

米国CLOUD法による米英データアクセス協定について

古 賀 琴 乃

要 旨

2022年10月3日、「アメリカ合衆国政府とグレートブリテン及び北アイルランド連合王国政府との間の重大犯罪対策を目的とする電子データへのアクセスに関する協定（以下、米英データアクセス協定）」が発効した。米英データアクセス協定は、2018年に制定された米国の「海外データ合法的使用明確化法（以下、CLOUD法）」に基づき締結された行政協定である。米英データアクセス協定の締結により、米英間における証拠となりうるデータや通信を共有する手順における手間と時間は大幅に削減された。CLOUD法に基づく行政協定であるデータアクセス協定は、他の国々とも締結・交渉段階に至っている。本稿では、米英データアクセス協定が締結されるまでの流れを整理すると共に、米英データアクセス協定の全訳を紹介する。

キーワード：データアクセス協定（DAA）・CLOUD法・司法共助・行政協定・サイバー犯罪

1. はじめに

現在、サイバー空間で頻発する犯罪について、国境を越えて証拠を取得する手段としての国際協力には限界があると指摘されている¹⁾。このサイバー空間とは、「コンピュータネットワークに保存されるデータ及びコンピュータネットワーク内で行われる通信の総体であり、物理空間（physical realm）の特性を持つと見なされるとされる²⁾。そして、サイバー空間では国境の概念が希薄であるため、現実の物理空間から隔てられている空間であると感じさせられてしまう。そのため、サイバー空間は、無法地帯であるかのように見なされてしまっている。しかしながら、サイバー空間は、独立した空間ではなく、コンピュータネットワーク内でのデータや通信、それらを保存する場所（サーバ）によって存在している。その意味で、サイバー空間は、現実の物理空間との接点なしに存在し得ない。よって、サイバー空間上の犯罪においても、サイバー犯罪の証拠となりうるデータやデータを保存するサーバが、現実の物理空間に存在することとなる。では、

その証拠となりうるデータはどのようにして収集すれば良いのであろうか？

2. 越境サイバー犯罪捜査の必要性と課題

サイバー犯罪の捜査では、捜査当局が、犯行に及んだ疑いのある発信者に関する情報を証拠として取得する必要がある。そのため、捜査当局は、データの保存先のサーバや電子機器等から関係する事業者を通して証拠を取得することとなる。

捜査の該当サーバや電子機器等は、捜査当局の所在国ではなく、外国に所在する場合もありうる。その場合、捜査当局が外国に所在する証拠を取得するための手順は、証拠が国内に所在する場合とは異なる。一般的に、証拠等（データに限定されない）の収集に関する国際司法共助は、大きく3つの手順に分類されている³⁾。その手順は、「外交ルート」、「中央当局ルート」、「ICPOルート」の3つである。

第一に「外交ルート」とは、外交当局が、警察や検察からの要請を相手国へ依頼する手順である⁴⁾。本ルートでは嘱託書（letter rogatory or letter of request）が用いられる。嘱託書とは、捜査当局が外国に所在する証拠を取得するために、外国の裁判所に対して援助を要請する書簡である⁵⁾。我

受付2024年1月9日

が国では「外国裁判所ノ囑託ニ因ル共助法」の第1条の2第1項1号に基づき対応する⁶⁾。しかし、囑託書に応じることは国際法上の義務ではなく、証拠共有の過程では非常に時間がかかり、予測が不可能であるとされる⁷⁾。したがって、本ルートの問題点は、迅速性に欠けることであり、サイバー犯罪における証拠となるデータの取得には不向きであると考えられる。

第二に「中央当局ルート」とは、相互司法共助条約 (MLATs) に基づき、捜査当局が、外国に所在するデータを取得するための国際的な法的手続である。各国は、複雑且つ組織的な国際犯罪に対する捜査の一般化に鑑みて、国境を越えて特定の証拠を取得するためにMLATsの締結を始めた⁸⁾。MLATsでは、条約にて指定された捜査当局及び外国の中央当局が直接連絡を取り合う⁹⁾。しかし、MLATsにおいても、締約国は支援の要請を拒否する裁量を有している。そのため、囑託書と同様に、サイバー犯罪における証拠となるデータの取得に最適であるとは言い難い。

第三に「ICPOルート」とは、ICPOの枠組みの中で警察当局が、ICPOに加盟している当該外国の警察当局に、裁判官の令状なしに入手可能な資料、情報のやり取りを依頼する手順である¹⁰⁾。また、ICPOは、加盟警察機関での独自の通信網を運用すると共に、指紋やDNAなどの国際的なデータベース機能も担っている¹¹⁾。ICPOは情報収集のために、24時間年中無休のコンタクトポイントを設置しており¹²⁾、全加盟国196カ国と事務局が繋がっている¹³⁾。しかし、迅速に要請についての結果を得ることができるが、調査の結果や資料収集が目的であるため入手できる資料は複製である¹⁴⁾。

一方、データが存在するサーバの所在地が判明していない場合、上記のいずれの手順も使用できないという課題がある¹⁵⁾。さらに、MLATsは非締結国において証拠を取得することはできず、現状、全世界で相互的にサイバー犯罪における証拠を取得できる手段は存在しない。

そのような課題を踏まえて、「サイバー犯罪に関する条約 (通称：ブダペスト条約)」は、条約締約国間においてMLATsなどの条約が締結されていなくても、MLATsなどと同様の国際共助を要請できることを目的の1つとした¹⁶⁾。サイバー犯罪に関する条約第32条では、締約国の捜査

機関が、押収すべきデータが他の締約国に蔵置されていた場合、無許可で当該データを取得できる場合について規定している。サイバー犯罪に関する条約の加盟国は、2024年2月時点で全てのG7諸国を含む69カ国である¹⁷⁾。これは、主要な国に対してサイバー犯罪における証拠を取得するための網 (web) が張られていると言える。しかし、どのような場合に越境アクセスが認められないか明示されておらず、注釈書においても規定外の状況に対して中立的な立場をとっている¹⁸⁾。

上記の通り、サイバー犯罪では、捜査において発信者 (犯罪の実行者とは限らない) の特定や証拠の取得に至るまで、難解な手順や多くの時間を要求されることになる。このような国境を越える捜査では、一国の取組みでサイバー犯罪に対処することは不可能であるとされる¹⁹⁾。

