

## 〔論 説〕

米英・米豪協定から推測される米国クラウド法上の  
行政協定締結に向けた課題

—電子証拠の迅速な越境捜査の実現に向けて—

中央大学法学部 教授

四 方 光

- I はじめに：問題の所在
- II 米国クラウド法の仕組
  - 1 クラウド法の概要
  - 2 行政協定の締約国に求められる要件（相手国要件）
  - 3 行政協定の内容に求められる要件（協定要件）
- III 米英協定
  - 1 米国における英国に対する相手国要件の検討
    - (1) 2016年捜査権限法（Investigatory Powers Act 2016）
    - (2) 2019年犯罪（海外提供命令）法（Crime（Overseas Production Orders）Act 2019）
    - (3) 2018年データ保護法（Data Protection Act 2018）
  - 2 米英協定の内容
- IV 米豪協定
  - 1 米国におけるオーストラリアに対する相手国要件の検討
    - (1) 2021年電気通信法改正法（国際提供命令）（IPO法）（Telecommunications Legislation Amendment（International Production Orders）Act 2021（IPO Act））
    - (2) 1988年プライバシー法（Privacy Act 1988）
  - 2 米豪協定の内容
- V 日米協定への示唆
- VI 資 料
  - 1 重大犯罪対策のための電子データへのアクセスに関するアメリカ合衆国政府と英国政府との間の協定
  - 2 重大犯罪対策のための電子データへのアクセスに関するアメリカ合衆国政府とオーストラリア政府との間の協定

## I はじめに：問題の所在

サイバー空間における捜査は、現実世界での捜査よりも格段に難しいが、その主たる原因となっているのが、国境を越えて行う捜査（越境捜査）の困難性である。インターネット上では、情報は国境を越えて世界中を駆け巡っており、サイバー犯罪の犯罪者も世界中の様々な国の国境をまたいでサイバー犯罪を敢行している。しかし、捜査機関にとっては厳然とした国境の壁がある。それは、捜査という行為は国家主権の発動の最たるものであり、強制捜査はもちろろん、任意捜査であっても外国では行うことができないのが原則だからである。したがって、国境を越えて何らかの捜査を行おうとすると、その捜査に当たる行為の一つ一つについて、当事国両国の中央政府機関の判断を経る国際捜査共助の手続を行わなければならない、一つの捜査共助について数か月を要するのが通常である。電子証拠の典型である通信ログの保存期間はプロバイダによって異なるが、比較的短期間であることが多く、上記の国際捜査共助の手続を一つ行っている間に犯罪に係る通信ログ全体が消去されてしまい、犯罪者を追跡することができなくなる。これが今日におけるサイバー犯罪捜査の現実であり、同様の問題は、インターネットやクラウドサービスを利用した現実世界の犯罪の捜査においても生じている。

このような越境捜査の問題を解決する方法の一つとして期待されているのが、各国の捜査機関が外国のプロバイダから直接に電子証拠を入手する方法であり、米国クラウド法は同法に基づく行政協定を締結した国の捜査機関には米国のプロバイダに対してそのような捜査手法を認めている。我が国も、越境捜査の困難性を軽減するためには、クラウド法に基づく行政協定を米国と締結することが望まれる。

本稿は、今日までに締結されている米英協定と米豪協定を分析することを通じて、将来における日米協定締結に向けて、日本においてどのような準備が必要なのかを検討するものである。

## Ⅱ 米国クラウド法の仕組

### 1 クラウド法の概要

上述のとおり、捜査機関の活動が他国の領域に及ぶと、国家主権の問題が生じる。そこで、捜査機関の活動を外国に及ぼそうとするのではなく、国内で適法にできる捜査を海外のプロバイダに対して行うことにより、国際企業たる海外のプロバイダにおいて電子証拠を越境させれば、国家主権の問題は生じない。

ところが、今日では各国とも個人情報の海外移転を容易には認めない個人情報保護法制を整備しているため、プロバイダが国内法の適用関係では私人と同様の扱いとなる外国の捜査機関に協力して電子証拠を越境移転すると、このような個人情報保護法制に反することになる。そのため、外国で営業を行うプロバイダが当該外国の捜査機関から令状の執行を受けてこれに応じると、当該プロバイダの所在する国の個人情報保護法制に反することになるという「義務の相反」が生じることとなる。

国際的なプロバイダの大半は米国にあるが、米国所在のプロバイダは米国の個人情報保護法制に服するので、外国の捜査機関から令状の提示を受けてもそれに従うことができないことがあった。そのため、米国に対して国際捜査共助要請が殺到し、米国の司法当局も大量の共助要請を処理しきれない困難に直面することとなっている。

以上の問題を解決するために制定されたのが、米国クラウド法である<sup>1)</sup>。同法は、米国のプロバイダに対し、一定の要件を満たし行政協定を締結した外国の政府機関からの要請に応じて、メール等の保管通信等に係る情報（米国民・米国居住者の情報を除く。）を開示することを許容したのである。具体的には、第一に、クラウド法による改正後の米国連邦法 18 編 121 章 2702 条 (b) 項 (9) 号において、米国のプロバイダが、「一定の要件を満たした外国政府」に対して、当該外国政府において発せられた開示命令（order）がある場合に、通信の内容を任意に開示することを認める旨規定し、同条 (c) 項 (7) 号において、

---

<sup>1)</sup> 中野目善則、四方光編著『サイバー犯罪対策』（成文堂、2021年）254-257頁、四方光「法執行における個人情報の越境移転の諸手法」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保護を考える』（法律文化社、2023年）293-305頁など参照。

顧客の記録を任意に開示することを認める旨規定することとなった。

第二に、同法 119 章において、行政協定を締結した外国政府機関の要請に応じることは、2511 条の定める通信の秘密を侵す罪に当たらないこととされた（同条 (2) (j) 項）。

第三に、同法 206 章において、行政協定を締結した外国政府機関に応じてする場合には、通信記録装置の設置は禁じられない旨規定された（3121 条 (a) 項）。

クラウド法に対しては、米国内においても賛否両論がある。主な賛成意見<sup>2)</sup>は、第一に越境証拠移転が格段に迅速に行われるようになること、第二に他国がその国内で米国の通信プロバイダに対して令状執行した場合に、当該プロバイダが令状発出国からの令状と米国の個人情報保護法との板挟みから救われることを根拠にしている。

これに対し、主な反対意見<sup>3)</sup>は、第一に米国のプロバイダに対して強制捜査が行われるのに米国の裁判所による審査がないこと、第二に情報提供の対象が一応米国民・米国居住者以外とされているが、その制約が守られているかは令状発出国及び令状を受けたプロバイダの判断に委ねられており、米国民・米国居住者に対する捜査が米国の裁判所の審査を受けないで行われることがあり得ることに向けられている。米国政府は、反対意見の第一に対しては、強制捜査が行われるのはあくまで各国の国内であって各国の捜査機関に対して相手国に対する越境捜査権を与えたものではなく、クラウド法は、プロバイダが外国において外国の令状に応じて米国から当該外国に個人情報を移転することを認め

---

<sup>2)</sup> Jennifer Daskal & Andrew K. Woods. 2015. Cross-Border Data Requests: A Proposed Framework. Just Security <https://www.justsecurity.org/27857/cross-border-data-requests-proposed-framework/>, Daskal, Jennifer, 2017, Access to Data Across Borders: The Critical Role for Congress to Play Now. *Journal of ACS Issue Briefs* <[https://www.acslaw.org/wp-content/uploads/2017/10/Access\\_to\\_Data\\_Across\\_Borders.pdf](https://www.acslaw.org/wp-content/uploads/2017/10/Access_to_Data_Across_Borders.pdf)>, Daskal, Jennifer & Swire, Peter. 2019. The U.K.-U.S. CLOUD Act Agreement Is Finally Here, Containing New Safeguards. *Lawfare* <<https://www.lawfaremedia.org/article/uk-us-cloud-act-agreement-finally-here-containing-new-safeguards>>参照。

<sup>3)</sup> Lin, Tiffany, and Maily Fidler. 2017. *Cross-Border Data Access Reform: A Primer on the Proposed U.S.-U.K. Agreement*. A Berklett Cybersecurity publication, Berkman Klein Center for Internet & Society. <<https://dash.harvard.edu/handle/1/33867385>>, Center for Democracy & Technology, 2016. *Cross-Border Law Enforcement Demands: Analysis of the US Department of Justice's Proposed Bill* <<https://cdt.org/wp-content/uploads/2016/08/DOJ-Cross-Border-Bill-Insight-FINAL2.pdf>>, Camille Fischer, 2018. *The CLOUD Act: A Dangerous Expansion of Police Snooping on Cross-Border Data*. Electronic Frontier Foundation <<https://www.eff.org/deeplinks/2018/02/cloud-act-dangerous-expansion-police-snooping-cross-border-data>>など参照。

るに過ぎないとしており<sup>4)</sup>、それによって移転が認められる個人情報の対象を米国民・米国居住者以外の者に限定することで米国憲法上の米国民・米国居住者のプライバシー保護の問題を回避しようとしているものと考えられ、結局第二の批判を回避できるかどうかにかかっている。そこで、この第二の批判に対処するため、米英協定・米豪協定は、後で見るように、一つにはプロバイダによる異議申立て手続を、二つ目には情報を受けた国における情報の取扱いの拡大を制限する「最小化手続」を設けているものと考えられる。日米協定締結に当たっても、プロバイダによる異議申立て手続と情報を受けた国における当該情報の取扱いの最小化手続が求められることとなるであろうから、国内法に所要の担保規定を置く必要が生じるであろう。

行政協定の要件については、クラウド法による改正後の米国連邦法 18 編 119 章 2523 条 (b) 項に下記のような事項が定められている。そこで、米英協定や米豪協定において、下記の要件がどのように検討され、どのような規定が置かれているかを分析すれば、将来日米協定を締結する際に検討が必要な論点を予測することができる<sup>5)</sup>。

## 2 行政協定の締約国に求められる要件（相手国要件）

行政協定の要件を定めた米国連邦法 18 編 119 章 2523 条 (b) 項は、まず行政協定を締結する相手国の要件として、次の各号をすべて満たすことを求めている（同項 (1) (B)）。本項は、行政協定を締結する外国がこれらの要件を満たすことを求めているから、日本が日米協定を締結するためには、締結前にこれらの要件を満たしている必要があるものと考えられる。

- (i) 2001 年 11 月 23 日にブダペストで締結され 2004 年 1 月 7 日に施行されたサイバー犯罪条約の締約国として適切なサイバー犯罪及び電子証拠に

---

<sup>4)</sup> U.S. Department of Justice. 2019 . “Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act” <[https://www.justice.gov/d9/pages/attachments/2019/04/10/doj\\_cloud\\_act\\_white\\_paper\\_2019\\_04\\_10.pdf](https://www.justice.gov/d9/pages/attachments/2019/04/10/doj_cloud_act_white_paper_2019_04_10.pdf)>

<sup>5)</sup> クラウド法が二国間の約束の形式を「行政協定」としているのは、米国では「行政協定」とはいつでも他の各国にとっては条約と同等の議会承認が必要であり、「条約」とする場合にはかなり厳格な議会手続が必要となるため「行政協定」としているものである。したがって、我が国にとっては条約に相当する内容であり、国会の承認が必要となろう。

関する実体法及び手続法を有していること、すなわち当該条約の第 1 章及び第 2 章に定める定義及び要件に適合する国内法を有すること。

- (ii) 法の支配 (rule of law) と公平の原則 (principles of nondiscrimination) に従っていること。
- (iii) 次に掲げるような国際的に認められている人権を保障する義務を保持しないし確約し (commitment) 又は尊重していること
  - (I) プライバシーに対する専断や不法侵害からの保護
  - (II) 公正な裁判を受ける権利
  - (III) 表現、結社、平穏な集会の自由
  - (IV) 専断的な逮捕・拘束の禁止
  - (V) 拷問及び残虐で非人道的又は個人の尊厳を損なう処遇又は刑罰の禁止
- (iv) データを収集、保管、利用及び共有する権限を与える手続やこれらの活動の監視など、本行政協定に基づいてデータを請求する権限を有することとなる外国政府機関を監督する法的権限と手続が明定されていること。
- (v) 当該外国政府による電子データの収集と利用に関して、説明責任と適切な透明性を提供する十分な仕組みを有していること。
- (vi) 国際的な自由な情報の流通と、インターネットの開かれた、どこでも利用可能で (distributed)、相互接続可能なインターネットの特徴を推進し、及び保護することを確保していること。

