

「重大犯罪に対抗するための米国と英国の間の電子データへのアクセスに関する協定」の意義と影響

板倉陽一郎¹³ 寺田麻佑²³

「重大犯罪に対抗するための米国と英国の間の電子データへのアクセスに関する協定」(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)は、越境捜査に関する米国クラウド法に基づく行政協定としては初のものであり、その内容が注目されるとともに、将来締結が見込まれる日本と米国との行政協定の内容を占うにあたっても意義を有するものである。本発表では、上記協定の内容を紹介するとともに、日本への影響を考察する。

Significance and Impact of the Agreement between the United States and the United Kingdom on Access to Electronic Data for the Purpose of Countering Serious Crime

YOICHIRO ITAKURA¹³ MAYU TERADA²³

The 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 is the first administrative agreement based on the US Cloud Act concerning cross-border investigations, and its contents attract attention. It is also significant in predicting the contents of an administrative agreement between Japan and the US that is expected to be concluded in the near future. In this paper the contents of the above agreement are introduced, and the effect on Japan is examined.

1. 問題状況

1.1 「重大犯罪に対抗するための米国と英国の間の電子データへのアクセスに関する協定」の成立

2019年10月3日、米国と英国の間で、「重大犯罪に対抗するための米国と英国の間の電子データへのアクセスに関する協定」(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, 以下、「米英 DSA 協定」という。)が締結された[1]。施行は、米国議会の検証等のための期間を経て、2020年3月になると見込まれている。既に、1994年の段階で、米国と英国の間には捜査共助に関する条約が締結されているところ[2]、何故新たに米英 DSA 協定が必要であったのか。その背景には、①外国の事業者に対する越境捜査、特に海外リモートアクセス捜査が行われていること、②海外のクラウドサービスの利用が一般化していること、③米国による海外データ合法的使用明確化法(Clarifying Lawful Overseas Use of Data Act: CLOUD Act.)、通称「クラウド法」の制定が存在する。本発表では、これらの背景を概説した上で、米英 DSA 協定の意義と、我が国への影響を考察する。

1.2 外国の事業者に対する越境捜査

外国の事業者に対する越境捜査の中でも、リモートアクセスが注目される。リモートアクセスとは、刑事捜査の文脈では、電気通信回線で接続している記録媒体からの複写のことをいう(刑事訴訟法 218 条 1 項参照)。そして、海外リモートアクセスとは、文字通り、当該記録媒体が海外に所在している場合のリモートアクセスを指す。刑事事件における捜索差押は、対象が物であることを前提としている。しかしながら、現代のコミュニケーションの多くはインターネット等を通じた情報交換であることに鑑みると、刑事事件における証拠収集は、ノート PC や、これに挿入された USB メモリなどの差押えでは十分ではなく、当該ノート PC にインストールされたメールソフトが接続しに行くメールサーバからダウンロードされる電子メール等についても、当該ノート PC 又は捜査機関が用意した USB メモリや CD-R に複写した上で差し押さえ、証拠にする必要がある。この例でいえば、メールサーバが海外にある場合、海外リモートアクセス、ということになる[3]。

海外リモートアクセスのように、クラウドサービスプロバイダ等に感知されない方法もあるが、もちろん、直接的に、海外のクラウドサービスプロバイダ等に対して、日本でいえば捜査関係事項照会を送ったり、捜索差押令状を取得したりすることによって捜査するということも考えられる。このような場合について、どのように対応したかを公表している取組が、いわゆる透明性レポートである。例えば、Google は、国及び法的根拠別に、リクエストの件数を、

1 弁護士・ひかり総合法律事務所
Attorney at Law, Hikari Sogoh Law Offices

2 国際基督教大学教養学部准教授
Associate Professor of Law, College of Liberal Arts, International Christian University

3 理化学研究所革新知能統合研究センター (AIP)
RIKEN AIP

グラフによって表示する形式で透明性レポートを提供している。

リクエスト数（レポート対象期間別）

Google では、政府機関からのユーザーデータリクエストに加え、6 か月間にそのリクエストで指定されたユーザーとアカウントの総数（6 か月単位）も公開報告で開示しています。リクエストされたユーザー数とアカウント数の報告は 2011 年上半期に始まりました。