先に指摘したように、サイバー空間は、物理空間であるデータセンターのサーバ内にデータとして存在する。現在、大規模のデータセンターの数は増加傾向が続いており、その53%が米国に存在する²⁰⁾。事実、米国は、外国からサイバー犯罪の捜査において、証拠となる可能性のあるデータを取得するための要請を数多く受けている²¹⁾。しかし、米国では、MLATsの不確実で煩雑な過程によって、要請の完了までに平均10か月かかる²²⁾。さらに普遍的な課題として、開示請求されたデータを所有し、保管し又は管理する企業に対して複数の国の法律が適用され、矛盾した法的義務が発生する可能性がある²³⁾。米国は以上のような課題を抱えている。そのため、今後、米国が、国境を越えて証拠を取得する手段に対する課題をどのように解消していくかは注目に値すると言えよう。

3. CLOUD法の制定と米英データアクセス協定の締結

このような状況に対応するために、米国は、2018年に「海外データ合法的使用明確化法 (Clarifying Lawful Overseas Use of Data Act) ²⁴⁾ (以下、CLOUD法)」を制定した。CLOUD法は、米国管轄下にある電子通信役務提供者又は遠隔情報処理役務事業者に対して、データの保存場所に関係なく電子データを開示すること、外国が米国内に所在する電子データへアクセスできること及び行政協定の承認手順の3点を明確化した²⁵⁾。

CLOUD法以前の米国における電子通信役務提供者又は遠隔情報処理役務事業者に対するデータの開示手順は、1986年に制定された「通信記録保管法（Stored Communications Act）」によって定められていた²⁶⁾。しかし、通信記録保管法では、立法段階で米国国内法である本法を外国に対して適用すること（域外適用）について意図されておらず、外国に対して通信記録保管法に基づく令状の執行は認められなかった²⁷⁾。さらに、前述の通り、囑託書やMLATsでは、非常に時間がかかること、開示請求をされた提供者が矛盾した法的義務に抵触する可能性があることなどの課題があった。以上の課題を解消するために、CLOUD法は、同法に基づいて締結する行政協定によって締約国双方が、重大犯罪の捜査において必要なデータを相互にアクセスすることを可能にした。

そしてCLOUD法成立後、最初に行政協定を締結した国は英国である。2019年10月3日、「アメリカ合衆国政府とグレートブリテン及び北アイルランド連合王国政府との間の重大犯罪対策を目的とする電子データへのアクセスに関する協定（米英データアクセス協定）」は署名され²⁸⁾、2022年10月3日に発効した²⁹⁾。CLOUD法による行政協定は英国のみならず、オーストラリアとは行政協定の締結に至っており、欧州連合、カナダとの間では、現在まで行政協定の締結に向けて交渉を進めている³⁰⁾。

米英データアクセス協定に署名した2019年10月3日から発効に至る2022年10月3日までの間には、行政協定の要件を満たしたという決定の書面による証明書³¹⁾や、サイドレターを用いて英国政府によって本条の要件を満たす決定の際に考慮された要因の概要³²⁾について調整を行っている。CLOUD法上、米国と外国が行政協定を締結するには、外国が、CLOUD法第105条「外国政府によるデータへのアクセスに関する行政協定」における合衆国法典第2523条第(b)項「行政協定の要件」を満たし、「適格外国政府³³⁾」と認められる必要があった。米英データアクセス協定では、当該協定が行政協定の要件を満たしており、英国が「適格外国政府」であることが認められた。

米国司法省及び英国内務省は、米英データアクセス協定締結により、重大犯罪の予防や捜査などに関する情報や証拠にこれまで以上の迅速なアクセスができるようになることでさらなる被害の防

止となることへの期待を表明している³⁴⁾。さらに、英国は、2019年犯罪（国外データ提出命令）法が使用される場合を含め、英国調査権限法委員会事務局（ICPO）に米英データアクセス協定の使用を監督する法的権限を与える新たな法律を可決した³⁵⁾。

米英データアクセス協定の使用状況としては、2023年7月時点で、英国から米国へ、捜査において米国の提供者が保有する証拠を取得するための米英データアクセス協定の条項に基づくデータ要求は7000件以上にのぼる³⁶⁾。同様に、米国から英国にも捜査上英国の提供者が所持する証拠を取得するために行政協定に基づく要請を出している³⁷⁾。

上記の情報を含むCLOUD法に関する現状は、2023年9月に韓国で開催されたサイバー犯罪への対応に関する国際シンポジウム（International Symposium on Cybercrime Response）にて、Richard W. Downing司法次官補によって語られた。Downing司法次官補は、米英データアクセス協定の現状にも触れながら、今後数ヶ月のうちに米国とオーストラリア間の行政協定の運用開始を検討していると話した³⁸⁾。また、その他の国との交渉も積極的に進めているとした。

4. 今後の展望

サイバー犯罪の捜査は、かつての犯罪捜査の手順において想定されていなかったことから、様々な課題が顕在化した。しかし、サイバー犯罪の件数は増加傾向にあり、証拠を取得する際の種々の課題を無視することはできない。その課題の1つとして、本稿で紹介した通り、自国外に存在する証拠を取得するための手順が、長時間且つ煩雑であることが挙げられる。さらに、時間の短縮が担保され、手間が省かれた手順では、限定された範囲内の資料収集が目的である。そのため、直接的に本課題が解決されたとは言い難い。

サイバー空間とは、データと通信の総体である。電磁的記録であるデータは、容易に改変されたり削除されたりしてしまう可能性が非常に高い。また、サイバー空間において、現実の物理空間に存在する国境と一致するものは存在しない。よって、サイバー空間の犯罪は、国境とは無関係に発生する。その一方で、現実である物理空間で国境を越えて証拠を取得するための手順が複雑で時間

を要するが故に、証拠の改変や削除の猶予を与えてしまうこととなる。

このような状況の中、CLOUD法に基づくデータアクセス協定は、証拠となりうるデータを取得する手段の不足という喫緊の課題に一石を投じるものであると言える。米英データアクセス協定に基づく要請数を鑑みれば、データアクセス協定の需要は非常に高く、今後、CLOUD法に基づくデータアクセス協定の増加が期待される。