これらの事項は、米国のプロバイダが電子証拠を提供しても、相手国がそれを濫用せず、プライバシーの保護が徹底されることを担保するものと考えられる。日本は、近代憲法に基づき基本的人権を尊重しているから、これらの事項の大半はすでに満たしていると考えられ<sup>6)</sup>、立法による担保措置が必要となる

---

<sup>6)</sup> 日本における人権保障が米国の政府関係者や研究者に理解されているかどうかは別問題である。米国以外の国民の立場からは、米国政府において人権保障が徹底されているかどうか不安を感じざるを得ないが、他方、米国内の議論においては、相手国の人権保障に不安を抱き、行政協定の締結によって米国民の権利が侵害されることへの懸念が表明されている。したがって、クラウド法に基づく日米協定締結に向けては、政府間の交渉以前に、日本における捜査手続上の人権保障が米国内において十分理解されるよう情報発信を行っておく必要があるように思われる。

可能性があるのは (iv) 号及び (v) 号が中心となるであろう。日本の個人情報保護法は、個人情報の収集、保管、利用及び共有について個人情報保護委員会による一定の監督がなされているが、同法は捜査情報については適用がない規定が少なくなく、刑事訴訟法において証拠の収集につき厳格な規律を定めているが、保管、利用及び共有については特段の規律がなく、国家公務員法及び地方公務員法による秘密保持の規律や捜査機関の内規によって管理されるにとどまる。したがって、米英協定及び米豪協定の締結過程において、英国及びオーストラリアについて、どのような基準で上記 (iv) 号及び (v) 号を満たしているとされたのかが、本稿の関心事項となる。

### 3 行政協定の内容に求められる要件（協定要件）

米国連邦法 18 編 119 章 2523 条 (b) 項は、行政協定の内容として次の事項が含まれることを求めている（同項 (4)）。これらの事項は行政協定の内容となるものであるから、少なくとも行政協定の発効時までに国内担保法が施行されている必要があるであろう。

(A) 当該外国政府が、合衆国人又は合衆国居住者を意図的に対象としないこと、及び本項の要件を満たすように対象を定める手続を定めること。

(B) 当該外国政府が、合衆国人又は合衆国居住者に係る情報の取得を目的とする場合には、合衆国人以外の者又は合衆国外に居住する者であっても意図的に対象としないこと。

(C) 当該外国政府は、米国政府や第三国政府の要請に応じて、又はこれに提供する情報を獲得するために命令を発しないこと、又は米国政府や第三国政府と協力して作成された情報を共有する要請に応じないこと。

(D) 当該外国が発する命令は次の要件を満たすこと。

(i) テロを含む重大犯罪の予防、発見調査活動、捜査又は訴追に係る情報の取得を目的としたものであること。

(ii) 命令の対象として、人物、アカウント、アドレス、機器又は請求の対象を特定するその他の事項を特定していること。

(iii) 当該外国の国内法に適合しており、電気通信サービス又はリモート・コンピューティング・サービスのプロバイダがデータを生成する義務が

当該国内法のみに基づくこと。

(iv) 明確で信頼できる事実、特定性、合法性、捜査対象の行為の重大性に基づく相当な理由を基礎付ける諸要件を満たしていること。

(v) 命令の発付に先立ち、発付手続中に、又はその執行の過程で、裁判所、裁判官 (judge)、マジストレイト (magistrate) その他の独立した主体による審査 (review) ないし監督 (oversight) を受けるものであること。

(vi) 命令が有線又は電気通信の傍受その他の拡大的手段 (extensions) である場合には、

(I) 確定的で限定された期間であること。

(II) 当該令状により許可された目的を達成するのに通常必要な期間を超えないこと。

(III) より侵害的でない方法により同じ情報を合理的に取得できない場合に限り発出されるものであること。

(E) 当該外国政府によって発せされる命令が、表現の自由を侵害するものではないこと。

(F) 当該外国政府は協定に基づき取得された情報を速やかに審査 (review) するとともに、審査していない通信は適切な手続により訓練された者のみがアクセスできる安全なシステムに保管すること。

(G) 当該外国政府は、可能な限り、海外諜報活動監視法 (50 U.S.C.1801) 第 101 条が定める最小化手続 (minimization procedures) の定義に従い、テロを含む重大犯罪の予防、発見調査活動、捜査又は訴追に関連する情報、あるいは人の身体に重要な侵害を与える危険を防止するために又は人の生命の危険若しくは重傷を回避するために必要であり又は重要と評価される情報でないことが判明したものについて、分類、封印、削除、不拡散のための最大限の措置をとること。

(H) サブパラグラフ (G) に従い、かつ、テロ、重大粗暴犯罪、児童虐待、国際組織犯罪、重大金融犯罪等の国家安全保障に係る犯罪など合衆国又は合衆国人への重大な侵害又は脅威となる通信を提供する場合を除き、当該外国政府は、合衆国人の通信の内容を合衆国政府当局に引き渡さないこと。

(I) 当該外国政府は、本来当該外国の法律が通信プロバイダのデータ開示を制限している場合には、可能な場合には (where applicable)、合衆国の司法管轄に属する事業者を含む通信プロバイダに対する規制を撤廃し、第 2711 条に規定す



る米国政府機関による合法的な法的手続に応じることができるようにするなど、データアクセスに関する相互主義的な権利を与えること。

(J) 当該外国政府は、同政府が当該協定の条項を遵守しているかを合衆国政府によってなされる定期的な審査を受けることに同意すること。

(K) 合衆国政府は、当該行政協定が適切に実施されることができないと認められる場合には、いかなる命令も執行されないよう当該行政協定を停止する権限を保留すること。

これらの事項のうち、通信傍受に係る (D) (vi) については、日本では通信傍受の対象犯罪にサイバー犯罪が含まれておらず、また、対象犯罪についても適用要件がかなり厳格なので、最初に行政協定を締結する段階においては、対象となる捜査手段に通信傍受は含めないかもしれない<sup>7)</sup>。また、日本にはインテリジェンス法制もないから、これを対象とするものと考えられる (G) 及び (H) についても、日米協定については適用対象外となろう。

立法上の担保が必要になると考えられるのは (I) であり、相互主義に基づき、米国の捜査機関が日本のプロバイダに対して令状を執行した場合に、日本のプロバイダが日本国内から米国に個人情報に移転することが認められるよう、個人情報保護法の改正又は特別法の制定が必要になろう。

また、令状の執行方法がどのようになるかにより、国家主権の問題や憲法問題が生ずる可能性がある。電子証拠を必要とする国がその国内で外国のプロバイダに対して令状執行するのであれば、それぞれの国にとっては国内における捜査権限の行使であるから、個人情報保護法制における個人情報の越境移転の問題が解消されれば問題はない（もっとも、実質的に次の第二の問題に該当するという批判はあり得る。）。日本では、電気通信事業法が日本で営業する通信事業者に対して国内で代表者を定めて法人登録することを義務付けている（同法 9 条、10 条 1 項 2 号、12 条 1 項 4 号）ので、国内で米国法人の日本での代表に対して命令を執行する手段は確保されているといえる。

これに対し、電子証拠を必要とする国の令状を相手国に所在するプロバイダ

---

<sup>7)</sup> もっとも、サイバー犯罪捜査にとっては重要な捜査手法であるから、通信傍受をこの枠組みの対象とするよう米国から求められる可能性はある。

に対して直接執行することについては、米国では従前から米国内で営業を行うなど一定の活動をしている外国企業に対しては米国の国内法が及ぶと考えており、本拠地が国外にあるかどうかは問題としない。米国としては、行政協定を締結していなくても現にこの立場で国内法を執行しているので、新たに外国の主権を侵害するものではないという立場である<sup>8)</sup>。これに対し、日本をはじめ大陸法系の国においては、国内法を適用するには令状執行の場所が国内である必要があり、執行場所が国外であれば越境捜査となると考える。そうすると、第一に信頼のできる外国とはいえ限定的ではあるが外国の捜査機関に捜査権の行使を認めることとなり、第二に相手国にとっては自国の裁判所の審査を経ずにプライバシーが侵害されるともいえる。もっとも、第一の点については、刑事訴訟法に基づく捜査権は海外にも及び得るとする外国主権制限説<sup>9)</sup>によれば、相互主義に基づき当事国が双方に自国内での相手国の捜査権の行使を認める限り国家主権は問題とならない。第二の点については、直接に令状の執行を受けるプロバイダは実質的にはプライバシーを侵害される者とは言えず、かつ、実質的にプライバシーの侵害を受ける電子証拠の権原者（主として被疑者がこれに当たると考えられる。）については、クラウド法は、プロバイダの所在国の国民及び居住者は対象外としている。ある国の憲法が人権を保障する対象は、基本的には自国民及び居住外国人であるはずであり、自国民でも居住者でもない者の人権をどこまで保障するかは立法に委ねられているとも考えられるが、大いに議論になり得る論点ではあろう。

英米法と大陸法のように法体系に一定の相違のある国の間で取極めを行う場合には、相互に相手国の法体系を尊重する必要がある。英国は米国と同じく英米法の国ではあるが、後述するように令状の執行場所については、おそらくはEUの影響を受け、米英協定締結のために制定した新法において英国国内で執行する旨の規定を設けているが、米国に対して同様の国内立法を求めているようである。このことは、日米協定締結においても参考となるであろう。

---

<sup>8)</sup> 前掲注4) 参照。

<sup>9)</sup> 山内由光「国外における捜査活動」(松尾浩也・岩瀬徹編『実例刑事訴訟法 I』10頁) 参照。

### Ⅲ 米英協定

#### 1 米国における英国に対する相手国要件の検討

米英協定の締結に当たって、英国が相手国要件を満たしているかどうかの検討については、当時のバー米国司法長官の宣誓書の付属文書「協定がアメリカ合衆国法典第 18 編第 2523 条 (b) の要件を満たすと決定する際の各検討事項の説明」（以下「英国説明文書」という。）に詳述されている<sup>10)</sup>。

上記の注目すべき同項 (1) (B) (iv) 及び (v) については、英国説明文書は、3 つの法律すなわち (1) 2016 年捜査権限法、(2) 2019 年犯罪（海外提供命令）法、(3) 2018 年データ・プライバシー法について説明を行っているので、これらの法律について英国説明文書がどのような点に注目しているのかを概観する。

##### (1) 2016 年捜査権限法（Investigatory Powers Act 2016）

2016 年捜査権限法は、主としてテロ対策のため、司法長官に情報通信に関して通信傍受の発付等の強い捜査権限を付与する代わりに、「司法委員」が令状の事後承認をすることとした法律である。本法第 8 部は、捜査機関による通信傍受等の強力な捜査権限を監督するため、捜査機関から独立した捜査権限監督官（Investigatory Powers Commissioner : IPC）等による審査体制を新たに設置している。

また、本法第 2 部 15 条は、米英協定の担保として、条約、協定等に基づいて海外の捜査機関に通信傍受を認める「相互共助令状」について規定している。同法の構成は、次の通りである。

第 1 部 一般的なプライバシー保護

第 2 部 合法的な通信傍受

第 3 部 通信データ取得権限

第 4 部 通信データの保持

---

<sup>10)</sup> “Explanation of Each Consideration in Determining that the Agreement Satisfies the Requirements of 18 U.S.C. § 2523 (b)” <[https://www.justice.gov/d9/pages/attachments/2020/01/02/2019-12-9\\_cloud\\_act\\_-\\_graham\\_et\\_al.pdf](https://www.justice.gov/d9/pages/attachments/2020/01/02/2019-12-9_cloud_act_-_graham_et_al.pdf)> pp25-45

第5部 機器に対する傍受 (Equipment Interference)

