参議院常任委員会調査室・特別調査室

論題	サイバー犯罪条約第２追加議定書の概要 －国境を越えるサイバー犯罪捜査のための国際協力－
著者 / 所属	寺林　裕介 / 外交防衛委員会調査室
雑誌名 / ISSN	立法と調査 / 0915-1338
編集・発行	参議院事務局企画調整室
通号	455 号
刊行日	2023-4-14
頁	13-20
URL	https://www.sangiin.go.jp/japanese/annai/chousa/rippou_chousa/backnumber/20230414.html

サイバー犯罪条約第２追加議定書の概要

― 国境を越えるサイバー犯罪捜査のための国際協力 ―

寺林　裕介
（外交防衛委員会調査室）

１．はじめに

近年、サイバー犯罪は増加傾向にあり、日本のサイバー犯罪検挙件数についても、2021年には１万2,209件と前年に比べて23.6％増となった[1]。サイバー空間を利用した犯罪の特徴の一つとして匿名性や秘匿性が高いことが挙げられる。世界中のサーバを経由して通信経路を匿名化したり、コンピュータ・ウイルスを拡散させて他人のコンピュータを利用したりすることで犯罪の実行者は巧妙にその正体を隠すことができる。サイバー空間を利用した犯罪は、世界中に張り巡らされたコンピュータ・ネットワークを舞台としており、国境を越えて実行される。また、サイバー犯罪に限らず、通常の犯罪の捜査過程においても、その証拠がインターネットを介して国外に存在するケースも多い。

こうしたサイバー空間を利用した犯罪に対処する捜査当局の側には、国家主権の限界が

[1] 法務省『令和４年版 犯罪白書』194頁

あることから、従来、各国間における国際協力が求められてきた。国境を越えて行われる犯罪に対する国際協力については、国際刑事司法協力として各国の捜査当局によるＩＣＰＯ（国際刑事警察機構、インターポール）を介した協力や、各国間の相互主義の下での捜査共助、二国間・多国間における刑事共助条約による協力が行われている。

2004年に発効した欧州評議会の「サイバー犯罪に関する条約」（ブダペスト条約。以下、単に「条約」ともいう。）は、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を犯罪化し、こうしたサイバー犯罪の証拠の収集に適用する刑事手続を規定するとともに、犯罪人引渡しのほか締約国間における刑事共助（相互援助）の仕組みを設定した。しかし、条約の起草・発効当時と比べて、日常生活におけるインターネットの利用は質・量ともに大きく拡大し、それに伴ってサイバー空間を利用した犯罪は、悪質化・複雑化し、犯罪捜査には国際的な協力が一層不可欠になっている。特に、捜査当局が他の締約国に蔵置された犯罪の証拠となるデータを取得する場合の困難な状況を解消する必要性が認識されていた。

このような課題に対処するため、条約の締約国間で2017年に交渉を開始し、2021年11月、欧州評議会において、サイバー犯罪に関するデータ（電子的形態）の証拠の収集等について定めた第２追加議定書（以下、単に「議定書」ともいう。）が採択された。日本政府は議定書の起草作業に参画し、2022年５月12日に行われた署名式でこの議定書に署名した。2023年３月10日、議定書はその締結について承認を求めるため、第211回国会（常会）に提出された（閣条第９号）。

本稿は、サイバー犯罪捜査のための国際協力の現状とサイバー犯罪条約で規定された犯罪化と刑事手続について確認するとともに、国境を越えるサイバー犯罪の捜査における課題について対応しようとした第２追加議定書の内容を紹介するものである。