現時点で、日本は米国との間でデータアクセス協定を締結するに至っていない。しかしながら、サイバー犯罪に対抗するためには、国境を越えて相互に証拠となりうるデータの取得を可能とする世界的な網の構築が必要となるであろう。

米国には、世界の過半数のデータセンターが存在している。したがって、米国の国内法であり、越境する証拠取得の網の1つとして、CLOUD法によるデータアクセス協定のさらなる動向に注目したい。以下に今後の参考として、米英データアクセス協定の全訳を紹介する。

5. 謝辞

本稿の作成に当たり、指導教員の中川智治先生には、翻訳全般、訳語について指導・アドバイスをいただきました。深く感謝申し上げます。

6. <資料>米英データアクセス協定全訳

アメリカ合衆国政府とグレートブリテン及び北アイルランド連合王国政府との間の重大犯罪対策を目的とする電子データへのアクセスに関する協定

アメリカ合衆国政府とグレートブリテン及び北アイルランド連合王国政府（以下「両当事国」という）は、

公共の安全の保護とテロリズムを含む重大犯罪と闘うことを目的とする両当事国の協力の強化に対する両当事国の相互の利益に促されて、

認可された法執行目的のための電子データへの時宜に適ったアクセスが、この取組において必要不可欠な要素であることを認識し、

プライバシー、人権及び言論の自由を含む市民的自由を尊重することの重要性、並びに、適法手続の重要性を強調し、

個人データを含む電子データの扱いについての両当事国それぞれの法に準拠した保護基準を提供すること、並びに、その目的のために適切な保護措置を提供する法的拘束力及び法的強制力のある文書を公的当局の間に作り出すことを意図し、

自由で開かれた安全なインターネットに対するデータローカライゼーションを要求することの弊害を指摘し、そのような要求を回避するよう努め、並びに、

電子データにアクセスするための両当事国のそれぞれの法的枠組みが、通信内容にアクセスする際に、適用可能な場合、必要性及び比例性の要件又は相当な理由の要件並びに過度に広範な命令（order）の制限を含むプライバシーや市民的自由を保護するための適切且つ実質的な保護措置を組み込んでおり、並びに、独立した司法的監視を組み込んでいることを認め、

以下の通り合意した。

第1条 定義

本協定は以下のことを目的とする。

1. 「アカウント」とは、例えばアカウント (an account)、電話番号、住所情報など、ユーザがコンピュータシステム又は電気通信システムへの個人的なアクセスを得るための手段をいう。
2. 「コンピュータシステム」とは、「サイバー犯罪に関するブダペスト条約」第1章第1 a

条において示された意味とする。すなわち、あらゆる全ての装置又は相互に接続された若しくは関連する一群の装置であって、プログラムに従って、そのうちの1若しくは2以上の装置がデータの自動処理を行うものをいう。

3. 「該当データ」とは、該当提供者としての役割を果たす民間事業者が所有又は管理する以下の種類のデータをいう。そのデータとは、電子通信若しくは有線通信の内容、ユーザのために保存若しくは処理されたコンピュータデータ、電子通信若しくは有線通信に関連するトラフィックデータ又はメタデータ、ユーザのために保存若しくは処理されるコンピュータデータに関連するトラフィックデータ又はメタデータ、及び、本定義で言及されるあらゆる他の種類のデータにも求める要請に従い、要求された場合の加入者情報である。
4. 「該当情報」とは、該当者が使用又は管理するアカウントの該当データをいい、要請受領国の人物が使用又は管理しないアカウントの該当データをいう。
5. 「該当犯罪」とは、要請発出国の法の下で、テロ活動を含む重大犯罪を構成する行為をいう。
6. 「該当者」とは、本協定第7条第1項により要求される手続を適用した結果、本協定第5条に基づく要請のために本協定が援用された時点で、要請受領国の人物でないと合理的に確信される者をいう。
7. 「該当提供者」とは、以下の範囲にある民間事業者をいう。
 - (i) コンピュータシステム若しくは電気通信システムによって、公衆に通信を提供する若しくはコンピュータデータの処理若しくは保存する能力を提供する民間事業者、又は、
 - (ii) 第 i 号に定める事業者に代わって該当データを処理若しくは保存する民間事業者。
8. 「指定当局」とは、英国については内務大臣により、合衆国については司法長官により、指定された政府機関をいう。
9. 「要請発出国」とは、関連する法的手続を

発出する当事国をいう。合衆国が要請発出国である場合、これには、法的手続が合衆国内の州、地方、領域、部族又はその他の当局によって発出される場合も含まれる。英国が要請発出国である場合、グレートブリテン及び北アイルランド連合王国内の州 (state) の当局によって法的手続が発出される場合を含む。

10. 「法的手続」とは、本協定の対象となる要請並びに本協定第10条により認められる保全手続及び加入者情報手続をいう。

11. 「要請」とは、保存された通信であるか現に行われている通信かを問わず、該当提供者による該当データ (当該データの認証要件を含む) の開示又は生成を要求する要請発出国の国内法に基づいて発出された法的文書をいう。

12. 「要請受領国の人物」とは、以下をいう。

合衆国が要請受領国である場合、

- (i) 州レベル、地方レベル、領域レベル、部族レベルを含む、あらゆる政府機関若しくはその当局、
- (ii) 合衆国の市民若しくは国民、
- (iii) 合法的に永住を認められた者、
- (iv) 第 ii 号若しくは第 iii 号に該当する構成員が相当数いる、法人化されていない団体、
- (v) 合衆国内で法人化された法人、又は、
- (vi) 合衆国領域内に所在する者、及び、

英国が要請受領国である場合、

- (i) 国のあらゆる政府機関若しくは当局、
- (ii) 非法人組織であって、その構成員の相当数が英国領域内に所在するもの、
- (iii) 英国領域内に所在し若しくは登録されている法人、又は、
- (iv) 英国領域内に所在するその他の者。

13. 「要請受領国」とは、要請発出国以外の当事国 (その政治的下部組織を含む) をいう。

14. 「重大な犯罪」とは、少なくとも3年以上を自由刑 (imprisonment) の最長刑期として処せられる犯罪をいう。

15. 「加入者情報」とは、該当提供者の加入者又は顧客を特定する情報をいう。その情報には、氏名、住所、サービスの期間及び種類、加入者番号又は人的属性 (identity) (割り当てられたネットワークアドレス及びデバイス