第6部 包括令状

第7部 個人データセット包括令状

第8部 監督体制

第9部 雑則及び総則

英国説明文書が評価している点は、次のとおりである。

①本法に基づき、通信傍受令状を請求したり、通信データ取得権限を得たりすることができる法執行機関や情報機関を含む公的機関を特定していること。

(18条、70条、73条)

②司法長官が通信傍受令状を発する場合に満たさなければならない必要性和比例性の法的基準を定め、英国の新しい「デュアルロック」メカニズムの下で、令状が発効する前に、あるいは緊急事態の場合は令状発行から3営業日以内に、司法委員による令状の審査と承認を受けなければならないこと。(6条、19条、23条)

③本法の令状によって収集されたデータへのアクセスを許可された機関を特定し、不正な開示からデータを保護する義務を課していること。(53-59条)

④本法の令状によって収集された保管データの関連性を定期的に審査することを義務付けており、データを保管する関連性がなくなった場合には、データを破棄することを当局に義務付けていること。(53条)

⑤本法は、捜査権限監督官とそのスタッフである司法委員、捜査権限監督官事務局 (IPCO) の検査官、弁護士、通信専門家からなるスタッフによる審査と監督を受ける。捜査権限監督官の任務は、IPAに基づく令状の行使を監査、検査、調査することである (229条)。捜査権限監督官と司法委員は、4人の高官 (うち3人は政府から独立した司法官) の共同推薦により、首相によって3年の任期で任命され、再任が可能である。また、監督官は、刑事上の有罪判決や破産命令など、特定の法的措置の対象となった場合は、国会の各議院の決議又は首相によってのみ、解任することができる (227条(1)-(4)、228条(2)、(3))。

上記①は、我が国の通信傍受法でも規定されていることであって、特に問題はない。②は、通信傍受令状を英国の司法長官が発付できるという強い権限を

事後審査するための規定に関する事項なので、日米協定では想定されないであろう。

③-⑤は収集したデータの保管や廃棄、独立の監督機関に関する規定であって、日本では実務上行っているものの法律にはない事項であるから、日米協定締結時に類似の国内法を整備すべきかどうかの問題となる可能性がある。

## (2) 2019年犯罪（海外提供命令）法（Crime (Overseas Production Orders) Act 2019)

2019年犯罪（海外提供命令）法は、保管通信について英国がEU諸国や米国に向けた越境証拠収集を行うために制定した法律である。

同法は、海外提供命令の執行方法について、本法14条2項は、裁判所が許可した電子的な方法によることを認めている。また、同条3項は、英国内で発付された令状の海外所在の者に対する執行は、英国内の主体たる事務所若しくは従業者の営業地、従業者の住所地など英国内で行う旨規定している<sup>11)</sup>。

同法は、次のような構成となっている。

- 第1条 申請による海外提供命令の発出
- 第2条 適格捜査官
- 第3条 電子データ及び例外電子データの意義
- 第4条 海外提供命令発出の要件
- 第5条 海外提供命令の内容
- 第6条 海外提供命令の効力
- 第7条 海外提供命令の修正又は撤回
- 第8条 海外提供命令における秘密保持義務
- 第9条 海外提供命令の執行の制限
- 第10条 電子データの保存と証拠としての利用
- 第11条 手続事項
- 第12条 報道に関するデータの適用通知
- 第13条 適用通知の効果

---

<sup>11)</sup> これに対し、本協定は両締約国が令状の域外執行を相互に認めたものだとする研究もある。Tim Cochrane, 2022, Hiding in the Eye of the Storm Cloud: How CLOUD Act Agreements Expand U.S. Extraterritorial Investigatory Powers, *Duke Journal of Comparative & International Law*. Vol 32, pp153-210

第14条 海外提供命令の執行方法

第15条 軍警察への適用

第16条 2016年捜査権限法第52条に規定する国際協定の指定

第17条 行政規則

第18条 一部文言の解釈

第19条 本法の適用範囲

第20条 施行日

第21条 本法の略称

英国説明文書が評価している点は、次のとおりである。

a. 英国国内での命令の条件と保護基準が満たされた場合に限り、特定の英国機関が裁判官に海外提供命令を求めることを認めている。(4条)

b. すべての海外提供命令は、起訴可能な犯罪が行われ、その犯罪に関して訴訟が開始された、又は捜査中である（又はテロ捜査の目的で命令が求められている）と信じるに足る合理的な根拠があること、求められているデータが訴訟又は捜査にとって実質的な価値がある可能性が高く、要求されたデータの全部又は一部が提供又はアクセスされることが公共の利益になること、申請が例外データ（例えば、法的特権を有する資料や医療記録などの機密の個人記録）を要求していないことを条件とする。(1条、4条)

c. 国内命令を通じて収集されたデータと同様、海外提供命令を通じて取得されたデータも、データ・プライバシー法に従って保管及び共有されなければならない、あらゆる状況において必要な限り、そのデータを保管することができる。(10条(1))

d. 裁判官は、権限のある政府機関の請求により、本法に基づく提供命令を許可し、命令の影響を受ける者又は特定の政府当局の申請により、命令を変更し又は取り消す権限を保有する。さらに、捜査権限法に基づく令状と同じ監査機関である捜査権限監督官事務局が、協定に従って海外提供命令の使用を監督する。(7条)

a及びbについては、日米協定締結前に制定すべき国内担保法においても同様

の規定が設けられるものと予想される。c及びdについては、日本の現行法にはない規定であるので、日米協定締結時に国内法を整備すべきかどうかが問題となる可能性がある。

### (3) 2018年データ保護法（Data Protection Act 2018）

英国の個人情報保護においては、基本的に EU 一般データ保護規則（GDPR）が適用され、本法がその例外を定めるような構造となっている。捜査に関しては、本法は、EU 法執行指令が適用されることも定めている。本法は、本法の施行について監督を行うため情報保護長官を設置し、第 5 部においてその広範な権限を定めている。

本法は、次のような構成となっている。

#### 第 1 部 予備

第 1 条. 概要 第 2 条. 個人情報の保護 第 3 条. 個人データの処理に関する用語

#### 第 2 部 一般的な処理

第 1 章 範囲と定義 第 2 章 GDPR 第 3 章 その他の一般的な処理

#### 第 3 部 法執行機関による処理

第 1 章 範囲と定義 第 2 章 データ保護原則 第 3 章 データ主体の権利

第 4 章 管理者と処理者 第 5 章 個人データの第三国等への移転

第 6 章 補足

#### 第 4 部 諜報機関の処理

#### 第 5 部 情報保護長官

#### 第 6 部 施行

#### 第 7 部 補足規定及び最終規定

英国説明文書は、次の事項について評価している。

i. 個人データが法執行目的のために処理される場合、その目的は特定され、明示され、かつ合法的でなければならず、処理されるデータは目的との関連において適切で、関連性があり、かつ過度であってはならず、データは処理される目的に必要な期間を超えて保管されることはなく、保管継続の必要性を定期

的に見直すための適切な期限が設定されなければならない。(36条、37条、39条)

ii. 適切な技術的及び組織的手段を用いて、個人データはリスクに応じたセキュリティレベルを確保する方法で処理されなければならない。データ管理及び処理をする機関は、データの変更又は開示を含む処理操作のログを保管しなければならない。また、データの最小化措置を含むデータ保護を「設計上」及び「デフォルトで」実施しなければならない。(40条、57条、62条、66条)

iii. EU域外へのデータ転送に制限を課しており、例えば、第三国へのデータ転送が法執行目的で必要であり、かつその転送先が関連する法執行機関である場合にデータ転送を許可している。(73条、76条)

iv. 人種、政治的意見、宗教的信念、又は健康、遺伝的データ、生体認証データを含むデータの処理に対する保護措置として、「センシティブな処理」に対する特定の方針を要求している。当該方針は、データ保護原則を遵守し、そのようなデータの保管と消去をする手順を説明しなければならない。ガバナンスと説明責任の対策と結びつけて、方針を必要に応じて見直し、更新し、要請に応じて情報保護長官に提供しなければならない。(42条)

v. データ主体はまた、情報、アクセス、誤ったデータの修正、処理の消去又は制限など、管理者及び処理者が満たさなければならない一定の権利を有する。データ管理者は、その身元及び連絡先、データを保有する目的、データ保護責任者の連絡先、データ主体の権利の存在など、一定の情報を一般に公開するか、その他の手段により、データ主体が利用できるようにしなければならない。特定の場合には、データ処理の法的根拠、データの保管期間、及びデータの受領者の種類に関する情報など、追加の通知が必要である。(44-47条)

vi. データ管理機関は、例えば、公的な合法的捜査を害することを回避し、公共安全を保護するためなど、公共安全の保護に関わる特定の状況において、データ主体の権利を制限することができる。このような制限を適切に行い、公的な調査の妨害を回避し、犯罪の予防、発見調査活動、捜査又は訴追を害することを回避し、公共安全又は国家安全保障を保護し、他者の権利及び自由を保護するために、制限が「必要かつ相当の」措置である限りにおいてのみ、制限することができる。このような状況において、データ管理機関は、データ主体に通知することが制限の目的を損なう場合（例えば、公共安全を保護す



る場合など）を除き、データ主体の制限に関する苦情を申し立てる権利を含め、データ主体に制限について通知する必要がある。データ管理機関は、制限の理由を記録し、要求があれば、その記録を情報保護長官に提供しなければならない。（45条）

vii. データ管理・処理機関は、司法当局を除くデータ管理機関が、特定の責任を負い、その職務の遂行によって解雇又は処罰されないデータ保護責任者を指名することを義務付けること、処理活動に関する文書を保持する要件、処理の種類が「個人の権利と自由に対して高いリスクをもたらす可能性がある」場合にはデータ保護影響評価を実施することなど、「包括的かつ相当な」説明責任とガバナンスの措置を導入しなければならない。（64条、67条、69-71条）

viii. 監督に関しては、情報保護長官は、本法の監視及び執行、議会及び英国政府の他の部門への助言、苦情の処理、調査の実施、データ漏洩の通知の受領及び調査、個人データ及び処理業務の検査、データ転送の一定の仕組みの審査及び承認を行う監督権限を有する。情報保護長官はまた、本法第3部の法執行規定とEU法執行指令の適用を監視する責任を負う英国当局でもある。（115-116条）

以上のうち、iiiは日米協定締結前に国内担保法を整備すべき事項であると言える。iii以外の事項は、日本では実務上実施していることで法律には規定がないことから、日米協定締結時に整備すべきかどうかの問題になり得る。

## 2 米英協定の内容

米英協定は、次のような条文構成となっている。

- 第1条 定義
- 第2条 協定の目的
- 第3条 国内法及び協定の効力
- 第4条 対象の制限
- 第5条 命令の発出及び送信
- 第6条 対象プロバイダによる情報の提供
- 第7条 対象制限及び最小化手続

- 第 8 条 利用及び転送の制限
- 第 9 条 プライバシー及びデータの保護措置
- 第 10 条 保存手続及び加入者情報
- 第 11 条 両立性及び非排除性
- 第 12 条 実施の審査及び協議
- 第 13 条 費用
- 第 14 条 改正
- 第 15 条 時間的適用関係
- 第 16 条 発効
- 第 17 条 協定の満了及び終了

米英協定にあって米豪協定にはない条文は、9 条「プライバシー及びデータの保護措置」である。同条 1 項は、「『犯罪の予防、発見調査活動、捜査および及び訴追に関連す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、本協定の命令の執行において提供されるすべての個人情報に対して両締約国が準用し、同等の保護を提供する。」と規定している。

6 条 1 項において、相互主義に基づき、相手国の命令に従ってプロバイダからデータ提供がされるようにする締約国の義務を定めている。また、5 条 5 項において、発出締約国は、本協定の命令を対象プロバイダに直接発することができる旨定めている。英国から米国所在プロバイダに対して発する命令を担保する国内法は上記 2016 年捜査権限法及び 2019 年犯罪（海外提供命令）法であり、米国から英国所在プロバイダが命令の提示を受け米国にデータを提供することを認める根拠規定が上記 2018 年データ保護法第 3 部第 5 章「第三国等への個人情報の移転」である。これらの規定からすると、上述のように各国が自国の令状を国内で執行することを想定していると考えられるが、執行場所については英国の 2019 年犯罪（海外提供命令）法は英国国内であることを定めているのに対し、米国国内法には特段の規定はないから、両国が従前から行ってきた令状の執行方法を認めたものと考えられる。