２．越境捜査のための国際協力

国境を越えて行われるサイバー犯罪の捜査には、各国による国際的な協力が必要となっている。世界中に張り巡らされたコンピュータ・ネットワークが構築されていることが当然となった現代社会においては、犯罪の証拠が外国に所在するサーバに蔵置されていることが犯罪者の意図的であれ、無意識であれ、多く存在する。しかし、捜査活動などの執行管轄権に基づく強制措置は、原則としてそれぞれの国家の領域内に限り認められており、外国の領域に立ち入って執行管轄権を行使できるのは、相手国との間で司法共助・捜査共助に関する特別の条約を結んでいる場合、あるいは相手国の明示又は黙示の同意がある場合に限られる[2]。

外国にある証拠を収集するための捜査共助の方法としては、まずＩＣＰＯルートにより、情報の発信・受信を行いつつ、捜査又は刑事訴訟に必要な証拠を収集する前段階としての各国の捜査当局間同士の国際協力が行われる。ＩＣＰＯでは、各国の警察機関の間に週７日、１日24時間の体制で利用可能な24/7ネットワーク[3]と呼ばれる通信網を整備し、これを

[2] 小寺彰ほか編『講義国際法』（有斐閣、2010年）173～174頁
[3] 1997年12月のＧ８司法・内務閣僚級会合において発出された「ハイテク犯罪と闘うための原則と行動計画」

利用して情報収集が行われている。次に、サイバー犯罪を含む捜査又は刑事訴訟に必要な証拠が外国に存在する場合には、外交ルートを通じた国際礼譲による捜査共助が実施される。日本においても、外国政府から証拠の提供等が求められた場合は、国際捜査共助法に基づき、相互主義の下で捜査共助に対応する。さらに、二国間刑事共助条約を締結している場合には、この条約によってあらかじめ指定される中央当局ルート、すなわち、日本の法務省又は警察庁と相手国の司法・捜査当局との間で直接共助の請求を交わすことができる[4]。また、サイバー犯罪条約には、締約国間において、サイバー犯罪やデジタル証拠の収集について、中央当局間による相互援助の仕組みが存在する。

しかし、二国間刑事共助条約又はサイバー犯罪条約に基づく中央当局ルートによる捜査共助においても、その要請への対応は各国の国内法に従って実施されることから、時間はかかり、手続の複雑さは避けられない[5]。さらに、サイバー犯罪に係る捜査には、複数国間に存在するサーバを経由して証拠が巧妙に隠蔽されていることや、証拠となるデータが複数の場所に保存されていること、データが移動することによってそもそもデータが所在する国が特定できないことなど困難な事情がある。

３．サイバー犯罪条約における犯罪化と刑事手続

（１）サイバー犯罪条約

サイバー犯罪条約は2004年に発効し、日本は2012年に締結した（2001年の条約作成時に署名）。現在、全てのＧ７諸国を含む68か国が締約国となっているが、中国、ロシア、インド等は未締結である。

サイバー犯罪条約においては、第一に、コンピュータ・システムを攻撃する犯罪行為やコンピュータ・システムを利用して行われる犯罪行為について犯罪化することを締約国に求めている。その対象犯罪は、①違法アクセス、違法傍受、データの破損や改ざん、ＤＤｏＳ攻撃などのシステム妨害、ウイルスやハッカーツールなどの製造・頒布、②データの偽造、これを利用した詐欺、③児童ポルノや著作権侵害などデータの内容に関連する犯罪、④これらの未遂及びほう助・教唆である。

第二に、サイバー犯罪やコンピュータ・システムを利用して行われる他の犯罪、犯罪の電子的形態の証拠の収集について、刑事手続に関する権限及び手続を整備することを求めている。その手続は、①データの迅速な保全、②通信記録の迅速な保全及び部分開示、③データ及び加入者情報の提出命令、④データの捜索及び押収、⑤通信記録のリアルタイム収集、⑥通信内容（自国の国内法に定める重大犯罪に限定）の傍受である。これら刑事手続に関する権限及び手続の設定・実施・適用に当たっては、欧州人権条約、自由権規約に