識別子を含む)、電話接続記録、セッション時間及び継続時間の記録、並びに、支払い手段などが含まれる。

16. 米国人とは、以下をいう。

- (i) 合衆国の市民若しくは国民、
- (ii) 合法的に永住を認められた者、
- (iii) 第 i 号若しくは第 ii 号に該当する構成員が相当数いる法人化されていない団体、又は、
- (iv) 合衆国内で法人化された法人。

第2条 協定の目的

1. 本協定の目的は、通信サービス提供者が一方の当事国から電子データの提出 (production) 又は保全を求める法的手続の送達を受けた場合に、これらの提供者が他の当事国の法の適用を受ける可能性がある場合の潜在的な法的義務の抵触を解決することにより、プライバシー、市民的自由、及び開かれたインターネットを保護し、並びに、公共の安全とセキュリティを向上させることである。本協定は、当事国それぞれに、自国の法及び他の当事国の法に合致する方法で、適切な対象制限に従い、重大犯罪の予防、探知 (detection)、捜査又は訴追に関連する電子データを取得するための、効率的で、実効的で、データ保護に適し、且つプライバシーを保護する手段を提供する。

2. 当事国それぞれの法の下でのあらゆる法的根拠又はその他の重要な利益の適用可能性を損なうことなく、本協定は、以下を支援する。

- a. 裁判所の司法活動及び当事国それぞれの法に基づく法的義務及び法的請求、
- b. 両当事国の実質的な公共の利益及びそれらの利益を達成するために必要な任務、並びに、
- c. 適正且つ適切に求められる正当な利益。

3. 本協定に関連する利益には、以下が含まれるが、これらに限定されない。

- a. 犯罪がその性質若しくは影響において越境的であるか否かを問わず、当事国それぞれによる重大な犯罪の予防、探知、捜査又は訴追。このような事項は、法の支配及び正義の実現に決意 (commitment) を示す両当事国の利益に関わり、並びに、重大犯罪が要請発出国の国境の外へ直接的又は間

接的に影響を及ぼしているという現実（practical reality）に関わる。

- b. 国際協力における相互性の精神，すなわち，本協定に従って電子データを入手することに対する当事国それぞれの利益は，両当事国に対し他の当事国に対しても，相互性の基盤の下で相対する方向でそのような情報を入手するための同じ法的能力（ability）を与えるよう求める。
- c. 管轄の選択によって監視から身を守ろうとする犯罪者によるデータローカライゼーションの悪用に対抗し，これを阻止するための国際協力の推進，
- d. 電子データへアクセスするシステムの確立。このシステムは，市民的自由と個人の権利を保護するため，当事国それぞれの法制度の下で適用される，例えば，相当な理由，必要性及び比例性，独立した司法的監視，並びに，個人に関するデータの取扱いと処理に関する法律の要件に組み込まれている拘束力があり適切且つ実質的な保護措置により，包括的に管理される。

第3条 国内法及び協定の効力

1. 当事国それぞれは，電子データの保全，認証，開示及び提出に関する国内法が，該当提供者が本協定の対象となる要請を遵守することを認めるように確保することを約束する。当事国それぞれは，本協定の運用を実質的に達成不能にし，又は，阻害するような国内法のいかなる重大な変更についても他方に通知するものとする。
2. 本協定の規定は，要請発出国が本協定を採用し関連ある該当事業者に通知した要請に適用する。本協定の対象となるいかなる要請の法的効果も，要請発出国の法にのみ由来する。該当提供者は，本協定の対象となる要請に対し，適用される法的異議を申し立てる既存の権利を別に保持する。
3. 本協定の執行にあたり当事国それぞれは，他の当事国の国内法（当該法の実施を含む）が，本協定の対象となるデータ収集並びに活動に照らして，プライバシー及び市民的自由のための強固な実体的保護及び手続的保護を与えていることを認める。当事国それぞれは，該当データに対する保護に著しく影響を

与える国内法のいかなる重大な変更についても他の当事国に通知し，本協定第5条又は第11条に従い，本項の下で生じるいかなる問題についても協議するものとする。

4. 本協定は，両当事国が電子データを取得する法的能力を促進することを目的とする。本協定の規定は，証拠を入手，抑圧若しくは排除すること，又は法的手続の実行を妨げることを含め，いかなる私人の側にも権利若しくは救済を生じさせるものではない。当事国それぞれは，本協定第9条の規定を含め，本協定の規定が，当事国それぞれの憲法上の構造（constitutional structure）及び憲法上の原則に合致して完全に実施されることを確保する。

第4条 標的の制限

1. 本協定の対象となる要請は，該当犯罪の予防，探知，捜査又は訴追に関連する情報を取得することを目的とするものでなければならない。
2. 本協定の対象となる要請は，言論の自由を侵害するため，又は人種，性別，性的指向，宗教，民族的出身若しくは政治的意見に基づいて不利益を与えるために使用してはならない。
3. 本協定の対象となる要請は，要請受領国の人物を意図的に標的にしてはならず，当事国は，第7条第1項に記載される本要件を実施するために設けられた対象化手続を採用するものとする。
4. 本協定の対象となる要請は，要請受領国の人物に関する情報を取得することを目的とする場合，該当者を標的にしてはならない。
5. 本協定の対象となる要請は，特定のアカウントを対象とし，要請の対象として特定の個人，アカウント（an account），住所，個人デバイス又はその他の特定の識別子を特定しなければならない。

第5条 要請の発出及び伝達

1. 本協定の対象となる要請は，要請発出国の国内法に準拠して発出されるものとし，捜査中の行為に関する理路整然とし且つ信頼に足る事実，特定性，合法性，及び厳格性に基づく合理的な正当化の要件に基づくものとする。
2. 本協定の対象となる要請は，要請発出国の

