすることが求められない点で、そのメリットは大きいといえる。

Ⅳ 二国間での行政協定の可能性

アメリカでは、2018年にCLOUD法が制定されたことにより、自国のプロバイダに対する開示命令の効力が、国外のサーバに蔵置されているデータにも及ぶことが明らかとなった。日本の記録命令付差押えに相当するような捜査手法であるが、それだけではなく、CLOUD法では、人権保障の観点から信頼できる国を対象として行政協定を締結することが示唆され、自国のプロバイダが、締約国に対して一定の情報を開示することを認める規定が置かれている点が注目される。そして、2019年10月にはイギリス、2021年12月にはオーストラリアとの間で行政協定が締結され、このうちイギリスとの行政協定については2022年10月に施行されるに至っている。そこで、本章では、CLOUD法が制定された経緯を確認するとともに、アメリカとの行政協定、ひいては二国間での行政協定の可能性を探ることとしたい。

１ アメリカ合衆国におけるCLOUD法の制定

アメリカには、保管通信法（Stored Communications Act）という、政府がプロバイダからその保管に係るデータを入手する方法について規律す

31) Explanatory Report (2) at paragraph 165.

32) Explanatory Report (2) at paragraph 148.

る法律が存在し、捜査機関が、プロバイダに対してメール、通信ログ、顧客情報等のデータを提供するよう求める際には、保管通信法に従う必要がある。この保管通信法に基づいて発付された令状の効力に関して問題となり、CLOUD法が制定されるきっかけとなった事案が、マイクロソフト事件（United States v. Microsoft Corp., 584 U.S. __ (2018)）である。

FBIが、マイクロソフト社に対して、薬物取引に用いられていると思料されるアカウントのメールその他の情報を開示するよう求める令状を得てこれを執行しようとしたところ、メールについては、アイルランドのダブリンにあるデータセンターに蔵置されているとして、マイクロソフト社はこの部分について令状を無効とするよう不服を申し立てた。マジストレイトはこの申請を却下し、District Courtがこれを確認して裁判所侮辱に当たると判断したが、第２巡回区Court of Appealsは、保管通信法の効力は国外へは及ばないとして、原裁判所の判断を無効とした。これに対して上告がなされ、合衆国最高裁判所がサーシオレイライを認容したが、その後、CLOUD法の制定により立法的に解決されたことで、争訟性がなくなった（moot）と判断された。

このCLOUD法は、捜査機関に対して、アメリカ国内で営業するプロバイダに、アメリカ国外に蔵置してあるデータをアメリカ国内に移動させた上で捜査機関に開示させる権限を付与するもので、行政協定を締結した外国に対しても一定の情報を開示することを認める規定を置いている。行政協定を締結することになれば、諸外国が、時間のかかる国際捜査共助によることなく、アメリカに拠点を置くプロバイダから迅速にデータを取得できることから、国際協力の新たな枠組みとして注目される。

2 アメリカ合衆国との行政協定の概要と展望

初めて行政協定を締結することになったのはイギリスであり、その内容は2022年10月に施行された[33]。この米英間の行政協定[34]は、2019年10

33) The United States Department of Justice, Landmark U.S.-UK Data Access Agreement Enters into Force, 2022/10/3, https://www.justice.gov/opa/pr/landmark-us-uk-data-access-agreement-enters-force, last accessed 2022/11/25 (hereinafter “Immediate Release on 2022/10/3”).

34) 本稿で引用する内容は、署名された合意文書を参照したものである。The United States

月、当時のアメリカの司法長官William P. Barrとイギリスの内務大臣Priti Patelが、ワシントンD.C.の英国大使公邸で行われた式典で署名したものである。両者ともに、捜査に必要なデータへの迅速なアクセスを可能にすることによって、テロや組織犯罪、児童の搾取といった重大犯罪により適切に対処できるようになることを期待する旨の声明を出している。両国は、相手国の捜査について幅広く制限を取り除くとともに、この協定を通じたデータの開示が、データ保護に関する法にも適合することをプロバイダに保証することに合意した35)。