## IV 米豪協定

### 1 米国におけるオーストラリアに対する相手国要件の検討

米豪協定の締結に当たって、オーストラリアが相手国要件を満たしているかの検討については、当時のガーランド米国司法長官の宣誓書の付属文書「協定がアメリカ合衆国法典第 18 編第 2523 条 (b) の要件を満たすと決定する際の各検討事項の説明」（以下「豪州説明文書」という。）に詳述されている<sup>12)</sup>。

上記の通り注目すべき同項 (1) (B) (iv) 及び (iv) については、豪州説明文書は、3 つの法律すなわち (1) 2021 年電気通信法改正法（国際提供命令）（通称 IPO 法）、(2) 1988 年プライバシー法、及び (3) 1986 年情報保安総括監察官法について説明を行っている。日本にはインテリジェンス法制はないので、ここでは (1) 及び (2) の法律について、豪州説明文書がどのような点に注目しているのかを概観する。

(1) 2021 年電気通信法改正法（国際提供命令）（IPO 法）（Telecommunications Legislation Amendment (International Production Orders) Act 2021 (IPO Act)）

2021 年電気通信法改正法（国際提供命令）（IPO 法）とは、オーストラリア政府が米豪協定締結を担保するために 1979 年電気通信法（通信傍受及びアクセス）に国際提供命令に関する附属章典（Schedule 1）を加えるなどした法律である。国際提供命令は、通信傍受、保管通信及びメタデータについて、オーストラリアの捜査機関が外国のプロバイダに対してデータの提供を命ずる令状である。

同法第 5 章は、国際提供命令が発出されると指定当局に回付され、その審査を受けた後に指定当局から対象プロバイダに送達（give）される旨規定しており、この規定からは同命令の執行が米国所在のプロバイダに直接執行されているように見える。

改正後の附属章典（IPO 法）は、次のような構成となっている。

## 第 1 章 総則

---

<sup>12)</sup> “Explanation of Each Consideration in Determining that the Agreement Satisfies the Requirements of 18 U.S.C. § 2523 (b)” (<https://www.justice.gov/d9/pages/attachments/2022/01/25/materials-us-congress-australia-cloud-act-agreement.pdf>) p33-52

- 第2章 刑法の法執行のための国際提供命令
- 第3章 管理命令のための国際提供命令
- 第4章 国家安全保障のための国際提供命令
- 第5章 国際提供命令の提示
- 第6章 国際提供命令の撤回
- 第7章 国際提供命令に対する異議申立て及び破棄
- 第8章 国際提供命令の遵守
- 第9章 必要要件の報告及び記録
- 第10章 連邦オンブズマンによる監視
- 第11章 国際提供命令により得られた保護情報の開示
- 第12章 プロバイダによる証拠証明書
- 第13章 外国からの命令及び要請
- 第14章 雑則

これらの規定のうち、豪州説明文書が合衆国法典第18編第2523条(b)(1)(B)(iv)及び(v)に関して注目しているのは、次の諸点である。

①法執行機関や情報機関を含め国際提供命令を申請できる公的機関を特定していること。

②国際提供命令を申請するために満たさなければならない法的基準を定めていること。

③発出当局は適格な司法官又は行政控訴裁判所の指名された構成員であり、命令の発出前に発出当局が考慮しなければならない要素が定められていること。

④国際提供命令が米豪協定を遵守しているかを審査するオーストラリアの指定当局を設置していること。

⑤重大犯罪の捜査、情報機能の遂行、監督目的など、法令により列挙された一定の例外が適用されない限り、収集したデータの利用や開示を禁止していること。

⑥許可された目的のためにデータを必要とする可能性がない場合には、データを破棄することも義務付けられていること。

⑦IPO法の遵守は、連邦オンブズマンによる審査と監督の対象となること。

⑧連邦オンブズマンは、秘密、侵入、強制的な法執行権の行使を監督する重要な既存の役割を担っており、調査と報告を通じて、法執行機関とIPO法の枠組みの下にあるオーストラリアの指定当局の活動を監督することとなっており、連邦オンブズマンの年次調査報告書は、各議会で公開されること。

これらの事項のうち、①-④は日米協定締結時までには新規立法などにより担保されることとなろう。これに対し⑤-⑧は現行法にはない枠組みなので、どのように対応すべきか議論の対象となろう。

## (2) 1988年プライバシー法（Privacy Act 1988）

1988年プライバシー法は、インテリジェンス情報以外の政府機関が保有する情報（捜査情報を含む）を適用対象としている。同法の構成は、次のとおりである。

### 第1章 総則

### 第2章 解釈

### 第3章 情報プライバシー

#### 第1節 プライバシー侵害

#### 第2節 オーストラリアのプライバシー原則

#### 第4節 税ファイル番号情報

### 第3A章 信用性報告

### 第3B章 プライバシーコード

### 第3C章 適格なデータ侵害の通知

### 第4章 情報長官の機能

### 第5章 調査等

### 第6章 公益の決定と一時的な公益の決定

### 第6A章 緊急時・災害時における個人情報の取扱い

### 第6B章 法執行

### 第7章 プライバシー諮問委員会

### 第8章 秘密保持義務

## 第9章 雑則

### 附属章典 オーストラリアのプライバシー原則

#### 第1章 個人情報のプライバシーへの配慮

#### 第2章 個人情報の収集

#### 第3章 個人情報の取り扱い

#### 第4章 個人情報の完全性

#### 第5章 個人情報へのアクセスと訂正

これらの規定のうち、豪州説明文書が合衆国法典第18編第2523条(b)(1)(B)(iv)及び(v)に関して注目しているのは、次の諸点である。

a. 政府機関が個人情報を収集する際には、個人が第三者からの収集に同意している場合、第三者からの収集がオーストラリアの法律若しくは裁判所若しくは法廷の命令によって許可されている場合を除き、同法の対象となるすべての機関が個人情報を収集する際には、個人から収集することが不合理又は実行不可能である場合を除き、その個人情報に関連する個人から直接収集されなければならないと規定していること。

b. 政府機関が収集できる個人情報は、政府機関の機能若しくは活動に合理的に必要な、又は直接関連しているものに限られること。

c. 特定の例外を除き、機微情報（例えば、個人の人種や民族的出身、政治的意見、宗教的信念、健康状態に関する情報）は、個人の同意があり、その機関の機能又は活動に合理的に必要な場合にのみ収集することができ、この情報は、その目的が収集の主要な目的に直接関連し、個人の合理的な期待の範囲内でない限り、二次的な目的のために利用又は開示することはできないこと。

d. 政府機関は、個人情報が収集されたことを、収集時若しくは収集前に、又は収集後可能な限り速やかに個人に通知するために、状況に応じて合理的な措置を講じなければならないこと。

e. 特定の目的のために収集された個人情報は、法執行機関の執行関連活動に合理的に必要な場合を含め、法律に規定されている場合を除き、他の目的のために利用又は開示することはできないこと。

f. 政府機関によって収集、利用又は開示される個人情報が、正確かつ最新か

つ完全であり、利用又は開示に関連するものであることを保証するために、状況に応じて合理的な措置を講じなければならないこと。

g. 政府機関が保有する個人情報、状況に応じて合理的な措置を講じることにより、誤用、妨害、紛失、不正アクセス、改ざん、又は開示から保護されなければならないこと。

h. 政府機関は、いかなる目的にももはや必要でなくなった個人情報、又は裁判所や法廷の命令により、あるいは連邦の記録目的のために、オーストラリアの法律に基づいて保有する必要がなくなった個人情報を破棄又は非識別化するために、状況に応じて合理的な措置を講じなければならないこと。

i. 個人は、オーストラリアの法律がアクセスを拒否する権限を政府機関に与えない限り、政府機関が保有する自己の個人情報にアクセスすることができること。

j. 個人は、政府機関が保有する自己の個人情報の訂正を要求することができ、政府機関が記録の訂正を拒否する場合は、不合理な場合を除き、その理由を書面で本人に通知しなければならないこと。

k. 法執行機関による遵守を含め、プライバシー法の遵守は情報長官によって監督されること。

l. プロバイダ等がオーストラリアプライバシー原則を遵守するための慣行、手順、及びシステムを実施し、関連する問い合わせや苦情に対応できるようにするために、状況に応じて合理的な措置をとることを確保することを含め、オープンで透明性のある方法で個人情報を管理するための要件を定めていること。

これらの事項は、日本の個人情報保護法においても規定されていることではあるが、日本では捜査情報は同法の対象外とされ、刑事訴訟法と捜査機関の内規に服するだけであるから、日米協定締結時には、捜査情報に関して新たな体系を構築すべきかどうか論点の一つとなろう。

その際留意すべきは、オーストラリアのプライバシー法においてもインテリジェンス情報は対象外とされているところ、日本ではインテリジェンス活動に相当するテロ対策及びスパイ対策が刑事訴訟法に基づいて行われていることである。すなわち、日本ではインテリジェンス情報の一部は捜査情報に含まれて

いるので、捜査情報全体をプライバシー法制の下に置くとインテリジェンス情報が十分に保護されないこととなる可能性があるということである。米国は、プライバシーの保護とともに捜査や国家安全保障上の必要性も重視する国ではあるので、日米協定締結に当たって両者の均衡をどのように図るべきかは、重要な検討事項となろう。

## 2 米豪協定の内容

米豪協定は、米英協定とほぼ同じ、次のような条文構成となっている。

- 第1条 定義
- 第2条 協定の目的
- 第3条 国内法及び協定の効力
- 第4条 対象の制限
- 第5条 命令の発出及び送信
- 第6条 対象プロバイダによる情報の提供
- 第7条 対象制限及び最小化手続
- 第8条 保存手続及び加入者情報入手手続
- 第9条 利用及び転送の制限
- 第10条 両立性及び非排除性
- 第11条 実施の審査及び協議
- 第12条 費用
- 第13条 改正
- 第14条 時間的適用関係
- 第15条 発効
- 第16条 協定の満了及び終了

上述した関心事項に関する規定は6条及び5条であり、米英協定とほぼ同じ規定ぶりとなっている。

相互主義に基づき、相手国の命令に従ってプロバイダからデータ提供がされるようにする締約国の義務を定めているのは、6条1項である。同項は、「両締約国は、本協定の命令に応じて対象プロバイダが提供する対象データは、発出



締約国の指定当局に直接提供されるべきであることに同意する。」と規定する。この規定を担保するため、オーストラリアは、上記の IPO 法を定め、行政協定を締結した外国（米国に限らず一般的な規定となっている。）のプロバイダに対して電子証拠の提供を求める手続（命令を受けたプロバイダからの異議申立ての手続（7章 121 条（1）を含む。）、及び当該外国から命令の提示を受けた場合の手続の詳細を定めている。IPO 法には、オーストラリアの個人情報保護法 Privacy Act 1988 の特則も定め、同法に基づく外国からの提出要求に応じた個人情報の提供は、同法によって認められるものとみなす旨規定されている（13章 169 条）。

日米協定を締結する場合であるが、クラウド法に基づく米国の命令は直接にプロバイダに対して発出されるもので、日本に対する捜査共助要請ではないから、必ずしも国際捜査共助法の改正を要するものではないと考えられるが、個人情報保護法の改正ないし特別法の制定は必要となろう。

プロバイダへの命令の発出方法を定めるのは、米豪協定 5 条 5 項である。同項は、「発出締約国は、本協定の命令を対象プロバイダに直接発することができる。本協定の対象になる命令は、発出締約国の指定当局により送信されなければならない。両締約国の指定当局は、5.5 条から 5.9 条、6.1 条、6.2 条に基づき各々が実施する機能の全部又は一部を、両締約国の政府のその他の当局が実施することを相互に決定することができる。両締約国の指定当局は、相互の決定により、当該主体に関する規則及び条件を定めることができる。」と定めている。この条文からは、米国所在の対象プロバイダに対して直接に令状執行するように見える。

