様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　４ 年　 ５ 月 ３０ 日現在

機関番号：１２６０１
研究種目：基盤研究(C)（一般）
研究期間：2019～2021
課題番号：１９Ｋ０１３４３

研究課題名（和文）サイバー犯罪への国際的対応

研究課題名（英文）International countermeasure to cyber crime

研究代表者
川出　敏裕（Kawaide, Toshihiro）

東京大学・大学院法学政治学研究科（法学部）・教授

研究者番号：８０２１４５９２

交付決定額（研究期間全体）：（直接経費）　　2,700,000円

研究成果の概要（和文）：　サイバー犯罪の増加とコンピュータ・ネットワークの拡大という要因があいまって、犯罪の証拠となるデータが国外にあるサーバ・コンピュータに蔵置され、捜査のためにそれを取得する必要があるという事案が飛躍的に増加している。しかし、外国に所在するデータを捜査により取得することは、その国の主権を侵害する可能性があり、それがいかなる場合に許されるのかが問題とされてきた。本研究は、この点に関するわが国における議論を振り返るとともに、諸外国や国際機関での最新の議論状況を参考にしながら、時代に即した新たな制度の枠組みを提言するものである。

研究成果の学術的意義や社会的意義
捜査機関が外国にあるデータを取得するためには、これまでは、その国の承認が得られないかぎり、国際捜査共助のルートにより、そのデータを獲得するべきだとされてきた。しかし、それには時間がかかるうえに、クラウド上のデータのように、その所在が判明しないものもあり、捜査現場では対応に苦慮する事態が生じている。本研究は、この問題に対する国際的な動向も踏まえて、理論的に裏付けられ、かつ、捜査機関にとっても現実的な対応策を提示するものであり、そこに本研究の学術的・社会的な意義が認められる。

研究成果の概要（英文）：The increase of a cybercrime and expansion of a computer network have made the situation more common that data related to crimes is stored in the server computer in a foreign country. However, acquiring the data by so-called cross border search might infringe on the sovereignty of the country. This problem has been one of the main topics on the criminal investigation.
This research proposes the framework of the new system adapted, referring to the argument in foreign countries or an international organization while looking back upon the argument in our country about this problem.

研究分野：刑事訴訟法

キーワード：サイバー犯罪　越境捜査　サイバー犯罪条約　執行管轄権

１．研究開始当初の背景

インターネットに代表されるコンピュータ・ネットワークは、国境のない世界であるうえに、グーグルをはじめとするインターネット企業は世界的な規模でのネットワークを構築している。そのため、とりわけサイバー犯罪については、その証拠となるデータが外国にあるサーバ・コンピュータに蔵置されている場合が少なくない。このことは既に共通の認識となっていたが、近年におけるクラウド・コンピューティングの発達により、そもそもデータがどこにあるのかがわからないという事態が生じることになり、そのような場合に捜査機関がとり得る措置を明らかにすることが求められる状況になっていた。

２．研究の目的

犯罪の証拠となるデータが外国にあるサーバ・コンピュータに蔵置されている場合、これまでは、捜査機関が当該データにアクセスすることは、原則として許されず、外国の承認が得られないかぎり、国際捜査共助のルートにより、そのデータを獲得するべきだとされてきた。しかし、クラウド上のデータのように、その所在が判明しないものもあり、従来の考え方では対応が困難な事態が生じている。本研究は、外国における捜査に対する従来の法的規律及び国際捜査共助の在り方が現状に合わなくなっているのではないかという問題意識のもとに、この点に関する諸外国及び国際機関での議論の状況を参考にしながら、時代に即した新たな制度の枠組みを提言することを目的としたものである。

３．研究の方法

本研究は３年の期間で行った。初年度（令和元年度）は、まず第１に、わが国における実務と理論の現状を把握するために、文献調査を行うとともに、研究会等への参加を通じて、国際刑事法に関わる実務家、及びこの問題を研究している国際法研究者との意見交換を行った。第２に、それと並行して、外国における議論を把握するため、大陸法系のドイツ、英米法系のアメリカについて、基礎的な文献調査を行った。