ただし、その捜査は重大犯罪、つまり長期３年以上の拘禁刑に当たる犯罪に関するものでなければならず、人種、性別、性的指向、宗教、種族的出身又は政治的見解に基づいて言論の自由を侵害し、又は不利益な扱いをするためにこの協定を利用してはならない。また、「命令を受ける国の者（Receiving-Party　Person）」はその対象から除外されるところ、政府機関や自国に居住する者等のほか、アメリカについては自国民や永住権のある者もこれに当たる。この協定に基づいて発せられる命令は、裁判所、裁判官、マジストレイトその他の独立した機関によって事前に審査又は監督されなければならず、指定機関が審査した上で、相手国のプロバイダに送達される。例えばアメリカの場合は、司法省の国際課（Office　of International　Affairs:　OIA）が指定機関であり、そのCLOUD法チームが、捜査機関の命令がこの協定に従ったものであるか審査、認証し、これ

Department of Justice, Agreement between the Government of the United States of America and the Government of the United Kingdom of Great Britain and Northern Ireland on Access to Electronic Data for the Purpose of Countering Serious Crime, https://www.justice.gov/ag/page/file/1207496/download#Agreement%20between%20the%20Government%20of%20the%20United%20States%20of%20America%20and%20the%20Government%20of%20the%20United%20Kingdom%20of%20Great%20Britain%20and%20Northern%20Ireland%20on%20Access%20to%20Electronic%20Data%20for%20the%20Purpose%20of%20Countering%20Serious%20Crimes, last accessed 2022/11/25.

35) The United States Department of Justice, U.S. And UK Sign Landmark Cross-Border Data Access Agreement to Combat Criminals and Terrorists Online, 2019/10/3, https://www.justice.gov/opa/pr/us-and-uk-sign-landmark-cross-border-data-access-agreement-combat-criminals-and-terrorists, last accessed 2022/11/25 (hereinafter “Immediate Release on 2019/10/3”).

をイギリスのプロバイダに送達するとともに、開示されたデータを捜査機関に送るよう手配することになる[36]。

また、このようにして入手した証拠の利用制限に関する規定も置かれており、例えば、自国の重大な利益にかかわるような場合には、事前に相手国の指定機関から承諾を得なければならない。重大な利益にかかわる場合とは、イギリスについては、アメリカの刑事裁判で死刑が求刑される場合において、イギリスのプロバイダから入手したデータが証拠として提出されるとき、アメリカについては、言論の自由にかかわるようなイギリスの刑事裁判で、アメリカのプロバイダから入手したデータが証拠として提出される場合をいう。承諾を求められた指定機関は、承諾するかしないかを判断するだけではなく、必要と思われる条件を課すこともでき、この場合、当該条件に従った利用のみ認められる。

このように、相互主義の保証の下、一定の制約があるとはいえ、アメリカとイギリスの捜査機関は、自国の裁判所の許可を受ければ、数か月、場合によっては数年かかることもある国際捜査共助によることなく、相手国に拠点を置くプロバイダから、指定機関を通じて直接データを入手することができるようになる。したがって、この行政協定は、外国からのデータの押収に関する法的障害を取り除くことによって、捜査を劇的に迅速化することになると期待されているのである[37]。「重大犯罪」や「重大な利益」の内容は国によって異なるのが当然であるが、行政協定によれば、どのような内容であれば互いに合意できるかを当事国において話し合い、きめ細かく取り決めることが可能となる。

さらに、2021年12月にはオーストラリアとの間でも行政協定が締結されており[38]、2022年３月にはカナダとの間でも行政協定のための公式の交渉に入ったようである[39]。オーストラリアとの行政協定においても、重大犯

36) Immediate Release on 2022/10/3.

37) Immediate Release on 2019/10/3.

38) The United States Department of Justice, United States and Australia Enter CLOUD Act Agreement to Facilitate Investigations of Serious Crime, 2021/12/15, https://www.justice.gov/opa/pr/united-states-and-australia-enter-cloud-act-agreement-facilitate-investigations-serious-crime, last accessed 2022/11/25.