国別：アメリカ合衆国

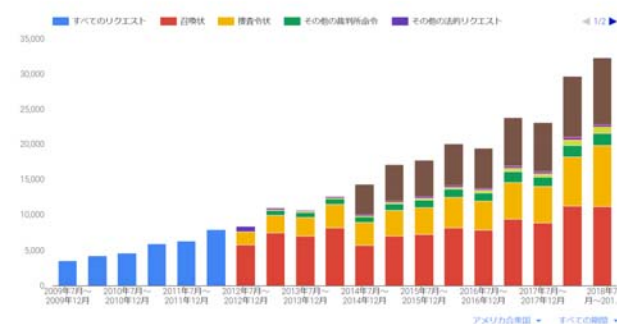


図 1 Google 透明性レポート（リクエスト数，米国）

リクエスト数（レポート対象期間別）

Google では、政府機関からのユーザーデータリクエストに加え、6 か月間にそのリクエストで指定されたユーザーとアカウントの総数（6 か月単位）も公開報告で開示しています。リクエストされたユーザー数とアカウント数の報告は 2011 年上半期に始まりました。

国別：日本

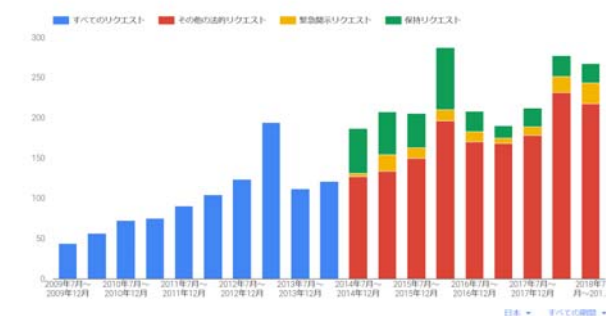


図 2 Google 透明性レポート（リクエスト数，日本）

1.3 海外のクラウドサービスの利用の一般化

クラウドサービスの利用が一般化しており、しかも、その多くは我が国からすれば海外のクラウドサービスである。具体的には、2018 年段階で、仕事で利用しているメールソフトのシェアについて「Gmail (G Suite を含む)」（38.36%）、「Outlook」（35.07%）、「iPhone (iPad) のメールソフト」（10.56%）、「Yahoo!メール」（10.11%）、「Office 365」（7.64%）であるという調査がある[4]。このうち、Gmail, iPhone のメール及び Office365 はそれぞれ、Google, Inc., Apple, Inc., Microsoft Cooperation によって運営されている。a. 同じく 2018 年の業務上で利用される法人契約のオンラインストレージについて、シェアが高い順に「Dropbox Business」（17.3%）、「Google Drive」（17.3%）、「OneDrive」（16.9%）。であるという調査がある[5]。これらはやはり、Apple, Inc., Google, Inc., Microsoft Cooperation によって運営されている。

我が国において海外のクラウドサービスを利用してい

a 例えば、Google はデータサーバの場所を公表しているが、米国、チリ、台湾、シンガポール、オランダ、フィンランド、ベルギーとしており、日本は含まれていない。Google, "Data center locations", <https://www.google.com/about/datacenters/inside/locations/> (2019 年 7 月 17 日閲覧)。

て、我が国の捜査機関から越境捜索が行われる場合、当該外国のクラウドサービスプロバイダ等（Google 等）は、越境捜査に対応しなければ我が国の刑事訴訟法に反する可能性があり、他方で、これに対応した場合主として米国のプライバシー保護法に反することがあり得る[b]。この点が裁判例に現れたのが、大阪高判平成 30 年 9 月 11 日判例集未登載（westlaw:2018WLJPCA09119002）である。ここでは、「…所論は、捜査機関による本件の海外リモートアクセスは、G 社及び D 社が米国内で保管・管理していた個人情報違法に捜査機関に提供するという米国法（連邦取引委員会法）違反を引き起こさせたという意味で、サーバ運営者・管理者の権利侵害を招いたものであり、これは、我が国における刑事法上の評価としての重大な違法を構成すると主張する。しかしながら、所論のいう情報提供に G 社及び D 社の何らかの行為が介在しているとは考え難い上、仮に何らかの行為が介在し、それが米国法上違法と評価されとしても、そのことから直ちに本件におけるリモートアクセスが刑事法上違法になるとは考えられない。」とされ、米国法（連邦取引委員会法）とのコンフリクトについて、論点とは認識されたが、違法性までは認められなかった。