- 国内法に基づき、要請の執行に先立ち又は要請の執行に関する手続において、裁判所、判事、治安判事 (magistrate)、若しくはその他の独立した当局による審査又は監督の対象となるものとする。
3. 有線通信又は電子通信の傍受に関する本協定の対象となる要請及びその延長は、一定の限定された期間とし、承認された要請の目的を達成するために合理的に必要な限定された期間を超えて継続することはできず、同じ情報を他のより侵害の少ない他の方法で合理的に取得できない場合にのみ発出されるものとする。
 4. 要請発出国は、要請受領国若しくは第三国政府の要求のために、又は要請受領国若しくは第三国政府に提供する情報を得るために、本協定の対象となる要請を発出することはできない。
 5. 要請発出国は、本協定の対象となる要請を該当提供者に直接発出することができる。当該要請は、要請発出国の指定当局により伝達されるものとする。両当事国の指定当局は、本協定第5条第5項から第5条第9項、第6条第1項及び第6条第2項を含む各条項に基づき各々が実行する機能は、その全部又は一部を、追加の当局により実施されることにつき相互に合意することができる。両当事国の指定当局は、相互の合意により、当該当局に関する規則及び条件を定めることができる。
 6. 伝達に先立ち、要請発出国の指定当局は、要請が本協定に準拠しているかどうかを審査するものとする。
 7. 本協定の対象となるそれぞれ要請は、要請発出国の指定当局による要請が合法であり、本協定の対象となる要請に関する要請発出国の実質的な基準を含め、本協定を遵守している旨の書面による証明書 (certification) を含めなければならない。
 8. 要請発出国の指定当局は、該当提供者に対し、当該指定当局は、要請に関して本協定を援用する旨を通知するものとする。
 9. 要請発出国の指定当局は、該当提供者に対し、要請に関連する法的問題又は実務上の問題について情報を提供できる要請発出国の指定当局の連絡先を通知するものとする。
 10. 本協定の対象となる要請が、要請発出国の領域外に所在していることが合理的に考えられる個人であり且つ要請発出国の国民でない個人に関するデータに対して発出されている場合、要請発出国の指定当局は、その通知が作戦上の安全又は国家の安全保障 (national security) を害し、捜査の実施を妨げ又は人権を侵害すると要請発出国が考える場合を除き、その個人が所在する第三国の適切な当局に通知するものとする。
 11. 両当事国は、本協定の対象となる要請を受領した該当提供者が、要請に関して本協定が適切に援用されていない可能性があるとして合理的に考える場合、具体的な異議を申し立てることができることに同意する。このような異議は、一般的に要請発出国の指定当局に対して第一審で提起され且つ要請を受領後合理的な期間内に行われるものとする。該当提供者から要請に対する異議申立てを受領した場合、要請発出国の指定当局はその異議申立てに応答するものとする。異議が解決されない場合、両当事国は、該当提供者が要請受領国の指定当局に異議を申し立てることに同意する。両当事国の指定当局は、当該異議申立てのいずれかを解決するよう協議し、定期的に会合し、本協定に基づき提起されたいかなる問題についても必要に応じて議論し検討する。
 12. 要請受領国の指定当局が、いかなる要請に関しても本協定は適切に援用することができないと結論づけた場合、要請発出国の指定当局及び関連ある該当提供者にその旨を通知するものとし、本協定は当該要請には適用されないものとする。

第6条 該当提供者による情報提出

1. 両当事国は、本協定の対象となる要請に応じて該当提供者が提出するいかなる該当データも、要請発出国の指定する機関に対して直接的に提出されるものとすることに同意する。
2. 要請発出国の指定当局は、適用法に両立する形で、本協定の対象となる要請の安全な伝達及び本協定の対象となる要請に応じて提出される該当データの安全な伝達について、該当提供者と取極を行うことができる。

3. 本協定は、要請発出国の法に従って発出された法的手続に応じてデータを提出する該当提供者のあらゆる法的義務を制限又は排除するものではない。
4. 該当データの提出方法に関する要請発出国の要件には、該当提供者が提出された記録の真正性を証明する書式又は当該記録の欠如若しくは非存在を証明する書式への記入が含まれる場合がある。

第7条 対象化手続と最小化手続

1. 当事国それぞれは、適切な対象化手続を採用し実施するものとする。当該手続により、本協定の対象となる要請により対象とされたいかなるアカウントも該当者によって使用又は管理されていることを確認するよう誠実且つ合理的な努力が行われるものとする。
2. 英国は、該当犯罪の予防、探知、捜査又は訴追に関連する該当情報を取得、保持及び流布するという英国の必要性と一致するように、本協定の対象となる要請に従って取得された米国人に関する情報の取得、保持及び流布を最小限に抑えるための適切な手続を採用し、実施するものとする。
3. 本協定の対象となる要請に従って取得された情報の最小化手続は、以下の資料を分離、封印又は削除し、流布しないことを英国に義務付ける規則を含むものとする。その資料とは、該当犯罪の予防、探知、捜査若しくは訴追に関連する情報の重要性、若しくは、あらゆる人の死の恐れ、若しくは、重大な身体的・物理的危険の恐れから保護するために必要な情報、若しくは、当該情報の重要性を理解若しくは評価するための情報ではない又はそのために必要となる情報ではないと判明した資料である。
4. 最小化手続は、本協定の対象となる要請に従って収集された資料の速やかな審査を英国に求める規則が含まれ、更に、いかなる未審査の通信も適用できる手順について訓練を受けた者のみがアクセスできる安全なシステムに保存するものとする。
5. 最小化手続は、以下の場合を除き、英国が合衆国に本協定の対象となる要請に従って取得された米国人の通信の内容を広めてはならないという条項を含むものとする。その例外

とされる場合とは、最小化手続に基づいて通信が流布される可能性がある場合、及び、通信が、テロリズム、重大な暴力犯罪、児童搾取、越境組織犯罪若しくは重大な金融詐欺などの国家の安全保障に関わる犯罪を含む、合衆国若しくは米国人に対する重大な危害又はその脅威に関連する場合である。

6. 当事国それぞれは、他の当事国と協議の上、承認を得て、本条によって要求される対象化手続及び最小化手続を作成するものとする。当該手続のいかなる変更についても、他の当事国による承認を得るものとする。