39) The United States Department of Justice, United States and Canada Welcome Negotiations

罪の定義、言論の自由に関する制限規定、命令の対象から除外される者の範囲（オーストラリアに関してはアメリカと同様）、独立した機関による審査又は監督、指定機関による審査及び送達、利用制限に関する規定（オーストラリアに関してはイギリスと同様）といった類似の規定が見受けられる[40]。したがって、他国との間の行政協定についても、同様の観点から交渉が進められるものと思われる。

Ⅴ 結びに代えて

本稿では、サイバー犯罪条約を受けて導入された記録命令付差押え及びリモートアクセス捜査に関して生じ得る主権の問題を概観した上で、第二追加議定書がサイバー犯罪捜査にどのような影響を及ぼし得るか検討した。日本では、捜査機関にとっての利便性からか、特に捜査機関が自らサーバにアクセスするリモートアクセス捜査に関して活発に議論がなされているが、第二追加議定書における主眼は、プロバイダを介する記録命令付差押えタイプの捜査手法にあると思われる。サイバー犯罪条約でも予定されている従来の記録命令付差押えは、自国のプロバイダに対する開示命令にとどまるが、他の締約国にあるプロバイダからのデータの開示が期待できる点で、第二追加議定書が策定された意義は大きい。

具体的には、ドメイン名の登録サービスを提供する団体に対するドメイン名の登録情報の要請、プロバイダに対する加入者情報の開示命令といった、直接他の締約国の団体又はプロバイダに要請又は命令することのほか、他の締約国に対して、プロバイダに対する加入者情報又は通信記録の開示命令の執行を要請すること、さらには緊急事態において、プロバイダからのデータの迅速な開示を受けるために連絡部局を通じて即時の援助を

---

of a CLOUD Act Agreement, 2022/3/22, https://www.justice.gov/opa/pr/united-states-and-canada-welcome-negotiations-cloud-act-agreement, last accessed 2022/11/25.

40) 署名された合意文書自体は確認できなかったため、アメリカの司法省が暫定的に掲載している内容を参照した。The United States Department of Justice, Agreement between the Government of the United States of America and the Government of Australia on Access to Electronic Data for the Purpose of Countering Serious Crime, https://www.justice.gov/dag/cloud-act-agreement-between-governments-us-and-australia, last accessed 2022/11/25.

求める要請を発することを認める内容となっている。

このようにプロバイダを介する方法による国際協力強化の姿勢は、アメリカのCLOUD法にも見て取れる。互いに自国のプロバイダからのデータの押収を許す二国間の行政協定は、第二追加議定書と同様、あるいはよりきめ細かな取決めをすることによって、互いの国民や居住者を適切に保護しながらも、サイバー犯罪に有効に対処することを可能とする国際協力の枠組みといえる。リモートアクセス捜査について主権侵害の可能性が否定できない以上、アメリカに限定されるとはいえ、多くの利用者が存在するプロバイダをその領域内にかかえる国であるから、本稿で紹介したイギリス、オーストラリア、カナダに続いて、日本がアメリカと行政協定を締結するのか、またどのような内容となるのか注目されるところである。さらに、サイバー犯罪条約及び第二追加議定書については、その締約国以外に効力が及ばないことから、アメリカに限らず、このような行政協定の可能性を探ることは、サイバー犯罪捜査の実効性を確保するためにも必要となると思われる。

もっとも、記録命令付差押えタイプのデータの押収においても、捜査機関の「命令」に基づくものであるから主権侵害の可能性があるとすると、自国のプロバイダが締約国以外の国のサーバに蔵置されているデータを提出する場合と同様、他の締約国のプロバイダが締約国以外の国のサーバに蔵置されているデータを提出する場合も、主権の問題を考える必要が出てきそうである。しかし、通常、プロバイダが他国の領域に適法にサーバを設置している場合において、その管理下にあるデータを移転することについては国家主権との関係では特に制限がないと思われ、ここで問われるのは、企業が保有するデータの取扱いと個人情報保護の関係であろう。この点、欧州連合（EU）域外への個人情報の移転に関して厳しく規制するGDPR（General Data Protection Regulation）についてみると、捜査機関への個人情報の提供は、適法な取扱いとして掲げられている事由のうち「管理者が服する法的義務を遵守するために取扱いが必要となる場合」（６条１(c)）に該当する場合が多いと考えられているという[41]。したがっ

41) 小向太郎「捜査機関による第三者保有の個人情報に対するアクセスと本人の保護」情報通信政策研究４巻１号63頁、73頁（2020年）。

て、他の締約国のプロバイダへの「命令」に関する国際的な取決めと、個人情報保護も含めこれに対応する適切な国内法の整備によって解決を図ることが合理的であるように思われる。

