【副読本 資料 ④】

『法務、リスク管理、クラウド主権、プライバシー、行政分野 参考教材』

ガバメント用クラウドの コンプライアンス対策としての 最高裁住基ネット合憲基準に照らした 米国クラウド法に関する調査研究

～ 国・地方自治体システムにおける
米国クラウド法を原因とする
日本国憲法および行政個人情報保護法違反の
リスクを安全解消する現実的方法の考察 ～

未発表のメモのため、参加者限り【再配布禁止】

2026/02/14

登 大遊

本資料は、独立した筑波大学の一研究者として自己の責任で技術研究および戦略立案手法のアイデアを述べるものであり、登の所属している各組織の見解を示すものではありません。また、本資料は個人で作成したメモであり、内容には誤りがある可能性があります。誤りを発見されましたら、dnobori@cs.tsukuba.ac.jp までお知らせいただければ幸いです。

内容

この資料は、ほとんど 2023/11/25 (土), 26 (日) の 2 日間に、図書館に篭って様々な書籍を調べながら急いで書いたものであり、また、法律は私の専門分野とまったく異なることから、誤りが存在する可能性が、他の技術系の資料と比較して、かなり高い確率で存在すると思います。その点をご了承いただきお読みいただければ幸いです。米国クラウド法については、ガバメント用クラウドに今後各自治体のシステムが次々と移行されてゆくと、適切な対策をとっていない場合、取り返しがつかない事態が発生し、住基ネットを越える大社会的問題に発展する可能性があると考えたので、この資料は、精度よりも速度を優先して、作成しようと考えました。内容について、法律の専門家の方々に精査していただく必要があると思います。そもそも、憲法的観点、個人情報的観点からの法律専門家による十分な検討がまだまだ足りていない部分があるように感じられます。その懸念をもう少し詳しく述べると、次のようになります。行政機関における IT システムに関する情報セキュリティやコンプライアンスについては、① これまで、何か少し新しいことをしようとか、コンピュータやネットワークの試行錯誤を行なおうとする際に、過度といえるほどに、『何物も容易に信じない』という、石橋を叩いた慎重さを要求してくる牽制力が存在してきました。ところが、なぜか、② ガバメント用クラウドに関しては、従来の ① と比べものにならない程の新たなリスクがあるにもかかわらず、巨大な一極集中型の米国系パブリッククラウド事業者を利用する際において発生し得るセキュリティのリスクや、本文書でみるような憲法上・個人情報保護法上のコンプライアンスリスクについて、従前の ① で通常みられる慎重な牽制力が逆にあまりみられないように感じられるのです。比例原則からいって、① における何物も容易に信じないという、石橋を叩いた慎重さを伴う牽制力は、② に取り組む際にこそ、そのリスクの大きさに比例し、最大限に加重され、推進に対する保守的な力となって、その効果を発揮させるべきであると思われるのです。

第１節　はじめに

サイバー攻撃者により、巨大な一極集中型パブリッククラウドサービスのサービス基盤領域 (特権領域) に対する侵入と最高水準の権限の奪取がひとたび行なわれると、そのクラウドサービス上のすべてのシステムのセキュリティ (完全性、機密性、可用性) のいずれもが損傷を受けるリスクが生じる。別に作成した資料は、サイバー攻撃者から国民情報を保護するセキュリティを実現するために最低限必要な措置を述べたものであった。

その後、著者は、日本以外の他の先進国の行政クラウドにおいて、前記のサイバー攻撃耐性をどのような手段で保障しているのか、興味を持った。そこで、主にヨーロッパ先進国の事例を調査研究してみた。その調査は期間とコストの問題から必ずしも十分なものではないが、一応の調査結果は、資料「④ - 2」として、共有をした。

この 資料「④ - 2」に係る調査研究を行なうにあたり、意外なことが判明した。ヨーロッパの先進国各国においては、最近、行政クラウドサービスの基盤として米国のパブリッククラウドサービスを利用する場合、「米国クラウド法」 (CLOUD Act: Clarifying Lawful Overseas Use of Data Act) と呼ばれる、2018 年 3 月 23 日に米国で成立した米国国内法が、きわめて大きな脅威として認識されているという点である。現在、他国の先進国においては、米国クラウド法にまつわるセキュリティ (機密性) と人権 (プライバシー権) の諸問題が、高度なサイバー攻撃の脅威よりもなお一層深刻なものと位置付けられているように見えるのである。