第8条 使用及び移送の制限

1. 本協定のいずれかで特定された制限を損なうことなく、本協定の対象となる要請に基づき要請発出国が取得したデータは、プライバシー及び情報公開法（freedom of information laws）を含む要請発出国の国内法に従って取扱われるものとする。
2. 要請発出国は、本協定の対象となる要請に従って受領したデータを、そのデータが要請発出国の国内法により既に公表されている範囲を除き、あらかじめ要請受領国の同意を得ることなく、第三国又は国際機関に移送しないものとする。
3. 要請発出国は、本協定の対象となる要請に従って提出されたいかなる情報も、要請受領国又は第三国政府と共有することを求められないものとする。
4. 要請発出国が、該当提供者から法的手続に従いデータを受領した場合に、
 - a. 英国が、死刑が求刑される犯罪について、当該データが合衆国における検察側陳述の証拠として提出されることで、英国の本質的利益が侵害される可能性があると言っている場合、又は、
 - b. 合衆国が、合衆国にとって言論の自由に関する懸念を合衆国に生じさせるような方法で、当該データが英国における検察側陳述の証拠として提出されることで、合衆国の本質的利益が侵害される可能性があると言っている場合、要請発出国は、これらの本質的利益に反する又は反する可能性のある方法でデータを使用する前に、要請受領国の指定当局を通じて、

使用許可を得るものとする。要請受領国の指定当局は、必要とみなされる条件に従い許可を与えることができ、許可を与えた場合、要請発出国はその条件に従ってのみ当該データを提出することができる。要請受領国が承認を与えない場合、要請発出国は、法的手続に従って受領したデータをそのような方法で使用してはならない。

5. 両当事国が相互に合意した範囲において、本協定に明記された使用制限に加えて、使用制限を課すことができる。

第9条 プライバシー及びデータ保護の保護措置

1. 2016年6月2日にアムステルダムで締結された犯罪の予防、捜査、探知及び訴追に係る個人情報の保護に関するアメリカ合衆国と欧州連合との間の協定は、本協定の対象となる要請の執行において提出されるすべての個人情報に細部に必要な変更を加えて (*mutatis mutandis*) 適用され、同等の保護を提供する。合衆国にとって、本文脈において同協定第19条を実施する主要な法は、2015年司法救済法及び情報公開法である。
2. 本協定の対象となる要請の履行におけるデータの処理並びに移送は、プライバシー及びデータ保護に関する両当事国のそれぞれの適用法に適合する。

第10条 保存手続及び加入者情報

1. 当事国それぞれは、電子データの保存、認証、開示及び提出に関する国内法が、以下の点につき、要請発出国の国内法に基づく法的手続に関して、該当提供者が遵守することを認めるよう確保することを約束する。
- a. 該当データ若しくは加入者情報の保存、又は、
- b. 犯罪の予防、探知、捜査若しくは訴追に関連する加入者情報の開示、提出若しくは認証。
2. 要請発出国は、該当提供者に直接当該手続を発出することができる。当該手続は、要請発出国の国内法に準拠して発出され、審査又は監視の対象となる。当該手続のいかなる法的効力も、要請発出国の法にのみ由来する。なお、該当提供者は、適用される法的異議を申し立てる既存の権利を保持する。
3. 当該手続は、合理的なものでなければなら

ず、犯罪の予防、探知、捜査又は訴追に関連する情報を取得する目的で発出されなければならない。

4. 当該手続は、言論の自由を侵害したり又は人種、性別、性的指向、宗教、民族的出身若しくは政治的意見に基づいて不利益を与えたりするために用いてはならない。
5. 当該手続に従って取得された加入者情報は、プライバシー及び情報公開法を含む要請発出国の国内法並びに本協定の適用規定に従って取扱われるものとする。
6. 要請発出国並びに該当提供者は、適用法に従い、当該手続及びこれに応じて提出される加入者情報の安全な送信について取極を行うことができる。
7. 要請発出国は、要請受領国又は第三国政府と加入者情報を共有することを求められないものとする。
8. 当事国それぞれは、保存された該当データ若しくは加入者情報の保護に重大な影響を与える、又は、当該手続の運用を実質的に阻害若しくは損なうような国内法のいかなる重大な変更についても、他の当事国に通知するものとし、本項の下で生じるあらゆる問題について協議するものとする。
9. 2016年6月2日にアムステルダムで締結された犯罪の予防、捜査、探知及び訴追に係る個人情報の保護に関する合衆国と欧州連合との間の協定は、当事国によって、当該手続に従って保存されたすべての保存された個人情報及び当該手続に従い提出された加入者情報に細部に必要な変更を加えて適用される。合衆国にとって、本文脈において同協定第19条を実施する主要な法は、2015年司法救済法及び情報公開法である。
10. 本条及び同法の履行を含む当事国の国内法で認められた保護措置に照らし、当該手続に関連して、プライバシーと市民的自由のための強固な実体的・手続的保護が存在する。当該手続に従ったデータの処理及び移送は、プライバシー及びデータ保護に関する当事国それぞれの適用法に適合する。
11. 加入者情報の提出方法に関する要請発出国の要件には、該当提供者が、提出された記録の真正性を証明する書式又は当該記録の欠如

若しくは非存在を証明する書式への記入が含まれる。

第11条 互換性及び非独占性

1. 本協定は、要請発出国が要請受領国から並びに要請受領国の管轄下にある該当提供者から電子データを取得し又は保存するために用いる他の法的当局及び法的メカニズムを損なうものではなく並びに影響を与えないものとする。そこには、いずれか一方の当事国の国内法での法的文書及び慣行であって、当該当事国が本協定を援用しない場合、当該当事国が相互法的な法的支援を要請する場合及び緊急開示の場合も含まれる。
2. 本協定は、本協定の対象となる要請から生じる強制措置、当該保存手続及び本協定第10条で認められた加入者情報に関して、協議、消尽並びに、1994年1月6日にワシントンで署名され、2004年12月16日にロンドンで署名された、アメリカ合衆国政府とグレートブリテン及び北アイルランド連合王国政府との間の刑事事件に関する相互司法共助に関する条約に関して、2003年6月25日に署名されたアメリカ合衆国と欧州連合との間の相互司法共助協定の第3条第2項が意図する同協定付属書第18条第2項、第3項、第4項、第5項並びに第6項のその他の要件を構成するものとする。

