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　６ 年　 ４ 月 ２８ 日現在

機関番号：３２６４１
研究種目：若手研究
研究期間：2021～2023
課題番号：２１Ｋ１３２０８

研究課題名（和文）サイバー犯罪におけるリモートアクセス捜査のあり方に関する比較法研究

研究課題名（英文）Comparative Research on Remote Access Investigation into Cybercrime

研究代表者
中村　真利子（Nakamura, Mariko）

中央大学・国際情報学部・准教授

研究者番号：９０８２６１３２

交付決定額（研究期間全体）：（直接経費）　　2,100,000円

研究成果の概要（和文）：本研究は、現行の刑事訴訟法に規定されるリモートアクセス捜査に関し、その意義と限界を明らかにすることを目的とする。この処分はサーバからのデータの押収を可能とするが、対象となるサーバは国内にあるとは限らないため、本研究では主として、越境リモートアクセス捜査の是非を検討した。サイバー犯罪条約では、利用者の同意を得て、相手国の承諾なく越境リモートアクセスすることが認められている。しかし、利用者が同意するとは限らず、国際的な動向としては、提出命令の形式でプロバイダからデータを押収することが期待される。今後、国内のプロバイダに加えて、国外のプロバイダに直接働きかける方法が模索されることになると思われる。

研究成果の学術的意義や社会的意義
多くの犯罪がネットワークを利用して行われたり、犯罪の証拠がデータとして存在したりする現代社会において、捜査機関が適切かつ迅速にデータを押収することは喫緊の課題である。本研究は、データの押収方法のうち、サーバからのデータの押収を可能とするリモートアクセス捜査に関して、欧州評議会の策定したサイバー犯罪条約、その後、データの押収に関する国際協力を拡充するために策定された第二追加議定書のほか、アメリカ・韓国の動向もふまえながら、その意義と限界を検討し、今後期待されるデータの押収方法を示唆した点で、意義があるといえる。

研究成果の概要（英文）：The purpose of this research is to examine the implications of the remote access investigation provided in the Code of Criminal Procedure. This procedure allows to seize data from servers through the users' computers. Since the servers might be outside of the country, this research mainly focuses on the pros and cons of the remote access investigation across borders. The Convention on Cybercrime admits this kind of investigation without the authorization of another Party based on the consent of the users, but the users would not necessarily agree with the procedure. Therefore, internationally, it might be more strongly expected to seize data, as a form of the production order, from providers that are both inside and outside the country.

研究分野：刑事法

キーワード：リモートアクセス捜査　サイバー犯罪　データの押収

※科研費による研究は、研究者の自覚と責任において実施するものです。そのため、研究の実施や研究成果の公表等については、国の要請等に基づくものではなく、その研究成果に関する見解や責任は、研究者個人に帰属します。

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

2001 年、欧州評議会において、サイバー犯罪から社会を保護することを目的として、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。）が採択された。サイバー犯罪条約は、世界初の包括的なサイバー犯罪対策としての役割を果たすもので、締約国に対して、刑事手続については主として「コンピュータ・データの捜索・押収手続の整備等」を求めている。日本では、2012 年にサイバー犯罪条約を締結するにあたって、国内法の整備を進め、2011 年には、「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」（平成 23 年法律第 74 号）が制定された。この改正法のうち、サイバー犯罪の証拠として必要となるデータを適正に収集するために新設された差押えの方法等のひとつが、リモートアクセス捜査（刑事訴訟法 218 条２項）である。

現在では、ネットワークを利用することで、コンピュータ本体やこれに付随する記録媒体ではなく、クラウドなど、物理的に離れた記録媒体にデータを保管することが可能となっている。例えば、必要なデータが、あるプロバイダのサーバに保管されていることが判明した場合、凶器や文書といった有体物を対象とした従来の差押え方法によると、そのサーバを特定して、サーバごと差し押さえることになる。しかし、どこに必要なデータが保管されているのか特定することは困難である場合も多く、特定できなければ、プロバイダの協力が得られない限り差押えは許されないことになる。また、一個人の関連する情報であっても、様々な場所に保管してある可能性のある多くのデータそれぞれについて差押えを行うことは煩雑で、全てのサーバを特定している間に、犯人等にデータの移転・消去による証拠隠滅を許してしまうことにもなりかねない。さらに、膨大なデータが蓄積されているサーバそのものを差し押さえると、処分を受ける者の業務等に著しい支障を生じさせるおそれもある。そこで、コンピュータにネットワークで接続しているサーバなどの記録媒体にリモートアクセスし、必要なデータを、そのコンピュータや CD-R など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というリモートアクセス捜査が新設された。