に基づいて設置された24時間体制のコンタクトポイントのこと。

[4] 日本は、刑事共助条約を米国、韓国、中国、香港、欧州連合（ＥＵ）、ロシア、ベトナムとの間で締結している。刑事共助条約については、中内康夫「欧州27か国への刑事共助ネットワークの拡大」『立法と調査』No.303（2010.4）、奥利匡史「第208回国会法律案等NAVI 日・ベトナム刑事共助条約」『立法と調査』No.444（2022.4）を参照。

[5] 小向太郎「クラウド上のデータを対象とする犯罪捜査に関する法的課題」『情報処理学会研究報告』(2018.2.16) ４頁

定める権利を確保し、比例原則を含む国内法の条件及び保障措置に従うことが義務付けられている。

第三に、犯罪人引渡しや証拠提供を始めとする国際協力が定められており、これらは広義の国際刑事司法共助に当たる。一般原則のほか、上記の刑事手続に関する締約国間における相互援助（共助）や24/7ネットワークの設置が規定されている。

（２）外国に所在するデータへのアクセス

サイバー犯罪やその他のコンピュータ・システムを利用した犯罪について、その捜査の刑事手続として課題となっているのが、外国に所在するサーバに蔵置されたデータを取得する方法についてである。蔵置されたデータに対する国境を越えるアクセスについてはサイバー犯罪条約の第32条に規定されており、公に利用可能なように公開されているデータにアクセスすること（第32条ａ）及び、自国の領域内にあるコンピュータから他の締約国に所在するデータにアクセスし、これを受領すること（第32条ｂ）を他の締約国の許可なしに行うことができるとしている。しかし、後者については、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定されている（第32条ｂただし書）。データが所在する締約国の同意を得ずに、この方法により捜査目的でデータを取得することが、国際法上、適法な執行管轄権の行使と認められるか否かについては各国間の考え方に隔たりがあり、また、日本の犯罪捜査においても、他国に所在するデータへのアクセスがどのような条件で認められるのかについて明確な基準は示されていない[6]。

捜査目的で外国に所在するデータにアクセスする方法を確保するため、締約国は、自国の領域内に所在する者に対し、当該者が保有・管理している特定のデータの提出を命じる権限（第18条１ａ）と、自国の領域内でサービスを提供するインターネット・サービス・プロバイダ（以下「ＩＳＰ」という。）に対し、当該ＩＳＰが保有・管理している加入者情報の提出を命じる権限（第18条１ｂ）を捜査当局に与えることがサイバー犯罪条約の第18条に規定されている。日本は条約の国内担保として2011年に刑事訴訟法を改正し、同法第99条の２に記録命令付差押え[7]を新設した。このときそのデータが仮に外国に所在しているとしても、そこにアクセスして記録する者は国内におり、また、権限を有して行うものであり、主権の制約にはならない[8]。

上記のデータ提出を命じる権限については、あくまで自国の領域内に所在する者、自国の領域内でサービスを提供するＩＳＰに対してであり、サイバー犯罪に関する捜査又は刑事訴訟において、他国のＩＳＰが保有・管理するデジタル証拠が必要になる場合、国際捜査共助の仕組みを利用する必要がある。この点に関しては、サイバー犯罪条約第２追加議定書において、他の締約国の領域内に所在するＩＳＰに対し、各締約国の捜査当局が直接命令を発する権限や手続が盛り込まれた。後述の**４．**でその概要を紹介する。

---

[6] 小向太郎『情報法入門（第６版）』（ＮＴＴ出版、2022年）50～53頁

[7] コンピュータ・データを保管する者等の利用権限を有する者に命じ、必要なデータを記録・印刷させた上で差し押さえること。

[8] 第177回国会衆議院法務委員会議録第15号14頁（平23.5.31）

なお、米国で2018年３月に制定されたクラウド法（CLOUD Act）[9]においては、米国内企業が米国外の自社サーバに保有しているデータの内容を強制的に開示させる米国政府の権限が規定された。また、この米国クラウド法では、米国と外国政府が行政協定を締結することで､外国政府が直接､米国内ＩＳＰ等に対してデータの開示を要求することを認めた。米国はイギリス、オーストラリアとの間で上記の行政協定を締結している。