２年目（令和２年度）は、サイバー犯罪における国際協力に焦点を当てた検討を行った。具体的には、欧州評議会の”Cloud Evidence Group”において、国境を越えるサイバー犯罪の捜査について継続的な検討が行われ、複数の報告書が公刊されており、その会議資料を含めて、それらの網羅的な検討を行った。なお、当初の予定では、文献の検討とあわせて、この問題についての議論が最も進んでいると考えられるドイツに赴き、司法省の担当者及びドイツにおけるサイバー犯罪研究の第一人者である、マックスプランク国際・外国刑法研究所の前所長である、Ulrich Sieber 教授のインタビューを行う予定であったが、わが国及びドイツの双方で、新型コロナウィルスの感染状況に改善が見られなかったため、やむなく訪問調査は中止することにした。

最終年度（令和３年度）は、まず、前年度までの研究成果を踏まえ、それまでの下級審裁判例の動向も含めて、同判例の詳細な分析を行った。さらに、欧州評議会のサイバー犯罪条約委員会や欧州委員会における議論、アメリカのクラウド法、他の諸国における越境捜査における判例の動向などを参考に、(1)捜査機関が外国に所在するデータを一方的に取得する行為に対して国際的にはどのような規律がなされているか、(2)サイバー犯罪に関する捜査についてどのような国際協力の枠組みが存在しているかについて調査するとともに、この両者について、今後どのような方向で国際的な合意が形成されていく可能性があるのかを検討した。そして、研究成果については、いくつかの雑誌論文として公刊した。

４．研究成果

(1) わが国も加盟している欧州評議会のサイバー犯罪条約（2001 年採択）においては、①当該データが地理的に所在する場所のいかんを問わず、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、及び、②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、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は、他の締約国の同意がなくとも行い得るとする規定が置かれている（32 条）。そして、条約の注釈書によれば、本規定は、締約国が、相互援助を要請することなく、コンピュータ・データに一方的にアクセスできることについて起草者全員が同意した場合を定めたものであり、その他の場合については、さらに経験が蓄積され、それらを踏まえてさらに議論がなされるようなときになるまで規定しないこととしたものとされている。これによれば、サイバー犯罪条約は、32 条に定められた場合以外には、締約国が、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、その締約国の同意なしにアクセスすることができないという趣旨までを含むものではないということになろう。

そのうえで、本規定が定める上記の２つの類型が、慣習国際法上どのように位置付けられるかには争いがある。このうち、①の類型は、慣習国際法上も認められているものであるとされるが、②の類型については、慣習国際法上認められている捜査手法を確認する趣旨の規定であるのか、それとも、慣習国際法上は認められていない捜査手法を、締約国の合意のもとに認めたものかは、締約国の間でも必ずしも見解が一致していない。

わが国は、サイバー犯罪条約に加盟したことにより、他の締約国との関係では、32 条が定める２つの場合に、相手国の同意を得ることなく、国外に蔵置されたコンピュータ・データにアクセスできることになったが、非締約国との関係で何ができるのか、また、締約国との関係でも、この２つの場合にしか同意なしのアクセスが許されないのかは、なお明らかでないのである。サイバー犯罪条約の批准のため、平成 23 年に刑事訴訟法の改正がなされ、いわゆるリモートアク

セス（刑訴 99 条 2 項・218 条 2 項）を含む新たな捜査方法が導入されたものの、外国に所在するサーバに蔵置されたコンピュータ・データの取得に係る問題については、立法過程でも必ずしも詰めた議論はなされていない。

なお、外国にあるサーバに蔵置されているデータを捜査機関が強制的に取得する方法としては、捜査機関自身が当該データにアクセスする方法とならんで、自国の管轄権に服するプロバイダに対して、外国にあるデータを取得して、提出することを命じるという方法がありうる。わが国の刑訴法に引き直せば、記録命令付差押え（99 条の 2・218 条 1 項）が、この捜査手法に該当する。それゆえ、捜査機関が取得しようとする電磁的記録が外国にあるサーバに記録されている場合には、命令に応じて、プロバイダ側で国外のサーバからデータを取得したうえで、記録媒体に記録し、その記録媒体を捜査機関が差し押さえるということになる。

立法担当者の解説では、こうした記録命令付差押えの場合は、国外からのデータの取得を含む記録行為自体は、捜査機関ではなく、命令を受けたプロバイダによって行われるものであるから、それによりデータが記録された記録媒体を捜査機関が差し押さえたとしても、外国の主権を侵害するものではないとされている。この解釈によれば、リモートアクセスとは異なり、この手法については、そもそも主権侵害の問題自体が生じないことになる。