もっとも、リモートアクセス捜査は差押えに付随する処分として規定されており、差押えの対象物であるパソコンなどと一体のものとして利用されているサーバなどの記録媒体について、差押えに先立って行うことが想定されている。しかし、事前にパソコンなどにログインするためのパスワードなどが判明していないこともある。そこで、パソコンなどを差し押さえた後に、リモートアクセス捜査を行うことができるか、またその場合に、どのような手続によるべきかが問題となる。したがって、まず、①差押えに先立って行われるリモートアクセス捜査以外のリモートアクセス捜査、とりわけ、対象の存在、性質、状態、内容を認識する処分である検証としてのリモートアクセス捜査の是非を明らかにする必要がある。

次に、現代の情報化社会においては、リモートアクセス捜査によってアクセスされるサーバなどが国外にあることは稀なことではない。サイバー犯罪条約では、「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。）。」、「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旨定めている（サイバー犯罪条約 32 条）。それ以外の場合については規定されるに至っておらず、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。そこで、②サーバなどが蔵置してある国の許可なく、又は国際捜査共助の手続をとることなく、越境リモートアクセス捜査を行うことの是非についても明らかにする必要がある。

２．研究の目的

インターネットの発展に伴い、人々の生活はより便利になり、時間と場所の隔たりをそれほど感じることなく、国境を越えてコミュニケーションをとったり、情報を入手したりすることができるようになった。このことは、犯罪者もまた便利なツールを手に入れたことを意味し、匿名性の高いサイバー空間においては、犯人を特定し、犯罪の証拠を収集することが困難な場合も少なくない。情報技術が日々発展していくなか、2011 年の改正により導入されたリモートアクセス捜査の意義と限界を明らかにするとともに、サイバー犯罪において重要な証拠となるデータを適正に収集するための方策を模索しようとする点で、本研究の学術的独自性がある。リモートアクセス捜査はサイバー犯罪の証拠を十分に収集するための重要な手続であるから、これが適法かつ有効に用いられるような研究を行うことの意義は大きい。

国境を観念し難いサイバー空間では、何を「犯罪」ととらえ、どのように捜査していくのか、各国で共通認識をもち、互いに協力していくことが不可欠である。したがって、各国の動向も把握しながら、日本におけるリモートアクセス捜査の手続について論じることは、情報化社会においては特に重要である。また、越境リモートアクセス捜査においては、対象となるサーバなどが、

日本のようなサイバー犯罪条約の締約国だけではなく、韓国のような非締約国に蔵置されていることも十分あり得る。したがって、サイバー犯罪条約のような国際法の枠組みについて、その動向を追うとともに、越境アクセスについての国際的な合意のない範囲において、どのような根拠に基づいて、どこまでリモートアクセス捜査を行うことができるのか検討することにも意義がある。

３．研究の方法

①差押え後のリモートアクセス捜査の是非に関しては、まず、現行法で明示的に認められているリモートアクセス捜査の導入趣旨と限界について、主として立法の過程や論者の議論を参照しながら明らかにした。②越境リモートアクセス捜査に関しては、「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」について定めるサイバー犯罪条約 32 条と、その後に策定された第二追加議定書及び韓国の動向のほか、データの収集や越境について扱う欧州連合(EU)の GDPR（General Data Protection Regulation）やアメリカ合衆国のクラウド法（Clarifying Lawful Overseas Use of Data Act）に関する議論状況もふまえて、サイバー空間におけるデータの押収方法のあり方を検討した。

いずれも、関連する図書を購入し、あるいは図書館及びオンラインデータベースを用いて資料収集を行うとともに、韓国法に関しては、現地でも調査を行った。また、サイバー犯罪捜査に関する最新の知見を得るために、適宜、関連する国内外の学会又は研究会に参加した。

４．研究成果

②の問いと関連して、サイバー犯罪条約 32 条においては、利用者の同意を得て越境リモートアクセス捜査を実施する場合に、サーバの設置してある相手国の承諾なく越境リモートアクセス捜査できる旨規定されている。

> Article 32 – Trans-border access to stored computer data with consent or where publicly available
>
> A Party may, without the authorisation of another Party:
> a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or
> b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