日本においては、日本の行政クラウドで米国系パブリッククラウド事業者を利用する際に、米国クラウド法に関連して、いかなる問題が発生し得、それらを予防するためにいかなる措置を講ずるべきであるかについて、十分な検討と対策がなされていないようである。そもそも米国クラウド法とは具体的にどのような構造となっており、何を規定しているのか、何が問題なのか、という最も根本的な部分の情報すら、日本人は、これまで、ほとんど確認、議論していないように見える。日本の行政クラウドにおける米国クラウド法による影響に関連する議論がわずかに存在

するのみである。ところが、米国クラウド法について議論するのであれば、まず、同法の条文 (原文) にあたらなければならないのに、どうやら、条文を十分に読まれ、理解された上で議論がなされた形跡があまり無いようなのである。

たとえば、米国クラウド法について考えるとき、米国刑事訴訟制度に関連して米国の連邦政府または州政府の捜査官は米国クラウド法をどのように活用でき、どのような範囲で米国系パブリッククラウド事業者を経由して日本国民のプライバシーデータが合法的に取得可能であるのかは、重要な問題である。加えて、そのような合法的データ取得がなされるときに、果たして、契約者 (顧客) である日本政府に対して通知がなされるのか、日本政府は適法に異議申立てを行なうことができるのか、その異議申立ては契約者である日本政府から直接的に当該米国連邦または州政府あるいは米国管轄裁判所に対して直接的に可能であるのか、それらの司法判断は正しく日本の裁判権に服するのかが重大な問題である。仮に、米国系パブリッククラウド事業者が米国政府の命令に従ったとして、日本政府に対する債務不履行、または各国民に対する不法行為を構成するとき、損害賠償請求が可能であるか、その賠償請求の審理は日本の裁判権に服するのか、その結果得られた判決は本当に執行可能であるか等も、日本国政府または国民が被る損害を回復するために極めて重要な論点である。日本政府および地方自治体が米国系パブリッククラウドサービスを利用する場合は、当然、こういった、とても基本的な事柄について、十分に審議検討されている必要があるのだが、その形跡がなかなか見あたらないのである。

インターネット上で、「米国クラウド法」で、日本語で情報検索をすると、米国系パブリッククラウド事業者自らが解説した日本語記事が、いくつか発見できる。ここに掲載されている情報は不完全であり、重要な事柄が欠けているように見える。日本人ユーザー各個人や日本国の主権者の信任を受けている日本政府のデータの保護のために、米国系パブリッククラウド事業者は、十分丁寧な解説をなすべきであるが、そういった資料は、全然見あたらないのである。米国系パブリッククラウド事業者自らが「米国クラウド法」について解説する際の文章には、あまり詳しく調査研究していないのか、不十分な点があいまいに暈かされてしまっていて、本当に存在するリスクを見えなくしてしまうように見えてしまう効果を、結果的に、

生じさせている。おそらく、米国系パブリッククラウド事業者には、このことについて、何ら悪意はないのであろう。だが、われわれ日本人、特に行政関係者は、米国クラウド法について、クラウド事業者側の情報のみを、鵜呑みにしていては、全然安心できなさそうである。関係者それぞれが、自分の目で米国クラウド法を読み、関連する事柄を理解した上で、リスクへの対処方法を考えなければならない。なぜならば、ガバメント用クラウドと米国クラウド法に関連する問題について、これから、過去の住民基本台帳ネットワークシステムに係る問題を再燃させる可能性がある識者たちは、それぞれが、自らの目で米国クラウド法を読み、関連する事柄を理解した上で、リスクを直球的に指摘してくる能力を、十分に有すると考えられるためである。そういった指摘は、国会で、裁判所で、または地方自治体の議会で、いつでも、発生し得る。そのような議論に呼応して、すでに問題対処を行なっていますと堂々と自信を持って返答することができるようにして信頼を勝ち取るためには、われわれ行政主体は、この問題を回避し先延ばしにするのではなく、今、問題に向き合って、一応の解決策を提示できるようにしなければならないのである。