(2) 前述のとおり、サイバー犯罪条約 32 条に該当しない事案において、外国にあるサーバへのリモートアクセスが行われた場合に、それが外国の主権を侵害するものとして違法となるのか、仮に違法となるとして、そのことが、それによって獲得された証拠の証拠能力にどのような影響を及ぼすのかは明らかではなかった。そうした中で、近年になって、いくつかの裁判例において、それが実際に争われ、令和 3 年 2 月に、最高裁による判断が下されることになった（最決令和 3・2・1 刑集 72 巻 5 号 123 頁）。

本件で、被告人は、日本国外に所在するサーバへのリモートアクセスによる電磁的記録の取得行為は、現行刑訴法によっては行うことができず、あくまで国際捜査共助によるべきものであるところ、警察官が、これらの点を認識したうえで、国際捜査共助を回避し、令状による統制を潜脱する意図のもとに、上記のリモートアクセスを実施した行為は、サーバ存置国の主権を侵害するものであり、重大な違法があるから、各手続によって収集された証拠は違法収集証拠として排除すべきである旨主張した。最高裁は、以下のように述べて、被告人側の主張を退けた。

まず、日本国外に所在するサーバへのリモートアクセスが現行刑訴法によって行いうるかどうかについては、刑訴法 99 条 2 項、218 条 2 項の文言や、これらの規定がサイバー犯罪条約を締結するための手続法の整備の一環として制定されたことなどの立法の経緯、同条約 32 条の規定内容等に照らすと、刑訴法は、日本国外にある記録媒体を対象とするリモートアクセスも想定したものと解されるとする。そのうえで、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、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した。そして、これを前提に、本件でとられた手続には重大な違法があるということはできないから、それにより収集した証拠の証拠能力は、いずれも肯定することができると判示したのである。

(3) 本件の原判決が、強制捜査により外国にあるサーバにリモートアクセスすることは、当該外国の主権を侵害する可能性があると判示したのに対し、最高裁決定は、その点について明言していない。しかし、「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、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は、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」という判示は、外国に所在するサーバへのリモートアクセスは主権侵害となりうるものであるが、条約 32 条に該当する場合には、それが正当化されるという理解を前提としたものと考えられる。

このように、サイバー犯罪条約 32 条に該当しないリモートアクセスは主権侵害となりうるという前提で考えた場合、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、かつ、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ものであった。そうすると、本件でとられた手続は、いずれも主権侵害を生じさせる可能性があったことになる。

(4) 外国に所在するサーバへのリモートアクセスが主権侵害を生じさせる場合があるとして、次に問題となるのは、当該リモートアクセスが、刑訴法上の要件は満たしているものの、外国の主権を違法に侵害しているという場合に、それは国際法上違法であるにとどまるのか、それとも、刑訴法上も違法となるのかである。最高裁は、その点につき明言していないが、その判示からは、違法な主権侵害があった場合にはそれが刑訴法上も違法と評価されることを前提としているものと考えられる。

そのうえで、いずれの手続についても、結論として、重大な違法があったとはいえないとしているから、主権侵害があったということだけでは、証拠排除を導くような重大な違法とはならないという立場をとっていることになろう。

(5) このように、サイバー犯罪条約 32 条に該当しない、強制処分としてのリモートアクセスは

サーバ所在国の主権を侵害する可能性があるし、同条に該当するリモートアクセスであっても、条約の非締約国との関係では、やはり主権侵害が生じる可能性がある、それゆえ、そのような場合に、わが国の捜査機関が外国に所在するサーバに蔵置されたデータを取得しようとするのであれば、リモートアクセスについてその国の同意を求めるか、国際捜査共助の手続に基づきデータを提供してもらうべきことなる。ただし、同意を得るにしろ、国際捜査共助の手続をとるにしろ、データがどこに蔵置されているかを捜査機関が認識していることが前提となる。しかし、サーバを管理するプロバイダがそれを明らかにしないため、あるいは明らかにできないために、それが判明しない場合もある。とりわけ、クラウドサービスにおいては、データの所在地が分散したり、移動したりするため、それを確定することは困難であるとされている。そのように、データが蔵置されている場所が判明しない場合にまで、捜査機関に対し上記のような手続をとることを要求するのは、不可能なことを強いるものであって妥当ではない。それゆえ、そうした場合には、データが外国にあるサーバに蔵置されている可能性があるとしても、捜査機関には、外国の同意を求めたり、捜査共助を要請したりする国際法上の義務はなく、その裏返しとして、刑訴法上の捜査権限は制約されないから、直ちにリモートアクセスを行うことが認められるべきであろう。