しかし、利用者が同意するとは限らず、この場合に、通常の差押えと同様に、強制的にリモートアクセス捜査を実施することが、相手国の主権侵害とならないかが議論されている。個人が不正アクセスなどすることなく利用しているサーバの領域に関しては、この部分に限って令状に基づきリモートアクセス捜査を実施することは主権を侵害しないと考えることも可能であるが、サイバー犯罪条約 32 条の範囲外となることから、利用者の同意が得られない場合には、相手国の承諾を得るか、国際捜査共助によるべきであるとの見解も根強い。

そこで期待されるのが、アメリカ合衆国のクラウド法にみられるような提出命令の形式によるデータの押収方法である。この方法は、プロバイダからデータを押収するものであるが、サイバー犯罪条約 18 条においても規定されており、日本でも記録命令付差押え（刑事訴訟法 218 条１項、99 条の２）として導入されたものである。

> Article 18 – Production order
>
> 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:
> a a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and
> b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.
> 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.
> 3 For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:

a the type of communication service used, the technical provisions taken thereto and the period of service;
b the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;
c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.

この方法によると、たとえデータのあるサーバが外国にあったとしても、プロバイダ自身がデータを入手して提出することから、相手国の主権を侵害しないと考えられている。さらに、クラウド法では、行政協定を締結した外国が、国内のプロバイダからデータを押収することが想定されており、サイバー犯罪条約第二追加議定書においても、同様に、国外のプロバイダからデータを押収することができるよう、データの押収に関する国際協力の促進が図られている。したがって、今後、国内のプロバイダに対する提出命令に加えて、国外のプロバイダに直接働きかける方法が模索されることになると思われる。

また、①の問いに関しては、現行法のリモートアクセス捜査は、差押えに先立ってサーバにリモートアクセスし、必要なデータをコピーした記録媒体を差し押さえるという捜査手法であることから、差押え後のリモートアクセスについて検討する必要がある。特に、差押えの現場でアクセスできない場合や、前述の通り、越境リモートアクセスの可能性があることも考えられることから、差押え後にリモートアクセス捜査を実施することについて、令状呈示の相手方や、不服申立ての手段も考慮しつつ、引き続き研究を行う所存である。

＜参考文献＞

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.

Cybercrime Convention Committee (T-CY), Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY, https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806a495e.

Hiroki SASAKURA, *Computer, Network ni Kanren Suru Keizai Hnazai [Economic Crimes in Relation to Computer and Network]*, Kuniji SHIBAHARA, et al. (eds), Keizai Keiho [Economic Criminal Law], Shojihomu, Tokyo, Japan (2017).

Hiroki SASAKURA, a commentary of Tokyo High Court, 12/7/2016, Jurist (1518) 182 (2018).

Hiroshi NAKAJIMA, a commentary of Osaka High Court, 9/11/2018, Hougaku Seminar (768) 130 (2019).

Kimihiro IKEDA, *Denjiteki Kiroku wo Fukumu Shoko no Shushu/ Hozen ni Muketa Tetsuzuki no Seibi [Improvements of Procedures for Collecting and Preserving Evidence Including Electronic or Magnetic Records]*, Jurist (1431) 78 (2011).

Ko SHIKATA, a commentary of Tokyo High Court, 12/7/2016, Criminal Law Journal (58) 143 (2018).

Ko SHIKATA, a commentary of the Supreme Court, 2/1/2021, Hogaku Kyoshitsu (491) 75 (2021).

Makoto IBUSUKI, *Cyberspace ni okeru Shoko Shushu to Digital Shoko no Kakuho [Collecting Evidence in Cyberspace and Preserving Digital Evidence]*, Horitsu Jiho 83(7) 84 (2011).

Makoto IBUSUKI, a commentary of Osaka High Court, 9/11/2018, Shin Hanrei Kaisetsu Watch (24) 187 (2019).

Makoto IBUSUKI, a commentary of the Supreme Court, 2/1/2021, Law & Technology (92) 40 (2021).

Mariko NAKAMURA, *Remote Access Investigation in Japan*, Japanese Journal of Global Informatics Vol.1, 105 (2021).

Masahide MAEDA, a commentary of the Supreme Court, 2/1/2021, WLJ Hanrei Column (227) (2021WLJCC006).

Masahito INOUE, *Computer Network to Hanzai Sousa [Computer Networks and Criminal Investigations]*, vol.2, Hogaku Kyoshitsu (245) 49 (2001).