日本政府および地方自治体が、ガバメント用クラウドにおいて、米国系パブリッククラウド事業者を利用して国民のプライバシーデータを保存・処理するに際し、最大のリスクは、やはり、① 日本国民からの訴訟リスクと、② 鋭い観点を持った多数の政治家や活動家の方々からの民主的論難への対応問題の、2 点であると思われる。これらは、いってみれば、2000 年代に住民基本台帳ネットワークシステムに関連して発生した事象が、またもや変形して再燃するというリスクである。現在のままでは、米国クラウド法にまつわる未解決・未整理の諸問題が、この ①、② のようなこの種の問題の次回の発生源となる可能性が、きわめて高い。そこで、われわれは、この大問題が表面化して炎上しないように予防しなければならない。われわれは、この問題が水面下にある今の間に、十分な予防策と理論構造を構築し、できるだけ、この問題をより良く解決しておくべきである。幸運と言って良いのかどうかわからないが、偶然にも、現在の日本社会においては、識者の多くは、①、② に関連して、米国クラウド法に関わるガバメント用クラウドの問題を、未だ重大な問題として気が付いていないようである。だから、今の間にこの問題に対処す

れば、コストは小さい。だが、もし、今、この問題に対処せずにこれを放置すると、後になって、必ず、住民基本台帳ネットワークシステム論争を大きく超える大論争に発展するであろう。それは、避けなければならない。われわれが今努力をして対策を施せば、その問題は、必ず避けることができる。

上記の ① 訴訟リスクは、日本国民各個人によって、彼らの個人情報が、米国クラウド法における米国政府機関による取得対象となっている具体的危険性を認識されたならば、すぐにでも、各地方公共団体や国に対して、多発的に発生するおそれがある。そして、万一、違憲判決が出ると、それは、致命的である。住民基本台帳ネットワークシステム訴訟は、高裁では、一度違憲判決が出てしまった。最高裁で、紙一重の衡量で合憲に覆った。その際に重要な合憲規範が示された。その合憲規範に沿って、われわれは、これから、今回の米国クラウド法の問題を予防する必要がある。

上記の ② 論難リスクは、① 訴訟リスクと密接に関連して生じる可能性もあるが、本質的には ① よりも影響範囲が大きいものである。国会やマスメディアを巻き込んだ大議論に発展するおそれがある。2000 年代の住民基本台帳ネットワークシステムに係る論争と訴訟を思い出すと、プライバシー権が侵害されたことに関する具体的な個々の損害というよりも、むしろ、行政が導入するネットワークシステムにおける、プライバシー権が侵害される危険の有無という抽象的な論点をめぐって争われていたのである。これにより、日本国民全体に、「住基ネットは、リスクがあるものである。」というイメージが広まり、固定化されてしまった。日本国民には、戦後、このような個人情報の一元的集約と処理に関する健全なリスク観念が総体的に存在する。そのリスク観念は、行政府 (特に、行政府のコンピュータ技術者たち) が普段考えているよりも、なお一層、大きなものである。今回の米国クラウド法に関連する問題においても、個々の具体的な損害というよりも、システム的な根本的・抽象的な問題が論争の対象となる可能性が、きわめて大きい。もちろん、米国クラウド法に基づき、米国連邦政府または米国州政府に属する個々の捜査員は、日本政府または地方自治体の米国系パブリッククラウド上の日本国民の個人情報データベースを (「資料 ③」で記述されているような、「クライアント側暗号化」等を適切に

施すといった、後述の適切な保護を行なわない限りにおいて)、適法な捜査令状、裁判所命令状または召喚状を取得すれば、いつでも、ダウンロードし、捜査機関のコンピュータ上で閲覧して分析することができてしまう。これによって、もちろん、個々の損害は発生する。だが、実際にどれくらいの損害が、日本政府、日本の地方自治体および日本国民に発生するかは、その具体的事案によって定まるので、予測することは困難である。それよりも、そもそもいつでもそのような日本の司法の審査権に服さない、他人 (外国政府) による日本国民の個人情報の無断のデータ取得が可能であるという状態こそが、憲法上の問題として、大きく取り上げられるリスクが高いのである。

住基ネット訴訟が 2008 年の最高裁判決により一旦は落ち着いたことにより、この 15 年間くらいは、日本国民の行政デジタル化に対するリスク反応は、いったんは沈着しているように見える。国会と行政府は、例えば、マイナンバーやマイナンバーカード、ガバメント用クラウド等の企画と導入にあたり、このような沈着している日本国民のリスク観念を不必要に刺激しないように十分注意をしながら、おそるおそる、行政事務のデジタル化を進めてきた。だが、われわれがいま一層注意しなければならないのは、日本国民のリスク感覚の質量と性質は、決して減少・消滅した訳ではないという点である。そのような国民感情の減衰を示唆する根拠はない。国民のリスク感覚の程度は、従前と同じ健全な水準で維持されている。ただ、国会と行政府が前述のとおり注意深く慎重に行動をしてきたことの成果として、今のところは、大きく再燃するに至っていないだけに過ぎない。だが、ひとたび、ガバメント用クラウドに関連して、米国クラウド法に関する健全な識者の注目が生じると、他の先進国と同様に、大論争が生じ、2000 年代と同型の市民情報のプライバシー問題が再燃するおそれが高い。折角スムーズに進行してきた行政のデジタル化を、再び著しく停滞させることになりかねない。その結果、国政に対する支持率は大きく低下してしまうおそれがある。そのような事態は、避けなければならない。折角強力に推進することができている、現在の国の行政デジタル化に水を差す原因は、解消しなければならない。