第12条 実施の監査及び協議

1. 両当事国は、本協定発効後1年以内及びその後定期的に、本協定の条項の当事国それぞれの履行の見直しに取り組むものとする。これには、本協定の目的及び条項が履行されていることを確認するための本協定の対象となる要請の発出及び移転の審査並びに本協定の下で採用された手続を修正するか否かを決定するための本協定の対象となる要請に従って取得されたデータに対する当事国の取扱いの審査が含まれる。
2. 両当事国は、必要に応じていつでも本協定の履行に関して又は紛争を解決するために協議することができる。本協定の履行に関するいかなる紛争も、いかなる裁判所、法廷又は第三者にも付託されないものとする。
3. 本協定の実施に関する懸念又は紛争を両当事国が解決できない場合、いずれか一方の当

事国は、特定の日付又はそれ以降に発出された法的手続を含め、特定区分の法的手続に関して本協定を援用することができないと結論付けることができる。当該結論の通知は、そのような結論を下した当事国の指定当局によって、他の当事国の指定当局に送付されなければならない。通知を受けた当事国は、当該通知を受領した時点で、特定された区分内の法的手続に関して本協定を援用しないものとする。このような結論は、他の当事国の指定当局への取消の通知を通じて、結論に達した当事国により、いつでも、その全部又は一部を取消することができる。要請発出国に提出されたいかなるデータも、本協定に定められた最小化手続を含む条件及び保護措置に引き続き従うものとする。

4. 要請発出国それぞれの指定当局は、運用上又は国家の安全保障上支障のない範囲で、本協定の使用に関する集計データを反映した年次報告書を要請受領国の指定当局に提示するものとする。

5. 本協定は、適用法に基づき、該当提供者が受領した法的手続に関する統計情報を報告することを、いかなる方法においても制限又は排除するものではない。

第13条 費用

当事国それぞれは、本協定の運用から生ずる費用を自ら負担するものとする。

第14条 改正

本協定は、両当事国の書面による合意により、いつでも改正することができる。

第15条 経過措置

本協定は、本協定の発効日以降に要請発出国が発出する法的手続に適用される。

第16条 効力の発生

本協定は、当事国それぞれが本協定の効力を発生させるために必要な措置を講じたことを示す両当事国間の外交書簡の交換を完了される後の書簡の日付をもって効力を生ずる。

第17条 協定の満了及び終了

1. 本協定は、5年間の効力を有するものとする。但し、本協定が満了する前に、両当事国が、書面にて、外交書簡の交換を通じて、本協定を更に5年間（又は両当事国間で合意されるその他の期間）延長する場合はこの限り

でない。

2. 本協定は、第1項に基づく満了とは別に、いずれかの当事国が外交経路を通じて他の当事国に対して書面による通告を行うことにより、本条約を終了される。終了は、当該通知の日から1箇月後に効力を生ずる。
3. 本協定が満了又は終了した場合、要請発出国に対して提出されたいかなるデータも引き続き使用することができ、本協定に定めた最小化手続を含む条件及び保護措置に引き続き従うものとする。

以上の証拠として、下名は、各自の政府から正当に委任を受け、本協定に署名した。

2019年10月3日、ワシントンにて、英語で、本書2通を作成した。

アメリカ合衆国政府のために

William P. Barr

グレートブリテン及び北アイルランド連合王国政府のために

Priti Patel

7. 脚注

- 1) 石井 [2023a], 102-103頁。
- 2) Prucher. [2007], p.31.
- 3) 中野目・四方 [2021], 199頁。
- 4) 法務省法務総合研究所 [2004]。一般的に、検察庁の依頼によって共助の要請をする場合は、検察庁から法務省、外務省、在外日本公館、相手国の外務省へ、警察の依頼による場合は、都道府県警察から警察庁、外務省、在外日本公館、相手国の外務省という順を追って、当該国の司法当局等が捜査を実施する。
- 5) U. S. [2018], Congressional Research Service, “Cross-Border Data Sharing Under the CLOUD Act.”
- 6) 外務省 [2018]。
- 7) U. S. [2019], Department of Justice, “Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act, White Paper.”
- 8) *Ibid.*
- 9) *supra* note 5.
- 10) 法務省法務総合研究所 [2004]。
- 11) 法務省法務総合研究所 [2023], 109頁。
- 12) 寺林 [2023] 14-15頁。
- 13) INTERPOL [*s.d.*], “INTERPOL-Five actions for a safer world.”
- 14) 中野目・四方 [2021], 205頁。
- 15) 中野目・四方 [2021], 131頁。
- 16) サイバー犯罪に関する条約第39条第1項「この条約の効果」。
- 17) Council of Europe [*s. d.*], “Parties/Observers to the Budapest Convention and Observer Organisations to the TCY”.
- 18) 筋 [2022], 185-186頁。
- 19) Downing. [2023], “Remarks of Deputy Assistant Attorney General.”
- 20) 総務省 [2023], 127頁。
- 21) *supra* note 7.
- 22) *Ibid.*
- 23) *Ibid.*
- 24) U.S. [2018], Consolidated Appropriations Act, Pub.L. No. 115-141, 132 Stat 1213.
- 25) CLOUD法の規定した域外適用の明確化については、尾崎・小向 [2023], 139-141頁参照。
- 26) U. S. [2002], 21st Century Department of Justice Appropriations Authorization Act, Pub.L. No.107-273, 116 Stat 1806.
- 27) U.S. [2016], Court of Appeals of 2nd Cir., “Microsoft Corp. v. United States (*In re* Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.),” Federal Reporter 3rd, vol.829, pp.197-233.
- 28) U. S. [2022], Department of Justice, Office of Public Affairs, “U.S. And UK Sign Landmark Cross-Border Data Access Agreement to Combat Criminals and Terrorists Online.”
- 29) 米英データアクセス協定の意義と影響については、板倉・寺田 [2019], 3-4頁参照。
- 30) *supra* note 19.
- 31) CLOUD法第103条「記録の保存、法的手続の礼讓分析」第b項における合衆国法典第2703条第h項「礼讓分析及び有線通信又は電子通信の内容を求める法的手続に関連する情報の開示」第1号から第4号それぞれの考慮事項の書面による証明及び説明を含む証明書。
- 32) CLOUD法第105条「外国政府によるデータへのアクセスに関する行政協定」における合衆国法典第2523条第(d)項「認証の発効日」第3号。
- 33) CLOUD法第103条「記録の保存、法的手続の礼讓分析」第b項における合衆国法典第2703条第h項「礼讓分析及び有線通信又は電子通信の内容を求める法的手続に関連する情報の開示」。
- 34) U. S. [2022], Department of Justice, Office of Public Affairs, “Joint Statement by the United States and the United Kingdom on Data Access Agreement.”; U. K. [2022] Government, Home Office, Home Office, “Policy factsheet on the UK-US Data Access Agreement.”
- 35) U.K. [2022], Government, Home Office, Home Office, “Policy factsheet on the UK-US Data Access Agreement.”
- 36) *supra* note 19.
- 37) *Ibid.*
- 38) *Ibid.*