クラウド法には明記されていないが、米豪協定 5 条 11 項は、命令を受けたプロバイダが、同命令が同協定に反していると考える場合に、異議申立てをする権利を認めている。これを受けて、上記附属章典 7 章 121 条（1）が定められている。日米協定にも同様の条項を定める場合には、個人情報保護法等に所要の規定を置く必要が生じる可能性がある。また、米豪協定 7 条は対象制限及び最小化手続を定めている。

## V 日米協定への示唆

以上紹介した米英協定及び米豪協定の締結に際して論じられてきた論点は、将来日米協定を締結する際にも、大いに参考になるものと言える。

第一に、日本の捜査法及び個人情報保護法に対する信頼を得ておく必要があるということである。クラウド法自体が米国国内においてプライバシー侵害を招来する可能性がある法律として認識されているので、米国にとって法体系が同一のいわゆる米英法系の国である英国とオーストラリアとの間の行政協定であっても米国内で様々な懸念が表明されてきた。日本の捜査法及び個人情報保護法は、大陸法から一定の影響を受けており米国と法体系がやや異なる上に、一般に日本に関する海外に向けた情報発信は少ないと見られており、そもそも米国政府や研究者の多くにとって日本は「法体系がよく分からない国」と認識されている可能性がある。日米協定締結作業に着手する場合は、同時に日本法に関する情報発信の作業にも着手する必要があるだろう。

第二に、日米協定が締結された場合に、日本のプロバイダが米国捜査機関から情報の提出を求められる機会はそれほど多くはないと考えられるが、相互主義の立場から、日米協定締結に当たっては、日本のプロバイダが米国捜査機関から令状を提示された場合に対象となる個人情報を含む情報を日本から米国に移転し、さらに米国の捜査機関に提出することを許容する法制度を整備する必要がある。その場合には、現行法制にはないプロバイダからの異議申立ての手続を創設する必要があるだろう。また、実質的には、日本国民・居住者以外の者に関するプライバシーの程度の高い日本国内に所在する情報を、日本の裁判所の審査を経ずに米国の捜査機関に提供することとなるのであるから、日本国民・居住者以外の者であれば法律によりそのような取扱いをすることが憲法上許されるか否かが議論されることとなろう。さらに、令状の執行場所について日米には考え方の相違があり、相互に相手国の法体系を尊重する枠組みを認めることができるかも問題となろう。

第三に、クラウド法の枠組みにおいて「最小化手続」と称される、日本の捜査機関が米国から入手した情報について十分な管理や利用の制限がなされる体制を確立する必要がある。この点について、法整備まで求められるのか、実務上十分な体制が整備されていることを示すことができればいいのかは、現時点

では分からないところであるが、米国側にとって重要な検討事項となる可能性がある<sup>13)</sup>。

クラウド法に基づく行政協定の締結は、サイバー空間における捜査にとってはかなり重要度が高いものであり、早期の締結が望まれるが、以上のように締結に向けて議論を整理し準備しなければならない論点は多岐にわたり、かつ、いずれも大きな論争になる可能性のある論点であると言える。その意味において、一刻も早く国内における議論を開始する必要があるが、そもそも我が国の政府関係者や研究者において、クラウド法の重要性の認識が必ずしも十分に浸透していないように見える。本稿がそのような共通認識の普及の一助となれば幸いである。

---

<sup>13)</sup> 本稿の検討の対象外ではあるが、将来 EU と同様の枠組みを締結する際には、法整備を求められる可能性が高い論点であると言える。

## VI 資料

### 1 重大犯罪対策のための電子データへのアクセスに関するアメリカ合衆国政府と英国政府との間の協定

四方 光監訳、趙 恩慶訳

アメリカ合衆国政府及び英国政府（以下、「両締約国」という。）は、公共の安全を保護し、テロリズムを含む重大犯罪対策という目的のために、両締約国が協力を強化するという相互利益に促され、適法な法執行目的のために電子データに適時にアクセスすることが、この取り組みにおいて不可欠な要素であることを認識し、プライバシー、言論の自由を含む人権、市民的自由、法の適正手続を尊重することの重要性を強調し、個人情報を含む電子データの取り扱いについて、締約国のそれぞれの法律を遵守した保護基準を提供し、そのための適切な保護措置を提供する公的機関間の法的拘束力と強制力を持つ文書を作成することを意図し、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要件の弊害に留意し、そのような要件を回避するよう努め、電子データにアクセスするための両締約国のそれぞれの法的枠組みが、通信の内容にアクセスする際には、必要性和比例性又は正当な理由と命令の拡大解釈の制限、独立した司法監督の要件を含め、プライバシー及び市民的自由を保護するための適切かつ相当な保護措置を組み込んでいることを認識して、次のとおり協定した。

#### 第1条 定義

本協定の適用上、

1. 「アカウント」とは、アカウント、電話番号、アドレス情報など、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私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、ブダペスト・サイバー犯罪条約第1章第1a条に規定されているところによる。すなわち、あらゆる装置や、相互接続されたり関連付けられたりした装置のグループであって、そのうちプロ

グラムに従ってデータの自動処理を行う一つ又は複数のものをいう。

3. 「対象データ」とは、対象プロバイダとしての資格において行動する私法人が保有又は管理する、以下の種類のデータをいう。すなわち、電気通信又は有線通信の内容、ユーザのために保管又は処理されたコンピュータデータ、電気通信若しくは有線通信に関連するトラフィックデータやメタデータ又はユーザのためのコンピュータデータの保管若しくは処理に関連するデータ、及びこの定義で言及されている他の種類のデータも求める命令に従って求められる場合の加入者情報である。
4. 「対象情報」とは、対象者により利用又は管理され、かつ受領締約国により利用又は管理されていないアカウントの対象データをいう。
5. 「対象犯罪」とは、発出締約国の法律の下で、テロ活動を含む重大犯罪を構成する行為をいう。
6. 「対象者」とは、第 7.1 条により要求される手続を適用した上で、第 5 条に従って命令のために本協定が発動された時点において、受領締約国の者でないと合理的に考えられる者をいう。
7. 「対象プロバイダ」とは、以下の範囲内の私法人をいう。
  - (i) コンピュータシステム又は電気通信システムにより、公衆に通信、コンピュータデータの処理又は保管の機能を提供する者
  - (ii) 第 (i) 号に定義される機関のために対象データを処理又は保管する者
8. 「指定当局」とは、英国については内務大臣が、合衆国については司法長官が指定する政府機関をいう。
9. 「発出締約国」とは、関連する（本協定の）法的手続を発する締約国をいう。合衆国が発出締約国である場合、合衆国内の州、地方、地域、部族、その他の機関が発した（本協定の）法的手続が含まれる。英国が発出締約国である場合、英国内の州の機関が発した（本協定の）法的手続が含まれる。
10. 「（本協定の）法的手続」とは、本協定の命令、及び本協定第 10 条で定められる保存手続、加入者情報手続をいう。
11. 「命令」とは、発出締約国の国内法に基づき発せられた対象プロバイダによる対象データの開示又は提供（当該データの認証の要求を含む）を要求する法的文書をいい、当該対象データは保管された通信のものであるか送信中

の通信のものであるかは問わない。

12. 「受領締約国の者」とは、次に掲げる者をいう。

合衆国が受領締約国である場合、

- (i) 州、地域、地方、部族レベルを含む政府機関又はその当局
- (ii) その市民又は国民
- (iii) 適法に許可された永住者
- (iv) 構成員の多数が (ii) ないし (iii) に該当する法人格なき団体
- (v) 合衆国で法人格を得た法人
- (vi) 受領締約国の領域内の居住者

英国が受領締約国である場合、

- (i) 州の政府機関又は当局
- (ii) 構成員の多数が領域内に居住する法人格なき団体
- (iii) その領域内に居住又は登録されている法人
- (iv) その領域内に居住するその他の者

13. 「受領締約国」とは、発出締約国以外の締約国（その地方行政機関を含む）をいう。

14. 「重大犯罪」とは、長期が3年以上の拘禁刑に処せられる犯罪をいう。

15. 「加入者情報」とは、氏名、住所、サービスの契約期間及び種類、加入者番号又は個人番号（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）、電話の接続記録、通話時間及びその長さ、支払手段など、対象プロバイダの加入者又は顧客を特定する情報をいう。

16. 「合衆国人」とは、次に掲げる者をいう。

- (i) 合衆国の市民又は国民
- (ii) 適法に許可された永住者
- (iii) 構成員の多数が (i) ないし (ii) に該当する法人格なき団体
- (iv) 合衆国で法人格を得た法人

## 第2条 協定の目的

1. 本協定の目的は、通信サービスプロバイダが一方の締約国から電子データの提供又は保存を求める（本協定の）法的手続を受けた場合、当該プロバイダが他方の締約国の法律の適用を受ける可能性があるときに、潜在的な法

的義務の衝突を解決することにより、公共の安全とセキュリティを向上させ、プライバシーの権利、市民的自由及び開かれたインターネットを保護することである。本協定は、各締約国が、自国の法律及び他方の締約国の法律に合致する方法で、重大犯罪の予防、発見調査活動、捜査及び訴追に関連する電子データを、適切な対象選択の制限のもとに取得するための効率的、効果的、データ保護を可能とし、かつプライバシーを保護する手段を提供する。

2. 各締約国の法律に基づくその他の法的権限（legal basis）又は重要な利益の適用可能性に影響を与えることなく、本協定は以下を支持する。
  - a. 裁判所の司法活動並びに各締約国の法律に基づく法的義務及び請求
  - b. 両締約国の重要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業務
  - c. 適正かつ適切に追求される正当な利益
3. 本協定に関連する利益には、以下のものが含まれるが、これらに限定されるものではない。
  - a. 当該犯罪の性質又は影響が国境を越えるものであるか否かを問わない、各締約国による重大犯罪の予防、発見調査活動、捜査又は訴追。これらの事項は、法の支配及び正義の実現を追求する両締約国の利益に資するものであり、また、重大犯罪が発出締約国の国境を越えて直接的又は間接的に影響を及ぼし得るという実質的な現実を認識したものである。
  - b. 国際協力における相互主義の精神。そこにおいては、本協定に従って電子データを取得できるという各締約国の利益は、相互主義に基づいて、各締約国が相手国に対しても当該情報を取得するための同じ能力を提供することを必要とするものである。
  - c. 司法管轄の選択による監視から自ら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、阻止するための国際協力の促進。
  - d. 両締約国それぞれの法制度、正当な理由、必要性、比例性、独立した司法による監督等の基準、個人に関するデータの取扱い、処理に関する法律の要件の下で適用可能な範囲内で、個人の市民的自由、

権利を保護するために、拘束力のある、適切かつ実質的な保護措置によって包括的に管理される電子データにアクセスするシステムを確立すること。

### 第3条 国内法及び協定の効力

1. 各締約国は、電子データの保存、認証、開示及び提供に関連する国内法が、対象プロバイダに本協定の命令を遵守することを許容することを保証する。各締約国は、本協定の実施を実質的に妨げる又は害するような国内法の重要な変更について、相手国に通知しなければならない。
2. 本協定の規定は、発出締約国が本協定を発動し関連する対象プロバイダに通知された命令に適用されなければならない。本協定の命令の法的効力は、発出締約国の法律にのみ基づく。それ以外の場合は、対象プロバイダは、本協定の命令に対して適切な法的異議を申し立てる既存の権利を保持する。
3. 各締約国は、本協定を施行するにあたり、他方の締約国の国内法（当該法律の実施を含む）が、本協定の対象となるデータ収集及び活動に関して、プライバシーと市民的自由に対する実体法及び手続法上の強力な保護を与えるものであることを認識する。各締約国は、対象データの保護に重大な影響を及ぼす国内法の重要な変更について相手国に通告するものとし、第5条又は第11条に関して本項に基づき生じる問題について協議しなければならない。
4. 本協定は、両締約国が電子データを取得する能力を増進することを目的とする。本協定の規定は、証拠を取得、隠滅、又は排除すること、又は（本協定の）法的手続の執行を妨げることを含め、あらゆる私人の側に権利又は救済を生じさせるものではない。各締約国は、第9条の規定を含め、この協定の規定が各締約国の憲法上の構造及び原則に合致して完全に実施されることを確実にしなければならない。