加えて、米国クラウド法の諸問題が過度に論争の対象とされたならば、これまで、

戦後極めて良好な関係で維持されている、日米間のパートナーシップ関係にも、影響が生じるリスクがある。米国クラウド法の問題が大きく取り上げられた場合、これは、日本と米国との間の協調関係にも関連する問題として、国民に認識される。一般に、日本人の米国に対する政治的感情は複雑であり、二面性を有しているようである。日本人は、普段は米国に対する一方の否定的な感情は隠されており、肯定的な友好関係が顕われている。だが、日本の大衆において水面下に蓄積されている米国に対する否定的感情は必ずしも消滅しておらず、何らかの契機があると一気に不信感が表面化するという現象が歴史的に見られる。

このように考えると、日本の行政クラウドにおいて米国系パブリッククラウド事業者を利用する際における、米国クラウド法に関する問題は、(a) 一般的国民が有している個人情報に関する日本政府へのリスク観念の問題 (住基ネットの延長線上の国内問題) と、(b) 米国に対する感情的問題 (国際問題) との 2 つがちょうど重なっているという、稀に見る重大な問題であるように思われる。(a) の問題は、前述のとおり行政のデジタル化、効率化を損なう問題であるため、丁寧に解決しなければならない。(b) の日米関係は、両国にとって、最大級に重要な財産であるから、日米信頼関係への深刻な影響が日本国の内部から生じ得るリスクは、最小化しなければならない。この 2 点が結合した将来の政治的大問題が発生しないよう、われわれは、この問題が小さい今のうちに、この問題に行政的に対処することが重要である。

著者は、当初、米国クラウド法について、全く関心がなかった。「資料 ③」の作成においては、主要な脅威として、不法に侵入を企てるサイバー攻撃者のみを想定しており、外国政府によって当該外国の法に基づき合法的にプライバシーデータの機密性が侵害されるリスクについては全く想定していなかった。しかし、その後、他の先進国の事例 (資料 ④ - 2) を調査する過程で、米国クラウド法について強い関心を得て、これをちょっと調査してみようと考え、色々調べたところ、日本のガバメント用クラウド計画においても、米国系パブリッククラウド事業者を採用するに際し、他の先進国と同様に重要な法的および政治的リスクが存在しているように思われた。本文書は、数日で調査可能な範囲で誠に不十分な出来であるが、日本の

ガバメント用クラウドについて、米国クラウド法に関連して生じると思われる問題とその予防策の研究結果を、一応、文書にしてまとめたものである。

第 2 節　自治体管理職とデジタル人材との深夜のガバメント用クラウドと米国クラウド法に関する諸問題の談論

行政管理職 X 「君は、行政コンピュータ技術者か？」

行政デジタル人材 Y 「そうだ。」

行政管理職 X 「夜遅くまで、コンピュータを触って、何をやっているのか。」

行政デジタル人材 Y 「われわれ自治体のシステムを、ガバメント用クラウドに移行する作業をしているのだ。」

行政管理職 X 「ガバメント用クラウドとは何か？」

行政デジタル人材 Y 「国が、ボリュームディスカウント効果を目的として、パブリッククラウド事業者と一括で契約し、これをわれわれ自治体に再販する構造となっている、クラウドサービスのことである。」

行政管理職 X 「今、君は、ガバメント用クラウドに、われわれ自治体のいかなるシステムたちを、移行しようとしているのか？」

行政デジタル人材 Y 「われわれ自治体が従前より大切に有する、市民管理のためのシステム群である。住民基本台帳、戸籍情報、税務記録、健康保険記録、生活保護情報、就学情報、障害者情報、健康管理情報、印鑑登録印影データ、失業保険情報、図書館貸出履歴、等の情報を処理・管理するシステムといったものを、次々