8. 参考文献

- 有本真由 [2019] 「域外リモートアクセスによる証拠収集にかかるCLOUD法に基づく行政協定に関する一考察」『情報ネットワーク・ローレビュー』Vol.18。
- 石井由梨佳 [2023a] 「刑事捜査における外国事業者からの通信情報取得—直接協力 (direct cooperation) の国際法上の課題—」『国際法研究』信山社, No.12。
- 石井由梨佳 [2023b] 「国際法学の観点から—越境リモートアクセスの評価」[指宿信・板倉陽一郎編『越境するデータと法——サイバー捜査と個人情報を考える』, 法律文化社, 171-186頁]。

- 板倉陽一郎・寺田麻佑 [2019] 『「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』『研究報告電子化知的財産・社会基盤 (EIP)』 Vol. 2019-EIP-86, No.6。
- 尾崎愛美・小向太郎 [2023] 「米国——越境捜索とCLOUD法」[指宿信・板倉陽一郎編『越境するデータと法——サイバー捜査と個人情報を考える』, 法律文化社, 131-170頁]。
- 外務省 [2018] 「外国の裁判所が日本に裁判文書の送達及び証拠調べを要請する方法」, https://www.mofa.go.jp/mofaj/ca/cp/page25_001296.html, 最終閲覧: 2024年2月28日。
- 株式会社ITリサーチ・アート [2022] 「米英のデータアクセス協定—法執行機関への直接情報提供要請」, <https://itresearch.biz/?p=4006>, 最終閲覧: 2024年2月28日。
- 筋伊知朗 [2022] 『サイバー犯罪——現状と対策——』, ミネルヴァ書房。
- 総務省 [2023] 『令和5年版 情報通信白書 ICT白書』, <https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r05/pdf/00zentai.pdf>, 最終閲覧: 2024年2月28日。
- 寺林裕介 [2023] 「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—」『立法と調査』 No.455。
- 中野目善則・四方光 [2021] 『サイバー犯罪対策』, 成文堂。
- 西村高等法務研究所CLOUD Act研究会 [2023] 『報告書: 企業が保有するデータと捜査を巡る法的課題の検討と提言』, Ver.2.0, 西村高等法務研究所, <https://www.nishimura.com/sites/default/files/articles/file/92692.pdf>, 最終閲覧: 2024年2月28日。
- 法務省法務総合研究所 [2004] 『平成16年版 犯罪白書』, https://hakusyo1.moj.go.jp/jp/48/nfm/n_48_2_2_6_3_1.html, 最終閲覧: 2024年2月28日。
- 法務省法務総合研究所 [2023] 『令和5年版 犯罪白書』 <https://www.moj.go.jp/content/001407767.pdf>, 最終閲覧: 2024年2月28日。
- Council of Europe [s. d.], “Parties/Observers to the Budapest Convention and Observer Organisations to the T-CY”, <https://www.coe.int/en/web/cybercrime/parties-observers>, last visited Feb.28, 2024.
- Downing, Richard. W. [2023], “Remarks of Deputy Assistant Attorney General,” <https://www.justice.gov/media/1315386/dl?inline>, last visited Feb.28, 2024.
- INTERPOL [s. d.], “INTERPOL-Five actions for a safer world,” <https://www.interpol.int/Who-we-are/What-is-INTERPOL/INTERPOL-Five-actions-for-a-safer-world>, last visited Feb.28, 2024.
- Prucher, Jeffery. R. [2007], *Brave New Words: The Oxford Dictionary of Science Fiction*, Oxford University Press, p.31.
- U.K. Government. [2022], Home Office, “Policy factsheet on the UK-US Data Access Agreement,” <https://www.gov.uk/government/publications/uk-us-data-access-agreement-factsheet/policy-factsheet-on-the-uk-us-data-access-agreement>, last visited Feb.28, 2024.
- U.S. [2018], Congressional Research Service, “Cross-Border Data Sharing Under the CLOUD Act,” <https://sgp.fas.org/crs/misc/R45173.pdf>, last visited Feb.28, 2024.
- U.S. [2018], Consolidated Appropriations Act, Pub.L. No.115-141, 132 Stat 1213, <https://www.govinfo.gov/content/pkg/PLAW-115publ141/pdf/PLAW-115publ141.pdf>, last visited Feb.28, 2024.
- U.S. [2016], Court of Appeals of 2nd Cir., “Microsoft Corp. v. United States (*In re* Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.),” *Federal Reporter 3rd*, vol.829, pp.197-233.
- U.S. [2022], Department of Justice, Office of Public Affairs, “Joint Statement by the United States and the United Kingdom on Data Access Agreement,” <https://www.justice.gov/opa/pr/joint-statement-united-states-and-united-kingdom-data-access-agreement>, last visited Feb.28, 2024.
- U.S. [2022], Department of Justice, Office of Public Affairs, “U.S. And UK Sign Landmark Cross-Border Data Access Agreement to Combat Criminals and Terrorists Online,” <https://www.justice.gov/opa/pr/us-and-uk-sign-landmark-cross-border-data-access-agreement-combat-criminals-and-terrorists>, last visited Feb.28, 2024.
- U.S. [2018], Department of Justice, Office of Treaty Affairs, “Treaty Procedures,” <https://www.state.gov/treaty-procedures/>, last visited Feb.28, 2024.
- U.S. [2019], Department of Justice, “Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act, White Paper,” <https://www.justice.gov/opa/press-release/file/1153446/download>, last visited Feb.28, 2024.
- U.S. [2002], 21st Century Department of Justice Appropriations Authorization Act, Pub.L. No.107-273, 116 Stat 1806, <https://www.govinfo.gov/content/pkg/PLAW-107publ273/pdf/PLAW-107publ273.pdf>, last visited Feb.28, 2024.