４．第２追加議定書の概要

（１）議定書の適用範囲

サイバー犯罪条約第２追加議定書は、コンピュータ・ネットワークに蔵置された犯罪の証拠が、国外の、複数の又は不明な管轄地に所在することが増えていることから、そのような場合に証拠となるデータの収集を強化するため、各国間の協力を強化するとともに、国家とＩＳＰ等の民間部門との間の直接的な協力に関する追加の手段を定め、一層効率化を図ろうとするものである。

本議定書の適用範囲は、条約の場合と同様であり、サイバー犯罪の捜査又は刑事訴訟だけでなく、一般の犯罪に関するデータ（電子的形態）の証拠の収集にも適用される（第２条１ａ）[10]。

また、本議定書の各締約国は、条約と同様、国内法の条件及び保障措置に従うことが義務付けられ、人権及び自由を保護することが規定されている（第13条)。その上で、他の国際協定や関係締約国間に別段の合意がある場合を除くほか、本議定書の適用範囲において受領した個人情報を処理すること、当該適用範囲の目的と関連性を有しており、かつ、当該目的との関係において過度でないことを確保すること等、個人情報の保護について具体的に規定された（第14条)。

（２）ドメイン名の登録情報の開示

本議定書の第６条においては、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（登録事業者）との直接協力のための権限や手続が規定された。サイバー犯罪の中には、ドメインを悪用し、マルウェアの拡散やフィッシング詐欺などを行っているケースが多くあり、ドメインの登録情報へのアクセスは、こうした犯罪の容疑者を特定するために必要となる。また、多くの犯罪捜査の初動のプロセスにあっても、捜査当局にとって容疑者特定につながる情報が必要とされ、ドメインの登録情報は有力な手がかりとなり得る。こうしたドメインの登録情報については、これまでWhois[11]に保存されて公開されてきたが、近年、ＥＵ一般データ保護規則（ＧＤＰＲ）を始め、各国の個人情報をめぐる取扱いが厳しくなり、登録者情報についてこれが保護されるべき情報として非公開とされるケースがある。本議定書においては、捜査当局が外国のドメイン名登録事業者に対し

---

[9] 米国のクラウド法については、筋伊知朗『サイバー犯罪』（ミネルヴァ書房、2022年）189～192頁を参照。

[10] なお、第１追加議定書（日本は未締結）の締約国間においては、第１追加議定書に定められた犯罪に関する特定の捜査又は刑事訴訟についても適用される（第２条１ｂ)。

[11] インターネット上のドメイン名やＩＰアドレスなどの登録者に関する情報を参照できる検索サービスのこと。

て情報開示を要請し、効率的に情報を取得するための枠組みが構築されることとなる。具体的には、各締約国は、自国の領域内に所在するドメイン名登録事業者が、国内法令に定める合理的な条件に従い、他国の捜査当局からの要請に応じてドメイン名の登録者を特定又は連絡するための情報を開示することを認める（第６条１、２）。また、こうした捜査当局からの要請のために必要な事項が規定され、手続が明確化された（第６条３）。ここでいう情報とは、ドメイン名の登録時に登録事業者に提出された氏名、住所、電子メールアドレス、電話番号等を指す（Explanatory Report[12]：ＥＲ81）。

上記の第６条の規定は、他国の捜査当局からの要請に対し、各締約国がドメイン名登録事業者に当該要請に応じることを義務付ける立法措置を要求するものではなく、ドメイン名登録事業者による情報開示は、国内法令に定める合理的な条件に従うこととなる。日本のドメイン名登録事業者が情報を開示するに当たっては、個人情報保護法第28条第１項に基づき、外国にある第三者に個人データを提供する場合には、あらかじめ本人の同意を得なければならない。その例外として、同法第27条第１項第１号に掲げる「法令に基づく場合」等が規定されているが、ここでいう法令には外国の法令は含まれない[13]。ドメイン名登録事業者が他国からの開示要請に協力しない場合には、その理由を示すよう要請することができるとともに、締約国間の協議を求めることができる（第６条５）。