本稿で取り上げた第二追加議定書では、国境を越えるデータの押収に関する国際協力の強化だけではなく、適用のある国際協定が存在しない場合の国際協力に関する手続として、ビデオ会議に関する規定（第二追加議定書11条）も置かれている。要請を行う締約国は、ビデオ会議により証人又は専門家から証言及び供述を取得することを要請することができるものとし、要請を受ける締約国は、これを認めることができるというもので、いわゆるビデオリンク方式による証人尋問を他の締約国に居住する者を対象に行うことを可能とする内容である。

日本では、2000年の改正（2001年６月施行）によって、一定の事件について同一構内でのビデオリンク方式が導入されたが（刑訴法157条の６第１項）、2016年の改正（2018年６月施行）で遠隔地における実施も認められるようになった（刑訴法157条の６第２項）。遠隔地といっても、ビデオリンク方式による証人尋問に必要な装置の設置された他の裁判所の構内とされていることから（刑訴規則107条の３）、これを他の締約国で実施し、かつ、そこで獲得された供述に証拠能力が認められるようにするための国内法の整備も求められることになる。とはいえ、国境を越えるデータの押収に加えて、供述の確保も容易になれば、より強固なサイバー犯罪対策が期待できる[42]。

また、サイバー犯罪条約に加盟していなかった韓国も、2022年10月、欧州評議会に対して加入意向書を提出したとのことである。第二追加議定書への対応、あるいは行政協定の締結に関して、今後の国際的、国内的な動向がなお一層注目される。

---

42) アメリカでの近年（特にコロナ禍）のビデオリンク方式による証人尋問のあり方に関して論じるものとして、拙稿「ビデオリンク方式による遠隔地での証人尋問に関する検討」明知法学（명지법학）21巻２号175頁（2023年）参照。

(논문투고일: 2023.2.28., 심사개시일: 2023.3.10., 게재확정일: 2023.3.24.)

中村真利子

サイバー犯罪条約、データの押収、第二追加議定書、CLOUD法、行政協定

【参考文献（掲載順）】

Ⅰ　判例・裁判例

東京高判平成28年12月７日高刑集69巻２号５頁
大阪高判平成30年９月11日高刑速（平30）344頁
最（一小）判昭和53年９月７日刑集32巻６号1672頁
最（二小）決令和３年２月１日刑集75巻２号123頁

Ⅱ　書籍・論文

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1049頁（2012年）
川出敏裕「コンピュータ・ネットワークと越境捜査」酒巻匡ほか編『井上正仁先生古稀祝賀論文集』（有斐閣、2019年）409頁以下
山内由光・研修832号13頁（2017年）
宇藤崇・法学教室445号152頁（2017年）
四方光・刑事法ジャーナル58号143頁（2018年）
笹倉宏紀・平成29年度重要判例解説182頁（2018年）
星周一郎「サイバー空間の犯罪捜査と国境・覚書き」警察学論集73巻４号71頁（2020年）
川出敏裕「サイバー犯罪の捜査」警察学論集71巻９号157頁（2018年）
中野目善則「サイバー犯罪の捜査と捜査権の及ぶ範囲―プライヴァシーの理解の在り方、法解釈の在り方、他国へのアクセスの及ぶ範囲等の観点からの検討」警察政策22巻130頁（2020年）
栗田理史・研修849号25頁（2019年）
指宿信・新判例解説Watch24号187頁（2019年）
宇藤崇・法学教室462号157頁（2019年）

中島宏・法学セミナー768号130頁（2019年）
深野友裕・警察学論集72巻4号151頁（2019年）
前田雅英・WLJ判例コラム227号（2021年）
田中優企・法学教室490号149頁（2021年）
四方光・法学教室491号75頁（2021年）
星周一郎・刑事法ジャーナル69号264頁（2021年）
吉戒純一・ジュリスト1562号98頁（2021年）
川出敏裕・論究ジュリスト37号121頁（2021年）
指宿信・Law & Technology 92号40頁（2021年）
指宿信・Law & Technology 93号32頁（2021年）
岩﨑正・新判例解説Watch 29号225頁（2021年）
大橋充直・捜査研究848号56頁（2021年）
中野目善則・令和３年度重要判例解説147頁（2022年）
水谷恭史=関口和徳・季刊刑事弁護109号140頁（2022年）
横山裕一・日本大学法科大学院法務研究19号95頁（2022年）
竹内真理・令和３年度重要判例解説249頁（2022年）
早乙女宜宏「リモートアクセスによる差押えに伴う問題点の一考察」日本大学法科大学院法務研究16号67頁（2019年）
芝原邦爾ほか編『経済刑法―実務と理論』（商事法務、2017年）551頁以下〔笹倉宏紀〕
小向太郎「捜査機関による第三者保有の個人情報に対するアクセスと本人の保護」情報通信政策研究４巻１号63頁（2020年）
中村真利子「ビデオリンク方式による遠隔地での証人尋問に関する検討」明知法学（명지법학）21巻２号175頁（2023年）