1.4 米国による海外データ合法的使用明確化法 (Clarifying Lawful Overseas Use of Data Act: CLOUD Act.) の制定

クラウドサービスプロバイダ等に生じるコンフリクトは、捜査共助に関する条約によることが原則である。捜査共助条約の正規の手續を踏めば、共助の請求（要請）を出すことで、被請求国の司法当局が捜査を行うことになる（国際捜査共助等に関する法律参照）。しかしながら、一般的に、捜査共助については結果が得られるまでに長期間を費やす必要がある他、双方可罰主義（双罰主義）は原則として否定されるものの、強制捜査においては双罰主義の影響が否定できない（国際捜査共助等に関する法律 2 条 2 号は「条約に別段の定めがある場合を除き、共助犯罪に係る行為が日本国内において行われたとした場合において、その行為が日本国の法令によれば罪に当たるものでないとき。」とする）。電磁的記録が容易に消去、改ざんされることからすると、長期間が必要な捜査共助条約の手續によることは現実的ではないし、インターネット上の犯罪が双罰主義に阻まれることもままあるであろう。実際に、大阪高判平成 30 年 9 月 11 日判例集未登載（westlaw:2018WLJPCA09119002）における訴因は無修正わいせつ動画の投稿・配信に係る公然わいせつやわいせつ電磁的記録公然陳列であり、無修正アダルト画像の配信が直ちに犯罪というわけではない米国に対しては、捜査共助条約の手續が効果的に働かないものと思われる。

[b] もっとも、我が国のリモートアクセス令状は、海外リモートアクセスを想定していない。したがって、我が国で海外リモートアクセスが生じるのはイレギュラーな事態である。

このような状況は我が国以外でも同じであり、特にクラウドサービスプロバイダ等の多くが拠点を構える米国では、外国からの越境捜査と、自国のプライバシー保護法のコンフリクトを解消するための簡易な手続が強く求められた。これに応じて成立したのが、米国海外データ合法的使用明確化法（Clarifying Lawful Overseas Use of Data Act: CLOUD Act, 「クラウド法」）である。クラウド法には、事業者等が米国外で保有しているデータについて令状で強制開示を求めることができることを明確化したという意義がある他、データ・シェアリング・アグリーメント（以下、「DSA」）を締結した外国からの強制開示を認める規定を有する。当該外国からの越境捜査については、対応して情報を提供しても、クラウド事業者からのセキュリティ侵害があったとしても、違法とは評価されないという帰結が導かれる。事業者はコンフリクトを免れるわけである。先行して検討開始された欧州では、①クラウド法上の DSA ではなく、強力な手続的・実体的な基本的権利の保護規定を備えた欧米の包括的な電子証拠についての協定が重要、②欧州レベルでのアプローチが重要で、米国と加盟国の二か国のパッチワークは望ましくない、等とする EDPB 及び欧州データ保護監察官（EDPS）連名の意見（欧州議会市民的自由・司法・内務委員会（LIBE）への応答が公表されており[6]、直ちに締結できる状況には見られないが、英国との間では、初の DSA である米英 DSA 協定が締結されたというわけである。

2. 米英 DSA 協定の意義と影響

2.1 米英 DSA 協定の意義

米英 DSA 協定は全 17 条からなり、その表題は以下のとおりである。

ARTICLE 1	Definitions（定義）
ARTICLE 2	Purpose of the Agreement（協定の目的）
ARTICLE 3	Domestic Law and Effect of the Agreement（国内法と協定の効力）
ARTICLE 4	Targeting Restrictions（対象の制限）
ARTICLE 5	Issuance and Transmission of Orders（命令の発付と通知）
ARTICLE 6	Production of Information by Covered Providers（対象プロバイダによる情報の作成）
ARTICLE 7	Targeting and Minimization Procedures（ターゲティング及び最小化の手続）
ARTICLE 8	Limitations on Use and Transfer（利用及び移転の制限）
ARTICLE 9	Privacy and Data Protection Safeguards（プライバシー及びデータ保護に関するセーフガード）
ARTICLE 10	Preservation Process and Subscriber Information（保存プロセスと加入者情報）