（３）ＩＳＰが保有する情報の開示

本議定書の第７条においては、他の締約国の領域内に所在するＩＳＰが保有し、管理している加入者情報を取得するため、各締約国の捜査当局が直接命令を発する権限や手続が規定された。３.（２）で述べたように、条約の第18条には、締約国に対し、自国の捜査当局が、自国の領域内に所在する者に対し、当該者が保有・管理するデータを提出するよう命令すること、また、自国の領域内でサービスを提供するＩＳＰに対し、当該ＩＳＰが保有・管理する加入者情報を提出するよう命令することを行う権限を与えることが定められていた（条約第18条１ａ、ｂ）。しかし、この権限は自国の領域内の者又はＩＳＰへの命令に限定されており、国境を越えたアクセスを可能とする補完的なメカニズムを確立することが重要であると考えられてきた。近年、多くのサイバー犯罪に関する捜査又は刑事訴訟において、他国のＩＳＰが保有・管理するデジタル証拠を必要としており、また、完全に国内的な犯罪についても、必要なデジタル証拠が他国のＩＳＰによって保有・管理されている場合がある。そこで本議定書では、各締約国は、自国の捜査当局が他国の領域内に所在するＩＳＰに直接、加入者情報を開示するよう命令を発する権限を与えるため、また、自国の領域に所在するＩＳＰが他の締約国からの命令に応じて加入者情報を開示することができるようにするため、それぞれ必要な立法その他の措置をとることとされた（第７条１、２ａ）。ここでいう加入者情報とは、条約第18条３で定義された加入者の身元、住所、

---

[12] 欧州評議会サイバー犯罪条約委員会の説明書（Council of Europe Treaty Series No.224, Strasbourg, 12/5/2022）

[13] 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（外国にある第三者への提供編）」（平成28年11月（令和３年10月一部改正））４頁

電話番号、料金請求情報等と同様であり、通信記録及び通信内容は含まない（ＥＲ92、93）。

ＩＳＰが保有する情報開示の規定については、本議定書を締結する際に当該規定を適用しない権利を留保することができる（第７条９ａ）。日本政府は、他の締約国とＩＳＰとの直接協力について、個人情報保護法第28条第１項に基づき、外国にある第三者に個人データを提供する場合にはあらかじめ本人の同意を得なければならないこと、また、電気通信事業法第４条に基づき、電気通信事業者の取扱中に係る通信の秘密は侵してはならないこと等の現行国内法と整合性を保つため、本議定書の第７条に定める留保を付する内容の宣言を行う予定としている（第19条）。

（４）データの迅速な開示のための国際協力の強化

条約の第23条にはサイバー犯罪に関する捜査共助についての国際協力が規定され、第25条以下では相互援助に関する具体的な協力義務と手続が規定されている。本議定書においては、ＩＳＰが保有し、管理する情報であって、特に加入者情報と通信記録について迅速な提出が実現するよう、捜査当局間の国際協力を強化するための手続が定められた。具体的には、他の締約国の領域内に所在するＩＳＰが保有・管理する情報の提出命令を要請する締約国は、その要請を受ける締約国に対し、命令の送達を受けるべきＩＳＰの名称及び住所や、捜査又は刑事訴訟の対象となっている犯罪などの事項を明記した命令を提出すること（第８条３ａ）、また、捜査又は刑事訴訟に関連する事実の要約や、加入者情報又は通信記録との関連性などの事項を明記した補助的な情報（要請を行う締約国の同意なしにＩＳＰに開示してはならない）を提出すること（第８条３ｂ）等の必要な情報が明示的に規定された。また、一般に時間を要するとされる国家間の相互援助について、要請を受ける締約国が遅くとも45日以内に命令をＩＳＰに送達する努力義務が規定された（第８条６ａ）。