Ⅲ 統計・資料

Council of Europe, Explanatory Report to the Convention on Cybercrime, https://rm.coe.int/16800cce5b
外務省「『協力及び電子的証拠の開示の強化に関するサイバー犯罪に関する条約の第二追加議定書』への署名」（仮訳文）、

https://www.mofa.go.jp/mofaj/files/100342968.pdf

Council of Europe, Explanatory Report to the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence, https://search.coe.int/cm/pages/result_details.aspx?objectid=0900001680a48e4b

The United States Department of Justice, Landmark U.S.-UK Data Access Agreement Enters into Force, 2022/10/3, https://www.justice.gov/opa/pr/landmark-us-uk-data-access-agreement-enters-force

The United States Department of Justice, Agreement between the Government of the United States of America and the Government of the United Kingdom of Great Britain and Northern Ireland on Access to Electronic Data for the Purpose of Countering Serious Crime, https://www.justice.gov/ag/page/file/1207496/download#Agreement%20between%20the%20Government%20of%20the%20United%20States%20of%20America%20and%20the%20Government%20of%20the%20United%20Kingdom%20of%20Great%20Britain%20and%20Northern%20Ireland%20on%20Access%20to%20Electronic%20Data%20for%20the%20Purpose%20of%20Countering%20Serious%20Crimes

The United States Department of Justice, U.S. And UK Sign Landmark Cross-Border Data Access Agreement to Combat Criminals and Terrorists Online, 2019/10/3, https://www.justice.gov/opa/pr/us-and-uk-sign-landmark-cross-border-data-access-agreement-combat-criminals-and-terrorists

The United States Department of Justice, United States and Australia Enter CLOUD Act Agreement to Facilitate Investigations of Serious Crime, 2021/12/15, https://www.justice.gov/opa/pr/united-states-and-australia-enter-cloud-act-agreement-facilitate-investigations-serious-c

rime

The United States Department of Justice, United States and Canada Welcome Negotiations of a CLOUD Act Agreement, 2022/3/22, https://www.justice.gov/opa/pr/united-states-and-canada-welcome-negotiations-cloud-act-agreement

The United States Department of Justice, Agreement between the Government of the United States of America and the Government of Australia on Access to Electronic Data for the Purpose of Countering Serious Crime, https://www.justice.gov/dag/cloud-act-agreement-between-governments-us-and-australia

Abstract

사이버 범죄 조약 제2추가 의정서에 따른 사이버 범죄 수사의 변화

사이버 범죄에 관한 국제 조약인 유럽평의회의 「사이버 범죄에 관한 조약」은 사이버 범죄 수사를 실효적으로 하는 것을 목표로 하는 것으로서, 일본에서도 이 조약에 따라 국내법을 정비하였으나, 국경을 넘는 데이터 압수에 대해서는 아직까지도 과제가 많이 남아 있다. 그래서 유럽평의회는 데이터 압수에 관한 국제협력을 강화하기 위해 「협력 및 전자증거 공개 강화에 관한 사이버 범죄에 관한 조약 제2 추가 의정서」를 새롭게 책정하였다. 일본도 2022년 5월에 열린 서명 개방식에서 이에 서명함에 따라, 본 논문에서는 이 제2추가 의정서의 내용을 수용함으로써 사이버 범죄 수사가 앞으로 어떻게 달라질 수 있는지에 관하여 검토하였다. 관련하여 새로운 국제협력의 형태로 주목받고 있는 미국의 CLOUD법(Clarifying Lawful Overseas Use of Data Act)과 2022년 10월부터 시행되기 시작한 영국과의 행정협정을 소개하면서 이러한 양자 간 행정협정 가능성에 대해서도 검토하였다.

"이 논문은 JSPS 과학연구비 21K13208 및 주오대학 2022년도 특정과제 연구비를 지원받아 수행된 연구임"

나카무라 마리코

사이버 범죄 조약, 데이터의 압수, 제2추가 의정서, 클라우드(CLOUD)법, 행정협정