### 第4条 対象の制限

1. 本協定の命令は、対象犯罪の予防、発見調査活動、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. 本協定の命令は、言論の自由を侵害し、人種、性別、性的指向、宗教、民族的出身又は政治的意見に基づいて不利益を与えるために利用されるものであってはならない。
3. 本協定の命令は、受領締約国の者を意図的に対象としてはならず、各締約国は、第 7.1 条に定められた本項の要件を満たすように対象を定める手続を定めなければならない。
4. 本協定の命令は、受領締約国の者に係る情報の取得を目的とした対象者を対象とするものであってはならない。
5. 本協定の命令は、特定のアカウントを対象とし、命令の対象として、特定の個人、アカウント、アドレス、個人デバイス、又はその他の特定の識別子を特定するものでなければならない。

## 第 5 条 命令の発出及び送信

1. 本協定の命令は、発出締約国の国内法に適合して発せられるものとし、明確で信頼できる事実、特定性、合法性、捜査対象の行為の重大性に基づく合理的な理由（reasonable justification）を基礎付ける諸要件を満たしていなければならない。
2. 本協定の命令は、発出締約国の国内法に基づき、命令の執行の前に又はその執行中に、裁判所、裁判官、マジストレイト（判事）その他の独立した主体による審査ないし監督を受けなければならない。
3. 有線又は電気通信の傍受に関する本協定の命令、及びその他の拡大的手段は、確定的で限定された期間であり、許可された命令の目的を達成するのに合理的に必要とされる期間を超えないものとし、より侵害的でない方法により同じ情報を合理的に取得できない場合に限り発せられなければならない。
4. 発出締約国は、受領締約国や第三国政府の要請に応じて、又はこれに提供する情報を獲得するために本協定の命令を発してはならない。
5. 発出締約国は、本協定の命令を対象プロバイダに直接発することができる。当該命令は、発出締約国の指定当局により送信されなければならない。両締約国の指定当局は、第 5.5 条から第 5.9 条、第 6.1 条、第 6.2 条に基づき各々が実施する機能の全部又は一部を、その他の当局が実施すること

を相互に合意することができる。両締約国の指定当局は、相互の合意により、当該その他の当局に関する規則及び条件を定めることができる。

6. 送信に先立ち、発出締約国の指定当局は、命令が本協定に適合しているかどうかを審査しなければならない。
7. 本協定の命令には、発出締約国の指定当局が、命令が適法であり、本協定の命令に関する発出締約国の重要な基準を含め本協定に適合していることの書面による証明が含まれていなければならない。
8. 発出締約国の指定当局は、命令に関して本協定を発動することを対象プロバイダに通知しなければならない。
9. 発出締約国の指定当局は、対象プロバイダに対し、命令に関する法的又は実務的な問題について情報を提供できる発出締約国の指定当局の連絡窓口を通知しなければならない。
10. 本協定の命令が、発出締約国の領域外に居住し、かつ発出締約国の国民でないと合理的に考えられる個人に関するデータについて発せられた場合、発出締約国の指定当局は、発出締約国が日常業務上の安全対策又は国家安全保障上有害であると考え、又は捜査の実施を妨げる場合、又は人権を侵害すると考える場合を除き、その個人が居住する第三国の適切な当局に通知しなければならない。
11. 両締約国は、本協定の命令を受領した対象プロバイダが、命令に関して本協定が適切に発動されていない可能性があると考え、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。当該異議は、一般的に、命令を受領した後、合理的な時間内に、最初に発出締約国の指定当局に提起されるべきである。対象プロバイダから命令に対する異議申立を受領した場合、発出締約国の指定当局はその異議申立に応じなければならない。異議が解決されない場合、両締約国は、対象プロバイダが受領締約国の指定当局に異議を申し立てることができることに同意する。両締約国の指定当局は、当該異議申立てを解決するために協議することができ、また、本協定に基づき申し立てられた問題について協議し、これに対処するために、定期的かつ必要に応じて会合することができる。
12. 受領締約国の指定当局が、いかなる命令に関しても本協定が適切に発動されることができないと認める場合には、発出締約国の指定当局及び関連す

る対象プロバイダにその旨を通知するものとし、本協定は当該命令には適用されてはならない。

#### 第6条 対象プロバイダによる情報の提供

1. 両締約国は、本協定の命令に応じて対象プロバイダが提供する対象情報は、発出締約国の指定当局に直接提供されるべきであることに同意する。
2. 発出締約国の指定当局は、適用されるべき法律に適合する範囲内で、本協定の命令及び本協定の命令に応じて提供された対象情報の安全な送信について、対象プロバイダと取決めを行うことができる。
3. 本協定は、発出締約国の法律に従って発せられた（本協定の）法的手続に応じ、対象プロバイダがデータを提供する法的義務を制限又は排除するものではない。
4. 対象情報の提供方法に関する発出締約国の要件には、対象プロバイダが、提供された記録の信憑性、又は当該記録の不存在もしくは非存在を証明する書式に記入することが含まれる。

#### 第7条 対象限定及び最小化手続

1. 各締約国は、本協定の命令の対象となるアカウントが対象者によって利用又は管理されているものであることを確保するために、誠実かつ妥当な努力を払うことにより、適切な対象を定める手続を定め、実施しなければならない。
2. 英国は、対象犯罪の予防、発見調査活動、捜査及び訴追に関連する対象情報を取得、保管及び配分する英国の必要性に合致するように、本協定の命令に従って取得された合衆国人に関する情報の取得、保管及び配分を最小限に抑える適切な手続を定め、実施しなければならない。
3. 本協定の命令に従って取得された情報の最小化手続には、対象犯罪の予防、発見調査活動、捜査及び訴追に関連する情報、又は死亡もしくは重大な身体的・物理的危険のおそれから保護するために必要な情報、又はその重要性を理解もしくは評価するために必要な情報とは認められない資料を、英国に分類、封印、削除又は不拡散を要求する規則が含まなければならない。

4. 最小化手続には、英国に対し、本協定の命令に従って取得された資料を速やかに審査するとともに、審査していない通信は適切な手続により訓練された者のみがアクセスできる安全なシステムに保管することを求める規則を含めなければならない。
5. 最小化手続には、最小化手続に従い、かつ、テロ、重大粗暴犯罪、児童搾取、国際組織犯罪、重大金融犯罪等の国家安全保障に係る犯罪など合衆国又は合衆国人への重大な侵害又は脅威となる通信を提供する場合を除き、本協定の命令に従って取得された合衆国人の通信の内容を、英国が合衆国に引き渡さしてはならないという規定を含めなければならない。
6. 各締約国は、他方の締約国と協議し、かつ他方の締約国の承認を得た上で、本条により定めることが求められる対象及び最小化手続を策定するものとし、これらの手続を変更する場合には、他方の締約国の承認を求めなければならない。

## 第8条 利用及び転送の制限

1. 本協定の他の条項に定められた制限を妨げることなく、発出締約国が本協定の命令に従って取得したデータは、プライバシー及び情報の自由に関する法律を含む発出締約国の国内法に従って取り扱われなければならない。
2. 発出締約国は、本協定の命令に従って受領したデータを、受領締約国の同意をあらかじめ得ることなく、第三国又は国際機関に転送してはならない。ただし、当該データが発出締約国の国内法に従ってすでに公表されている場合はこの限りでない。
3. 発出締約国は、本協定の命令に従って提供されたいかなる情報も、受領締約国や第三国政府と共有することを要求されない。
4. 発出締約国が、(本協定の) 法的手続に従って対象プロバイダからデータを受領する場合であって、次の各号のいずれかに該当する場合には、当該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利用する前に、発出締約国は受領締約国の指定当局を通じてその許可を得なければならない。受領締約国の指定当局は、必要とみなされる条件に従って許可を与えることができ、許可を与える場合、発出締約国はその条件に従ってのみデータを導入することができる。受領締約国が許可を与えない場合、発出締

約国は（本協定の）法的手続に従って受領したデータを当該方法で利用してはならない。

- 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起訴された事件の証拠として導入されることにより、自国の本質的利益が侵害される可能性があるとして宣言した場合
  - b. 合衆国が、合衆国にとって言論の自由の問題を引き起こす方法で、当該データが英国における起訴された事件の証拠として導入されることにより、自国の本質的利益が侵害される可能性があるとして宣言した場合
5. 本協定に定められたもの以外に追加される利用制限は、両締約国が相互に合意した範囲において課することができる。

## 第9条 プライバシー及びデータの保護措置

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、発見調査活動、捜査及び訴追に関連する個人情報保護に関する合衆国と欧州連合との間の協定」は、本協定の命令の執行において提供されるすべての個人情報に対して両締約国が準用し、同等の保護を提供する。合衆国にとって、この文脈において同協定第19条を実施する主な法律は、2015年司法救済法及び情報公開法である。
2. 本協定の命令の執行におけるデータの処理及び転送は、プライバシー及びデータ保護に関する両締約国の各適用法に従うものとする。

## 第10条 保存手続及び加入者情報

1. 各締約国は、電子データの保存、認証、開示及び提供に関連する国内法が、対象プロバイダに発出締約国の国内法に基づく犯罪の予防、発見調査活動、捜査及び訴追に関連する次の各号に掲げる（本協定の）法的手続に適合することを確保することを保証する。
  - a. 対象データ又は加入者情報の保存
  - b. 加入者情報の開示、提供、又は認証
2. 発出締約国は、対象プロバイダに直接当該手続を発することができる。当該手続は、発出締約国の国内法に適合し、審査ないし監督を受けて発せられなければならない。当該手続の法的効果は、発出締約国の法律にのみ基

づく。それ以外の場合は、対象プロバイダは、適切な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、妥当なものであり、犯罪の予防、発見調査活動、捜査又は訴追に関連する情報を取得する目的で発せら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、人種、性別、性的指向、宗教、民族的出身又は政治的意見に基づいて不利益を与えたりするために利用されるものであってはならない。
5. 当該手続に従って取得された加入者情報は、本協定の適用条項とともに、プライバシー及び情報公開に関する法律を含む発出締約国の国内法に従って取り扱われなければならない。
6. 発出締約国及び対象プロバイダは、適用法に適合する方法で、当該手続及びこれに応じて提供される加入者情報の安全な送信に関する取決めを行うことができる。
7. 発出締約国は、加入者情報を受領締約国や第三国政府と共有することを要求されてはならない。
8. 各締約国は、保存された対象データ又は加入者情報の保護に重大な影響を及ぼす、又は当該手続の実施を実質的に妨げる又は害するような国内法の重要な変更について、相手国に通知するものとし、本項に基づき生じる問題について協議しなければならない。
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、発見調査活動、捜査及び訴追に関連す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、当該手続に従って保存されるすべての個人情報又は提供される加入者情報に対して両締約国が準用しなければならない。合衆国にとって、この文脈において同協定第19条を実施する主な法律は、2015年司法救済法及び情報公開法である。
10. 本条で定められた保護措置とその法律の実施を含む各締約国の国内法に照らせば、当該手続に関して、プライバシーと市民的自由に対する実体法及び手続法上の強力な保護が存在する。当該手続に従ったデータの処理及び転送は、プライバシー及びデータ保護に関する両締約国の各適用法に合致するものである。
11. 加入者情報の提供方法に関する発出締約国の要件には、対象プロバイダ

が、提供された記録の信憑性、又は当該記録の不存在もしくは非存在を証明する書式に記入することが含まれる。

## 第 11 条 両立性及び非排除性

1. 本協定は、発出締約国が受領締約国及び受領締約国の司法管轄に属する対象プロバイダから電子データを取得又は保存するための他の法的権限及び仕組みにとって不利益となるものではなく、またこれらに影響を与えないものとする。これらの法的権限には、いずれかの締約国の国内法に基づく法的文書及び実務であって当該締約国が本協定を発動しないもの、刑事共助要請、緊急開示が含まれる。
2. 本協定は、本協定の命令及び第 10 条で定められる保存、加入者情報に対する当該手続から生じる強制措置に関し、2003 年 6 月 25 日に署名された合衆国と欧州連合との間の刑事共助に関する協定第 3 条 (2) に規定された文書の付属書第 18 条第 2 項、第 3 項、第 4 項、第 5 項、及び第 6 項の協議、他の手段の消尽、及びその他の要件を構成しなければならない。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刑事事件における刑事共助に関する合衆国政府と英国政府との間の条約の適用に関しても同様である。