さらに本議定書においては、自然人の生命又は安全への重大なかつ差し迫った危険がある事態を緊急事態と定義し（第３条２ｃ）、条約における相互援助の仕組みに加え、緊急事態における相互援助の手続が定められた。本議定書の起草に当たり、テロ攻撃、病院のシステムを麻痺させるランサムウェア攻撃、誘拐犯の使用する電子メールのアカウント等を捜査する場合などの緊急事態において、ＩＳＰが保有する情報を迅速に取得する必要性が認識されていた（ＥＲ42、148）。そこで、このような緊急事態においては、条約の相互援助の手続によることなしに、条約の第35条に規定された24/7ネットワークを通じ、他の締約国の領域内に所在するＩＳＰが保有・管理するコンピュータ・データの迅速な開示を要請する規定が盛り込まれた（第９条）。また、締約国間における相互援助についても、各締約国は緊急事態が存在すると認める場合には、特に迅速な相互援助を要請することができるとされた（第10条）。

５．むすびにかえて――今後の課題

本文でも述べたとおり、外国に所在するサーバに捜査目的でアクセスし、そこに蔵置されているデータを取得する際に、権限を有する者の同意なしに直接入手したり、ＩＳＰに命じて提出を求めたりする場合には、現在の国家実行においては各国間における捜査共助

が必要とされる。その手続の効率化・迅速化を図るため、国家とＩＳＰ等の民間部門の直接協力の枠組みを構築しようとする本議定書が、各国のサイバー犯罪の捜査に資することが期待される。ただし、外国に所在するデータに直接アクセスするリモートアクセスまで認めるか否かについては結論が出ていない[14]。また、それ以前に考慮すべき課題として、サイバー空間という国境を越えて存在する領域において、コンピュータ・データという無形の情報について、出入国管理がなされている人や税関管理がなされている物を捜査する場合とデータを同様に扱うことの限界も指摘されている[15]。

インターネットの普及によるデジタル化は情報の流通を拡大させ、また、グローバルな電子商取引も急速に発展した。これと同時に個人情報の漏洩やプライバシーの侵害が問題化し、各国には個人情報保護の規制を強化することが求められた。しかし、このような厳格な個人情報の取扱いは、各国の捜査当局が捜査のために証拠となるデータを迅速に収集する行為と競合する場面が出てくる。サイバー空間における通信の秘密やプライバシーの権利、個人情報保護の観点と犯罪捜査における情報開示の関係性についても引き続き整理しながら検討していく必要がある[16]。

サイバー空間における規制として、サイバー犯罪条約にはＧ７を含む主要な西欧諸国が締約国となっているが、中国やロシアなどいわゆるサイバー大国と呼ばれる国が締結していない。むしろロシアは、2021年６月に、より広範なサイバー犯罪を取り締まる新たな国際条約案を国連に提出した。国境を越えて行われるサイバー犯罪の捜査のためには国際協力は必須であるが、国家による規制を一層強化しようとする考え方を持つこうした国々と共通項を見い出すことは困難であろう。自由や人権を擁護しつつ、的確なサイバー犯罪対策を実行していくためにも、時代に即した法秩序の形成について各国間で検討を重ねるとともに、引き続きサイバー犯罪条約や本議定書の締約国を増やしていく働きかけが求められる。

（てらばやし　ゆうすけ）

---

[14] 越境リモートアクセスの課題については、川出敏裕「ネットワーク犯罪と越境捜査」『法の支配』No.202（2021.8）、竹内真理「サイバー捜査と国家管轄権」『ジュリスト』No.1547（2020.7）を参照。
[15] 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』第73巻第４号（2020.4）81～86頁
[16] 尾崎久仁子『国際人権・刑事法概論（第２版）』（信山社、2021年）382～383頁