Ministry of Justice: Japanese Law Translation, http://www.japaneselawtranslation.go.jp/?re=02, last accessed 9/8/2021.

Mitsunao OHASHI, a commentary of Tokyo High Court, 12/7/2016 and the Supreme Court, 2/1/2021, Sousa Kenkyu 70(6) 56 (2021).

Noriaki SUGIYAMA & Masayuki YOSHIDA, *Comments on the Act for Partial Revision of the Penal Code, etc. to Respond to an Advancement of Information Processing*, vol.2, Lawyers Association Journal 64(5) 1049 (2012).

Satoshi KURITA, a commentary of Osaka High Court, 9/11/2018, Kenshu (849) 25 (2019).

Shuichi YOSHIKAI, a commentary of the Supreme Court, 2/1/2021, Jurist (1562) 98 (2021).

Shuichiro HOSHI, *Memorandum on a Correlation between Criminal Investigations in Cyberspace and Borders*, Journal of Police Science 73(4) 71 (2020).

Supreme Court of Japan: Judgments of the Supreme Court, https://www.courts.go.jp/app/hanrei_en/detail?id=1811, last accessed 9/8/2021.

Takashi UTO, a commentary of Tokyo High Court, 12/7/2016, Hogaku Kyoshitsu (445) 152 (2017).

Takashi UTO, a commentary of Osaka High Court, 9/11/2018, Hogaku Kyoshitsu (462) 157 (2019).

Tomohiro FUKANO, a commentary of Osaka High Court, 9/11/2018, Journal of Police Science 72(4) 151 (2019).

Toshihiro KAWAIDE, *The Point at Issues on Criminal Procedure Act*, vol.5, Journal of Police Science 71(9) 157 (2018).

Toshihiro KAWAIDE, *Computer Network to Ekkyo Sousa [Computer Networks and Investigations Across Borders]*, Tadashi SAKAMAKI, et al. (eds), Inoue Masahito Sensei Koki Shukuga Ronbunshu [Festschrift in honor of the Seventieth Birthday of Masahito INOUE], Yuhikaku, Tokyo, Japan (2019).

Yoshihiro SAOTOME, *A Study on the Issue of a Remote Access Seizure*, Nihon University Law Review (16) 61 (2019).

Yoshimitsu YAMAUCHI, a commentary of Tokyo High Court, 12/7/2016, Kenshu (832) 13 (2017).

Yoshinori NAKANOME, *Investigation of Cybercrime crossing a National Border*, Security Science Review (22) 130 (2020).

Yuki TANAKA, a commentary of the Supreme Court, 2/1/2021, Hogaku Kyoshitsu (490) 149 (2021).

５．主な発表論文等

〔雑誌論文〕　計3件（うち査読付論文　3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 中村真利子	４．巻 21(2)
２．論文標題 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	５．発行年 2023年
３．雑誌名 明知法学	６．最初と最後の頁 175-202
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 有
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 中村真利子	４．巻 35(1)
２．論文標題 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	５．発行年 2023年
３．雑誌名 成均館法学	６．最初と最後の頁 513-541
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 有
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 Mariko NAKAMURA	４．巻 13/ 2
２．論文標題 Remote Access Investigation Across Borders	５．発行年 2021年
３．雑誌名 HUFS Global Law Review	６．最初と最後の頁 1-18
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 有
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4件（うち招待講演　4件／うち国際学会　4件）

１．発表者名 中村真利子
２．発表標題 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
３．学会等名 International Joint Conference on Legal Policy of Smart City（招待講演）（国際学会）
４．発表年 2022年

１．発表者名
Mariko NAKAMURA

２．発表標題
The Remote Access Investigation in Japan

３．学会等名
2021 KLRI-KAFL International Conference（招待講演）（国際学会）

４．発表年
2021年

１．発表者名
中村真利子

２．発表標題
日本における電磁的記録の差押え

３．学会等名
全南大学校法学研究所・韓国刑事法学会共同学術大会　若手刑事法学者フォーラム（招待講演）（国際学会）

４．発表年
2021年

１．発表者名
中村真利子

２．発表標題
討論：裵相均「韓国におけるサイバー犯罪捜査の最近の動向に関する検討」

３．学会等名
韓国刑事法学会 若手刑事法学者フォーラム学術会議（招待講演）（国際学会）

４．発表年
2023年

〔図書〕　計0件

〔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