## 第 12 条 実施の審査及び協議

1. 本協定の発効から 1 年以内、及びその後定期的に、両締約国は本協定の条件を遵守状況について審査しなければならない。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命令の発出及び送信の審査、及び本協定に基づいて定められた手続を修正するか否かを決定するための本協定の命令に従って取得されたデータの各締約国の取扱いの審査が含まれる。
2. 両締約国は、本協定の実施又は紛争解決に関して、必要に応じて協議することができるものとし、当該紛争はいかなる裁判所、法廷又は第三締約国にも付託されないものとする。
3. 本協定の実施に関する問題又は紛争が両締約国間で解決されない場合には、いずれの締約国も、特定の日付以降に発せられた（本協定の）法的手続

を含め、特定されたカテゴリーの（本協定の）法的手続に関して本協定を発することができないと結論付けることができる。その結論の通知は、その結論を出した締約国の指定当局によって、他方の締約国の指定当局に送らなければならない。通知された締約国は、当該通知を受領した時点で、特定されたカテゴリー内の（本協定の）法的手続に関して本協定を発してはならないものとする。当該結論は、他方の締約国の指定当局への取消の通知を通じて、結論に達した締約国により、いつでも、その全部又は一部を取り消すことができる。発出締約国に対して提供されたいかなるデータも、本協定に定める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. 各発出締約国の指定当局は、運用上又は国家安全保障上支障のない範囲で、本協定の利用に関する集計データを反映した年次報告書を受領締約国の指定当局に発行しなければならない。
5. 本協定は、対象プロバイダが受領した（本協定の）法的手続に関する統計情報を、適用法に従って報告することを、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

各締約国は、本協定の実施から生じる自らの費用を負担しなければならない。

### 第14条 改正

本協定は、両締約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 時間的適用関係

本協定は、本協定の発効日以後に発出締約国が発する（本協定の）法的手続に適用されなければならない。

### 第16条 発効

本協定は、各締約国がこの協定の発効に必要な措置をとったことを示す両締



約国間の外交上の文書の交換が完了した後の方の書簡の日付をもって発効する。

### 第17条 協定の満了及び終了

1. 本協定は、本協定の終了前に両締約国が外交上の文書の交換を通じて、本協定を更に5年間（又は両締約国間で合意されるその他の期間）延長することに書面で合意しない限り、5年間効力を有する。
2. 第1項に基づく満了とは別に、本協定は、いずれかの締約国が、外交上の経路を通じて他方の締約国に書面で通告することにより終了させることができる。終了は、当該通告の日から一カ月後に効力を生ずる。
3. 本協定が満了又は終了した場合、発出締約国に提供されたデータは引き続き利用することができ、本協定に定める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、それぞれの政府から正当な委任を受けて、本協定に署名した。

2019年10月3日にワシントンで、英語により2通を作成した。

アメリカ合衆国政府のために

ウィリアム・P・バー

英国政府のために

プリティ・パテル

## 2 重大犯罪対策のための電子データへのアクセスに関するアメリカ合衆国政府とオーストラリア政府との間の協定

四方 光監訳、趙 恩慶訳

アメリカ合衆国政府及びオーストラリア政府（以下、「両締約国」という。）は、公共の安全を保護し、テロリズムを含む重大犯罪対策という目的のために、両締約国が協力を強化するという相互利益に促され、適法な法執行目的のために電子データに適時にアクセスすることが、この取り組みにおいて不可欠な要素であることを認識し、プライバシーの保護、言論の自由を含む人権、市民的自由、法の支配を尊重することの重要性及びそれに対する共通の確約を強調し、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要件の弊害に留意し、そのような要件を回避するよう努め、電子データにアクセスするための両締約国のそれぞれの法的枠組みが、通信の内容にアクセスする際には、正当な理由又は疑うに足る合理的な根拠、独立した審査又は監督の要件を含め、プライバシー及び市民的自由を保護するための適切かつ相当な保護措置を組み込んでいることを認識して、次のとおり協定した。

### 第1条 定義

本協定の適用上、

1. 「アカウント」とは、アカウント、電話番号、アドレス情報など、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私的なアクセスを得るための手段をいう。
2. 「オーストラリア人」とは、(i) オーストラリアの市民、(ii) オーストラリアの永住者、(iii) 構成員の多数が (i) ないし (ii) に該当する法人格なき団体、又は (iv) オーストラリアで法人格を得た法人をいう。
3. 「コンピュータシステム」とは、欧州評議会のサイバー犯罪条約第1章第1a条に規定されているところによる。すなわち、あらゆる装置や、相互接続されたり関連付けられたりした装置のグループであって、そのうちプログラムに従ってデータの自動処理を行う一つ又は複数のものをいう。
4. 「対象データ」とは、対象プロバイダとしての資格において行動する私法

人が保有又は管理する、以下の種類のデータをいう。すなわち、電気通信又は有線通信の内容、ユーザのために保管又は処理されたコンピュータデータ、電気通信又は有線通信に関連するトラフィックデータやメタデータ、又はユーザのためのコンピュータデータの保管又は処理に関連するデータ、この定義で言及されている他の種類のデータも求める命令に従って求められる場合の加入者情報である。

5. 「対象犯罪」とは、発出締約国の法律の下で、テロ活動を含む重大犯罪を構成する行為をいう。
6. 「対象者」とは、第7.1条により要求される手続を適用した上で、第5条に従って命令のために本協定が発動された時点において、受領締約国の者でないと合理的に考えられる者をいう。
7. 「対象プロバイダ」とは、以下の範囲内の私法人をいう。
  - (i) コンピュータシステム又は電気通信システムにより、公衆に通信、コンピュータデータの処理又は保管の機能を提供する者
  - (ii) 第(i)号に定義される機関の代わりに対象データを処理又は保管する者
8. 「指定当局」とは、オーストラリアについては内務大臣が指定する政府機関をいい、合衆国については司法長官又は司法長官が指定する者をいう。
9. 「発出締約国」とは、関連する（本協定の）法的手続を発し、可能な場合には、本協定を発動する締約国（その地方行政機関を含む）をいう。合衆国が発出締約国である場合、合衆国内の連邦、州、地方、又は地域機関が発した（本協定の）法的手続が含まれる。オーストラリアが発出締約国である場合、オーストラリア内の連邦、州、又は地域機関が発した（本協定の）法的手続が含まれる。
10. 「（本協定の）法的手続」とは、本協定の対象となる命令、対象データの保存、又は加入者情報の保存、開示、提供もしくは認証に関連する手続をいう。
11. 「命令」とは、発出締約国の国内法に基づき発せられた対象プロバイダによる対象データの開示又は提供（当該データの認証の要求を含む）を要求する法的文書をいい、保管された通信、又は送信中の通信を含む。
12. 「個人データ」とは、識別された、又は識別可能な個人に関する情報をい

う。

13. 「受領締約国の者」とは、次に掲げる者をいう。

(i) 受領締約国の連邦政府機関又はその地方行政機関の機関を含む政府機関

(ii) 受領締約国の市民又は国民

(iii) 受領締約国において適法に許可された永住者

(iv) 構成員の多数が (ii) ないし (iii) に該当する法人格なき団体

(v) 受領締約国で法人格を得た法人

(vi) 受領締約国の領域内の居住者

14. 「受領締約国」とは、発出締約国以外の締約国（その地方行政機関を含む）をいう。

15. 「重大犯罪」とは、長期が3年以上の拘禁刑に処せられる犯罪をいう。

16. 「加入者情報」とは、氏名、住所、サービスの契約期間及び種類、加入者番号又は個人番号（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）、電話の接続記録、通話時間及びその長さ、支払手段など、対象プロバイダの加入者又は顧客を特定する情報をいう。

17. 「合衆国人」とは、次に掲げる者をいう。

(i) アメリカ合衆国の市民又は国民

(ii) アメリカ合衆国において適法に許可された永住者

(iii) 構成員の多数が (i) ないし (ii) に該当する法人格なき団体

(iv) アメリカ合衆国で法人格を得た法人

## 第2条 協定の目的

本協定の目的は、通信サービスプロバイダが一方の締約国から電子データの提供又は保存を求める（本協定の）法的手続を受けた場合、当該プロバイダが他方の締約国の法律の適用を受ける可能性がある時に、潜在的な法的義務の衝突を解決することにより、公共の安全とセキュリティを向上させ、プライバシーの権利、市民的自由、及び開かれたインターネットを保護することである。そのため、本協定は、各締約国が、自国の国内法の枠組み及び他方の締約国の国内法の枠組みに合致する方法で、重大犯罪の予防、発見調査活動、捜査及び訴追を目的として電子データを取得し、適切な対象選択及び利用制限、プライ

プライバシー保護、各締約国の国際人権保障及びその他の国際法の義務に合致する方法でそのデータを利用するための効率的、効果的、かつプライバシー保護的な手段を提供する。

### 第3条 国内法及び協定の効力

1. 各締約国は、電子データの保存、認証、開示及び提供に関連する国内法が、対象プロバイダに（本協定の）法的手続に適合することを確保することを保証する。各締約国は、本協定の実施を実質的に妨げる又は害するような国内法の重要な変更について、相手国に通告しなければならない。
2. 本協定の対象となる命令に関する本協定の規定は、発出締約国が本協定を発動し、関連する対象プロバイダーにその旨を通知した命令に適用されなければならない。（本協定の）法的手続の法的効力は、発出締約国の法律にのみ基づく。それ以外の場合は、対象プロバイダは、（本協定の）法的手続に対して適切な法的異議を申し立てる既存の権利を保持する。
3. 各締約国は、本協定を施行するにあたり、他方の締約国の国内法の枠組み（当該枠組みの実施を含む）が、本協定の対象となるデータ収集及び活動に関して、プライバシーと市民的自由に対する実体法及び手続法上の強力な保護を与えるものであることを認識する。
4. 対象プロバイダから（本協定の）法的手続に従って受領した個人データは、発出締約国の国内法の枠組みに従って保護されなければならない。プライバシーの保護には、各締約国の国内法枠組みの下での合理的な規制を条件として、以下が含まれる。
  - a. 個人データの利用及び開示を、それが取得された目的に反しない目的に制限すること。
  - b. 個人データの保管を必要かつ適切な場合に限り制限すること。
  - c. 個人データの紛失、不慮の又は不正なアクセス、開示、変更、破壊を保護するための保護措置。
  - d. 個人が自身に関する個人データへのアクセスを求め、取得し、不正確な個人データの訂正を適切な場合に求めるための枠組み。
  - e. 個人からの苦情に対応するための枠組み。
5. 各締約国は、（本協定の）法的手続に従って受領したデータの保護に重大な影

響を及ぼす国内法の重要な変更について相手国に通告するものとし、第5条又は第11条に従って本項に基づき生じる問題について協議しなければならない。

6. 本協定は、両締約国が特定の電子データを取得する能力を増進することを目的とする。本協定の規定は、証拠を取得、隠滅、又は排除すること、又は（本協定の）法的手続の執行を妨げることを含め、あらゆる私人の側に権利又は救済を生じさせるものではない。各締約国は、この協定の規定が、自国の中央政府と構成州又はその他の類似の領域内の組織との間の関係を管理する基本原則に合致して実施されることを確保しなければならない。