ARTICLE 11	Compatibility and Non-Exclusivity（互換性と非独占性）
ARTICLE 12	Review of Implementation and Consultations（施行状況の監査及び協議）
ARTICLE 13	Costs（費用）
ARTICLE 14	Amendments（改正）
ARTICLE 15	Temporal Application（経過措置）
ARTICLE 16	Entry into Force（施行日）
ARTICLE 17	Expiry and Termination of the Agreement（協定の終了）

特徴的な内容としては以下が挙げられる。

本協定の目的には、通信サービスプロバイダーが、電子データの作成または保全のために行う法的プロセスにおける潜在的コンフリクトを解消し、公共の安全及びセキュリティを向上させ、プライバシー、市民的自由、オープンインターネットを保護することが最初に挙げられている（2 条 1 項）。

対象データは、コンテンツ、トラフィックデータ、メタデータ及び加入者情報を含む（1 条 3 項）。

対象プロバイダは「コンピューターシステムまたは情報通信システムを使用して、コンピューターデータを通信または処理または保存する機能を公衆に提供する」事業者が上げられている（1 条 7 項 i）。我が国でいう電気通信事業者の他、クラウドサービスプロバイダ等を含む趣旨であろう。

対象犯罪は、テロ活動を含む重大な犯罪を構成する行為とされている（1 条 5 項）。懲役 3 年以上の犯罪を意味すると指摘するものもある[7]。

命令の発付及び通知手続には、明確かつ信頼できる事実に基づくこと等が求められる（5 条 1 項）他、期間限定が必要であること（5 条 3 項）等の要件が加えられているが、命令の域外適用そのものは協定に定められていない。米国における命令の域外適用はクラウド法（による Stored Communication Act の改正）で認められており、英国でも国内法で認められている。

協定によって認められた異議申立手続が存在する（5 条 11 条）。命令の対象情報が外国人の個人データを含む場合、当該第三国の適当な当局への通知義務がある（5 条 10 項）。

2.2 米英 DSA 協定の影響

我が国が DSA を締結する場合への若干の示唆を得る。

まず、我が国からみると、協定によって、締約国の法執行機関の権限が拡充されるというわけではないということが重要である。つまり、我が国では認められていない海外リモートアクセス等、越境捜査の域外適用については国内法の手当てが必要になる。

また、英米間の場合と異なり、米国から英語でなされるであろう異議申立手続の実効性をどのように担保するのか

という問題がある。

情報を作成して提供することを前提とする条項が散見される。しかしながら、そもそも、我が国の刑事訴訟法上、そのような命令が想定されるかが問題となる。現行のリモートアクセス令状はあくまで接続先記録媒体からの複写である。

このように、クラウド法下の DSA を締結するにあたり、まずは、国内法の整備が必要な事項を洗い出し、法改正を行うのか、解釈及び運用で対応可能であるのかを検討する必要がある。その上で、対象犯罪をどのように定め、どの程度の実用を想定するか、という国際的な協議に入る必要がある。実務的には直ちに締結できる段階になかろう。

参考文献

- [1] Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime, Washington, 3 October 2019.
- [2] MUTUAL LEGAL ASSISTANCE Treaty Between the UNITED STATES OF AMERICA and the UNITED KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND, Washington 6 January 1994.
- [3] 板倉陽一郎「海外リモートアクセスをめぐる諸問題 事業者の現実的リスクとしてのサイバー事件捜査」ビジネス法務 2019 年 10 月号 144 頁。
- [4] 一般社団法人日本ビジネスメール協会「『ビジネスメール実態調査 2018』発表」(2018 年 6 月 5 日)。
- [5] スターティアホールディングス株式会社「業務におけるオンラインストレージの利用実態調査第 4 弾 (2018 年版)」(2018 年 11 月 28 日)。
- [6] EPDB-EDPS Joint Response to the LIBE Committee on the impact of the US Cloud Act on the European legal framework for personal data protection, 10 July 2019.
- [7] U.S.-UK data-sharing agreement: The final piece of the puzzle, 21 October 2019, <https://www.linklaters.com/en/insights/blogs/digilinks/2019/october/us-uk-data-sharing-agreement-the-final-piece-of-the-puzzle> (Accessed at 30 October 2019).