と、移行しようとしているのである。」

行政管理職 X 「私は、管理者だから、それらの各システムのことは、よく知っている。それらは、市民の内面にも関わる機微な個人情報が入っていることもあるシステムだから、法令に基づいて他の自治体や国の機関にデータを提供する場合をのぞき、決して第三者に開示してはならないということで、高い水準のセキュリティ (特に機密性) を、常に立派に維持するよう、歴代の名高い市長たちにいつもうるさく言われてきたのである。そこで、安全性を担保するため、われわれはこれまで、閉域網にプライベートクラウドを作り、これを長年運営してきたのである。これを商用の公衆向けパブリッククラウドサービスで構成されるガバメント用クラウドに移行することで、セキュリティは低下しないか？」

行政デジタル人材 Y 「ガバメント用クラウド上に作る IaaS の VM やその仮想ディスクを含むクラウド領域は、われわれ自治体専用に割り当てられ、自ら支配・管理する領域となっている。他の自治体や国の機関、その他の第三者などは、アクセスができないから、従前と比較して、セキュリティレベルは、変わらない。」

行政管理職 X 「それは結構なことである。セキュリティについて検討・判断するときは、様々な要素を、深く観察・分析する必要がある。検討対象は、技術的な側面と、法的な側面の 2 つに大別できる。技術的側面について、ガバメント用クラウドを支えるクラウド基盤の広大な特権領域、すなわちすべてのクラウドユーザー間で共有される根本的共通部分は、われわれから検証不能な部分であり、ここにセキュリティ上のリスクが存在し得る。しかし、本日は、この技術的能力の側面についての議論はひとまず留保する。これから、法的側面について、少し議論をすることにしよう。さて、われわれ行政の仕事において、最も重要なものはなんだろうか？」

行政デジタル人材 Y 「行政の仕事で最も重要なのは、もちろん、第一に、憲法遵守義務である。第二に、法律に基づく行政の原則である。」

行政管理職 X 「憲法遵守義務と、君の今回のシステム移行の仕事の間には、どのような関連性があるのか。」

行政デジタル人材 Y 「憲法 13 条の幸福追求権が大きく関係する。幸福追求権

には、プライバシー権が含まれていると解される (京都府学連事件最高裁判例 最大判昭和 44 年 12 月 24 日、住基ネット事件最高裁判例 最判平成 20 年 3 月 6 日)。住基ネット判例は、個人情報をみだりに第三者に開示されない自由は憲法 13 条によって保障されると認めている。」

行政管理職 X 「住基ネット判例は、もう 15 年も前のことだが、われわれ行政関係者は全員よく覚えているのである。さて、個人情報を『みだり』に第三者に開示されない自由というが、『みだりに』とは、より正確には、どういう意味だろうか。」

行政デジタル人材 Y「ちょっと同判例の表現を借りれば、『法令等の根拠に基づかずに又は正当な行政目的の範囲を逸脱して』、という意味だと考える。」

行政管理職 X 「なるほど。ところで、住基ネット判例は、結局住基ネット接続を合憲として、大阪府守口市を勝訴させているが、どのような理論で住基ネット接続を合憲化したのだろうか。」

行政デジタル人材 Y 「住基ネット判例は、次の 3 つの理論構造になっているようである。(1) 扱われる情報は氏名住所等の 4 項目に住基コードを合わせたものであり、従前より本人確認のため自治体間でやりとりされている情報に過ぎず、個人の内面に関わるような秘匿性が高い情報は含まれないこと。(2) 市町村から県を通じて国の機関 (J-LIS) の全国サーバーにこれらの情報が送付され保存されるが、全国サーバーを設置管理する J-LIS 役職員はみなし公務員であり、公務員守秘義務という刑罰付きの法制度上の情報漏えい対策がなされていること。(3) システム技術上も個人情報が容易に漏えいする具体的危険がないこと。よって、個人情報が法令等の根拠に基づかず又は正当な行政目的の範囲を逸脱して第三者に開示または公表される具体的危険が生じているとはいえず、合憲としたのである。」

行政管理職 X 「その住基ネットの合憲基準に照らすと、今回のわれわれのシステムのガバメント用クラウドへの移行は、合憲と評価されるだろうか、考えてみよう。判例理論 (1) については、どうだろうか。」

行政デジタル人材 Y 「確かに、ガバメント用クラウドに移行する予定の、税務記録、健康保険記録、生活保護情報、就学情報、障害者情報、健康管理情報、失業

保険情報、図書館貸出履歴、等の情報を処理・管理するシステムの情報には、判例理論 (1) の個人の内面に関わるような秘匿性が高い情報が含まれていることは、間違いがない。」