(6) サイバー犯罪条約 32 条が規定する以外の形態でのリモートアクセスについて、それが主権侵害となるかどうかについては、国際的に見ても、未だ意見は一致していない。同条約の締約国の中にも、それを主権侵害でないとしている国もあれば、主権侵害となりうるという前提で、一定の場合に例外を認めるという立場をとっている国もある。国際的な合意を得ることは、なお難しい状況にあるといってよいであろう。

国外に所在するサーバに蔵置されたデータを取得する方法としては、リモートアクセス以外に、プロバイダに対し、当該データを提出することを命じるという方法がある。このうち、自国の管轄権内のプロバイダに対してそれを命じることについては、サイバー犯罪条約にもそれを想定した規定が置かれているから（18 条）、残るのは、自国の管轄外にある外国のプロバイダに対して、直接にそれを依頼する方法である。そして、現在は、国際的に、この仕組みづくりに向けた動きが進みつつある。

その一つが、2018 年に制定されたアメリカのクラウド法（Cloud Act）である。同法においては、アメリカ政府と外国政府が行政協定を結ぶことにより、アメリカの管轄権に服するプロバイダが、アメリカ政府を介することなく、外国政府からの直接の命令に応じてデータを適法に開示することができるとした規定が置かれた。

同じような動きは、サイバー犯罪条約を成立させた欧州評議会においても見られる。そこでは、近年のクラウドサービスの普及という現状を踏まえて、リモートアクセスを含めた越境捜査についての検討が行われ、2021 年 5 月に、「協力の強化と電子的証拠の開示に関するサイバー犯罪条約の第二追加議定書」の最終案が、サイバー犯罪条約委員会により承認され、公表された。そこでは、より効果的な国際捜査共助の仕組みを構築するとともに、特定の犯罪の捜査のために、締約国の政府が、自国の領域外のプロバイダに対して、直接に、加入者情報の開示を命じることができるとする規定を置くことなどが定められている。

これと並行して、欧州委員会においても、外国にある電子的証拠（e-Evidence）の収集方法について検討が行われ、2018 年に、プロバイダに対し EU 域内に指定代理者を置く義務を課す指令案と、EU 構成国が、データの保全命令と提出命令を、指定代理者を含む名宛人に対して直接に発することができるとする、刑事事件における電子的証拠のための欧州保全・提出命令規則案が公表された。これにより、EU 構成国は、自国の管轄権に服さないプロバイダに対してもデータの保全と提出を命じることができるようになる。

(7) アメリカのクラウド法も、欧州評議会及び欧州委員会の提案も、捜査機関が外国に所在するサーバに自らアクセスしてデータを取得するのではなく、捜査機関が外国のプロバイダに対して、外国にあるデータを提出することを命令ないし依頼する仕組みを設けるものである。実際問題としても、多くの場合は、それによって捜査に必要なデータを獲得することができるであろうから、わが国としても、まずはこの仕組みに加わるべく、解決すべき課題について検討を進めることが必要である。

ただし、事案によっては、そのような対応をしていたのでは、データが消去されてしまうおそれがあり、捜査機関が直ちにサーバにアクセスして、データを取得する必要がある場合も考えられる。前述の第二追加議定書案には規定が置かれていないが、欧州評議会においては、リモートアクセスをいかなる場合に認めるかについても合意に向けた検討が引き続き行われており、わが国は、サイバー犯罪条約の加盟国として、その議論にも積極的に参加していく必要があろう。

５．主な発表論文等

〔雑誌論文〕　計3件（うち査読付論文　0件／うち国際共著　0件／うちオープンアクセス　0件）

１．著者名 川出敏裕	４．巻 92巻6号
２．論文標題 刑事法をめぐる問題－国際的協調の観点から	５．発行年 2020年
３．雑誌名 法律時報	６．最初と最後の頁 41－47
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 川出敏裕	４．巻 202号
２．論文標題 ネットワーク犯罪と越境捜査	５．発行年 2021年
３．雑誌名 法の支配	６．最初と最後の頁 122-134
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 川出敏裕	４．巻 37号
２．論文標題 リモートアクセスの許容性	５．発行年 2021年
３．雑誌名 論究ジュリスト	６．最初と最後の頁 121-130
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

〔学会発表〕　計0件

〔図書〕　計1件

１．著者名 川出敏裕	４．発行年 2019年
２．出版社 立花書房	５．総ページ数 234
３．書名 刑事手続法の論点	

〔産業財産権〕

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関