#### 第4条 対象の制限

1. 本協定の命令は、対象犯罪の予防、発見調査活動、捜査又は訴追に関連する情報を取得することを目的としなければならない。
2. 本協定の命令は、言論の自由を侵害し、人種、性別、性的指向、宗教、民族的出身又は政治的意見に基づいて不利益を与えるために利用されるものであってはならない。
3. 本協定の命令は、受領締約国の者を意図的に対象としてはならず、各締約国は、第7.1条に定められるとおり、本項の要件を満たすように対象を定める手続を定めなければならない。
4. 本協定の命令は、受領締約国の者に係る情報の取得を目的とした対象者を対象とするものであってはならない。
5. 本協定の命令は、特定のアカウントを対象とし、命令の対象として、特定の個人、アカウント、アドレス、個人デバイス、又はその他の特定の識別子を特定するものでなければならない。

#### 第5条 命令の発出及び送信

1. 本協定の命令は、発出締約国の国内法に適合して発せられるものとし、明確で信頼できる事実、特定性、合法性、捜査対象の行為の重大性に基づく相当な理由（reasonable justification）を基礎付ける諸要件を満たしていなければならない。
2. 本協定の命令は、発出締約国の国内法に基づき、命令の執行の前に、又は

執行中に、裁判所、裁判官、マジストレイト（判事）その他の独立した権限者による審査ないし監督を受けなければならない。

3. 有線又は電気通信の傍受に関する本協定の命令、及びその他の拡大的手段は、確定的で限定された期間であり、許可された命令の目的を達成するのに通常必要な期間を超えないものとし、より侵害的でない方法により同じ情報を合理的に取得できない場合に限り発せられなければならない。
4. 発出締約国は、受領締約国や第三国政府の要請に応じて、又はこれに提供する情報を獲得するために本協定の命令を発してはならない。
5. 発出締約国は、本協定の命令を対象プロバイダに直接発することができる。本協定の対象になる命令は、発出締約国の指定当局により送信されなければならない。両締約国の指定当局は、第 5.5 条から第 5.9 条、第 6.1 条、第 6.2 条に基づき各々が実施する機能の全部又は一部を、両締約国の政府のその他の当局が実施することを相互に決定することができる。両締約国の指定当局は、相互の決定により、当該主体に関する規則及び条件を定めることができる。
6. 送信の前に、発出締約国の指定当局は、命令が本協定に適合しているかどうかを審査しなければならない。
7. 本協定の命令には、発出締約国の指定当局が、命令が適法であり、本協定の命令に関する発出締約国の重要な基準を含む本協定に適合していることの書面による証明が含まれていなければならない。
8. 発出締約国の指定当局は、命令に関して本協定を発動することを対象プロバイダに通知しなければならない。
9. 発出締約国は、対象プロバイダに対し、命令に関する法的又は実務的な問題について情報を提供できる発出締約国の指定当局の連絡窓口を通知しなければならない。
10. 本協定の命令が、発出締約国の領域外に居住し、かつ発出締約国の国民、市民又は合法的な永住者でないと合理的に考えられる個人に関するデータについて発せられた場合、発出締約国の指定当局は、発出締約国が日常業務上の安全対策又は国家安全保障上有害であると考え、調査の実施を妨げる場合、又は人権を侵害すると考える場合を除き、その個人が居住する第三国の適切な主体に通知しなければならない。

11. 両締約国は、本協定の命令を受領した対象プロバイダが、命令に関して本協定が適切に発動されない可能性があるとは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。当該異議は、一般的に、命令を受領した後、合理的な時間内に、最初に発出締約国の指定当局に提起されるべきである。対象プロバイダから命令に対する異議申立を受領した場合、発出締約国の指定当局はその異議申立に応じなければならない。異議が解決されない場合、両締約国は、対象プロバイダが受領締約国の指定当局に異議を申し立てることができることに同意する。両締約国の指定当局は、当該異議申立てを解決するために協議することができ、また、本協定に基づき申し立てられた問題について協議し、これに対処するために、定期的かつ必要に応じて会合することができる。
12. 受領締約国の指定当局が、本協定の命令に関して本協定が適切に発動されることができないと認める場合には、発出締約国の指定当局及び関連する対象プロバイダにその旨を通知するものとし、本協定は当該命令には適用されないものとする。

## 第6条 対象プロバイダによる情報の提供

1. 両締約国は、本協定の命令に応じて対象プロバイダが提供する対象データは、発出締約国の指定当局に直接提供されるべきであることに同意する。
2. 発出締約国の指定当局は、適用されるべき法律に適合する範囲内で、本協定の命令及び本協定の命令に応じて提供された対象データの安全な送信について、対象プロバイダと取決めを行うことができる。
3. 本協定は、発出締約国の法律に従って対象プロバイダがデータを提供する義務を制限又は排除するものではない。
4. 対象プロバイダが命令に応じる方法に関する発出締約国の要件には、対象プロバイダが、提供された記録の信憑性、又は当該記録の不存在もしくは非存在を証明する書式に記入すること、命令及び応答として提出された情報又は証拠の秘密を保持されることが含まれる。

## 第7条 対象制限及び最小化手続

1. 各締約国は、本協定の命令の対象となるアカウントが対象者によって利用



又は管理されていることを確保するために、誠実かつ妥当な努力を払うことにより、適切な対象を定める手続を定め、実施しなければならない。

2. オーストラリア及び合衆国は、対象犯罪の予防、発見調査活動、捜査及び訴追に関連する対象データを取得、保管及び配分する両締約国の必要性に合致するように、本協定の命令に従って取得された合衆国人及びオーストラリア人それぞれに関する情報の取得、保管及び配分を最小限に抑える適切な手続を定め、実施しなければならない。
3. 本協定の命令に従って取得された情報の最小化手続には、対象犯罪の予防、発見調査活動、捜査及び訴追に関連する情報、又は死亡もしくは重大な身体的危害のおそれから保護するために必要な情報、又はその重要性を理解もしくは評価するために必要な情報とは認められない資料を、両締約国に分類、封印、削除又は不拡散を要求する規則が含まなければならない。
4. 最小化手続には、両締約国に対し、本協定の命令に従って取得された資料を速やかに審査するとともに、審査していない通信は適切な手続により訓練された者のみがアクセスできる安全なシステムに保管することを求める規則を含めなければならない。
5. 最小化手続には、最小化手続に従い、かつ、テロ、重大粗暴犯罪、児童搾取、国際組織犯罪、重大金融犯罪等の国家安全保障に係る犯罪など合衆国又は合衆国人への重大な侵害又は脅威となる通信を提供する場合を除き、本協定の命令に従って取得された合衆国人の通信の内容を、オーストラリアが合衆国に引き渡さしてはならないという規定を含めなければならない。
6. 各締約国は、他方の締約国と協議し、かつ他方の締約国の承認を得た上で、本条により定めることが求められる対象及び最小化手続を策定するものとし、これらの手続を変更する場合には、他方の締約国の承認を求めなければならない。

## 第8条 保存手続及び加入者情報入手手続

1. 発出締約国は、対象データの保存のみを、又は加入者情報の保存、開示、提供又は認証を求める（本協定の）法的手続を発し、対象プロバイダに直接

送信することができる。当該プロセスは、犯罪の予防、発見調査活動、捜査及び訴追に関連するものでなければならず、発出締約国の国内法に基づいて発せられ、必要に応じて審査ないし監督を受けなければならない。

2. 発出締約国及び対象プロバイダは、適用法に基づき、本条第1項で言及される（本協定の）法的手続及びこれに応じて提供される加入者情報の安全な送信に関する取決めを行うことができる。
3. 本条第1項で言及される対象プロバイダが（本協定の）法的手続に応じる方法に関する発出締約国の要件には、対象プロバイダが、提供された記録の信憑性、又は当該記録の不存在もしくは非存在を証明する書式に記入すること、（本協定の）法的手続及び応答として提出された情報又は証拠の秘密を保持されることを含めなければならない。

## 第9条 利用及び転送の制限

1. 発出締約国が（本協定の）法的手続に従って取得したデータは、プライバシー及び情報の自由に関する法律を含む発出締約国の国内法に従って取り扱われなければならない。
2. 発出締約国は、本協定の命令に従って受領したデータを、受領締約国の同意をあらかじめ得ることなく、第三国政府又は国際機関に転送してはならない。ただし、当該データが発出締約国の国内法に従ってすでに公表されている場合はこの限りでない。
3. 発出締約国は、（本協定の）法的手続に従って提供されたいかなる情報も、受領締約国や第三国政府と共有することを要しない。
4. 発出締約国が、（本協定の）法的手続に従って対象プロバイダーからデータを受領する場合であって、次の各号のいずれかに該当する場合には、上記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利用する前に、発出締約国は受領締約国の指定当局を通じてその許可を得なければならない。受領締約国は、必要とみなされる条件に従って許可を与えることができ、許可を与えた場合、発出締約国はその条件に従ってのみデータを導入することができる。受領締約国が許可を与えない場合、発出締約国は（本協定の）法的手続に従って受領したデータをそのように利用してはならない。

- a. オーストラリアが、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起訴された事件の証拠として導入されることにより、自国の本質的利益が侵害される可能性があるとして宣言した場合
  - b. 合衆国が、合衆国にとって言論の自由の問題を引き起こす方法で、当該データがオーストラリアにおける起訴された事件の証拠として導入されることにより、自国の本質的利益が侵害される可能性があるとして宣言した場合
5. 本協定に定められたもの以外に追加される利用制限は、両締約国が相互に合意した範囲において課することができる。

## 第10条 両立性及び非排除性

本協定は、発出締約国が受領締約国及び受領締約国の司法管轄に属する対象プロバイダから電子データを取得又は保存するための他の法的権限及び仕組みを不利益となるものではなく、またこれらに影響を与えないものとする。これには、いずれかの締約国の国内法に基づく法的文書及び実務であって、当該締約国が本協定を発動しないもの、刑事共助要請、緊急開示が含まれるがこれらに限定されない。

## 第11条 実施の審査及び協議

1. 本協定の発効から1年以内、及びその後両締約国が相互に決定した場合には定期的に、両締約国は本協定の条件を遵守状況について審査しなければならない。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命令の発行及び送信の審査、及び本協定に基づいて定められた手続を修正するか否かを決定するための本協定の命令に従って取得されたデータの各締約国の取扱いの審査が含まれる。
2. 両締約国は、必要に応じて又は本協定の実施に関する紛争を解決するために協議することができるものとし、当該紛争はいかなる裁判所、法廷又は第三締約国にも付託されないものとする。
3. 各発出締約国の指定当局は、運用上又は国家安全保障上支障のない範囲で、本協定の利用に関する集計データを反映した年次報告書を受領締約国の指定当局に発行しなければならない。

4. 本協定は、対象プロバイダが受領した（本協定の）法的手続に関する統計情報を、適用法に従って報告することを、いかなる意味においても制限又は排除するものではない。

## 第12条 費用

各締約国は、本協定の実施から生じる費用を自ら負担しなければならない。

## 第13条 改正

本協定は、両締約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。当該改正は、各締約国が改正を発効させるために必要な措置をとったことを示す両締約国間の外交上の文書の交換が完了した後の書簡の日付に発効する。

## 第14条 時間的適用関係

本協定は、問題となっている犯罪がこの協定の発効の前後に行われたか否かにかかわらず、この協定の発効日以後に発出締約国が発する（本協定の）法的手続に適用されなければならない。

## 第15条 発効

本協定は、各締約国がこの協定の発効に必要な措置をとったことを示す両締約国間の外交上の文書の交換が完了した後の書簡の日付をもって発効する。

## 第16条 協定の満了及び終了

1. 本協定は、5年間効力を有する。両締約国は、本協定の延長について書面で合意することができる。
2. 第1項に基づく満了とは別に、本協定は、いずれかの締約国が、外交上の経路を通じて他方の締約国に書面で通告することにより終了させることができる。終了は、当該通告の日から一カ月後に効力を生ずる。
3. 本協定が満了又は終了した場合、本協定の規定は、本協定が満了又は終了した日以前に既に発せられた本協定の命令に関して引き続き適用されなければならない。

4. 本協定が満了又は終了した場合、発出締約国に提供されたデータは引き続き利用することができ、本協定に定める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、それぞれの政府から正当な委任を受けて、本協定に署名した。

2021年12月15日にワシントンで、英語により2通を作成した。

アメリカ合衆国政府のために

メリック・ガーランド

オーストラリア政府のために

カレン・アンドリュース