行政管理職 X 「なるほど。すると、ガバメント用クラウドに移行して扱われるプライバシー情報の機微性は、住基ネットと比較して各段に高いことになれば、ガバメント用クラウド利用行為が違憲となってしまう心配が生じないか？」

行政デジタル人材 Y 「それは大丈夫だ。住基ネットへの接続と、ガバメント用クラウドの利用とは、性質が異なる。住基ネットは、われわれ自治体と、他の自治体や国の機関との間で、市民の個人情報を共有・交換する仕組みであるが、他の自治体や国の機関はわれわれ自治体から見て異なる法人 (行政主体) であるから、第三者提供の問題として憲法問題となったのである。だが、ガバメント用クラウドの利用は、先に述べたとおり、単に国がパブリッククラウド事業者からボリュームディスカウントを得ることを目的に一括契約した大きなクラウド領域を切り出して、国から各自治体に再販し、各自治体がこれを利用するだけであって、各自治体のクラウド領域は、国や他の自治体 (他人) からシステム技術上隔離されている。だから、ガバメント用クラウドに移行したとしても、単にわれわれが自らパブリッククラウド事業者と契約してクラウドを利用することと同様の構造となるだけで、第三者に個人情報を開示してしまう具体的危険は生じない。判例理論 (2), (3) に照らして考えれば、ガバメント用クラウドの利用は、合憲だと考えている。」

行政管理職 X 「なるほど。ところで、ガバメント用クラウドは国が一括契約したクラウド基盤であるとのことだが、それらの事業者はどのような事業者か。」

行政デジタル人材 Y 「そのことは重要なので、国に質問をしたら、事業者は数社あり、いずれも、米国系パブリッククラウド事業者である、とのことである。それらの事業者と国がそれぞれ一括契約をし、われわれ自治体に再販して利用させる仕組みとなっている。」

行政管理職 X 「判例理論 (2),(3) に照らして、今少し深く検討してみよう。ガバメント用クラウドのサーバーは、誰がどこに設置し、管理するのか。」

行政デジタル人材 Y 「ガバメント用クラウドのサーバーは、米国系パブリック

クラウド事業者が、日本国内のデータセンタに設置し、彼ら米国系パブリッククラウド事業者またはその関連会社の取締役および従業員たちが管理すると聞いている。」

行政管理職 X「判例理論 (2) においては、住基ネット全国サーバーにデータを預けるとして、全国サーバーを設置管理する J-LIS の役職員がみなし公務員とされ、刑罰により守秘義務を遵守させる法制度上の担保があるから、住基ネット全国サーバーにデータを送付しても、そこから先にデータが漏れるおそれがないとして合憲していた。ガバメント用クラウドのサーバーを米国系パブリッククラウド事業者が設置管理しているとしたら、住基ネット判例と比較すると、米国系パブリッククラウド事業者が J-LIS に相当し、米国系パブリッククラウド事業者の取締役や従業員が J-LIS 役職員に相当するように見える。これらの米国系パブリッククラウド事業者の、実際にサーバーを設置管理する行為を担う取締役や従業員たちには、日本法に基づき、J-LIS 役職員と同等程度のみなし公務員としての公法上の守秘義務が課せられているのか？ また、いずれも日本人であるか？」

行政デジタル人材 Y「彼ら取締役や従業員には、そのような公法上の守秘義務は、課せられていない。また、彼ら取締役や従業員の中には、数多くの外国人が含まれていると聞いている。」

行政管理職 X「そうすると、米国系パブリッククラウドを利用することは、住基ネット判例理論 (2) に照らして、漏えいを予防するための法制度上の担保がなく、違憲となるリスクがあるのではないか？」

行政デジタル人材 Y「あなたのその理論は、正しくない。あなたが、これから、マルチテナント型の仮想化技術 (VM 技術、仮想ディスク技術) の登場以後の技術に関する理解を進めれば、住基ネット判例の前提となるシステム構造と、ガバメント用クラウドのシステム構造とは異なることが理解いただけるであろう。ガバメント用クラウドにおいては、確かに、物理サーバーは、米国系パブリッククラウド事業者の取締役や従業員によって設置管理される。そして、確かに、1 つの物理サーバー群に、他人である他の自治体や国や国の機関のシステムや、より敷衍すれば、実のところ、行政と全く関係がない民間ユーザーのシステムが、混在して動作すること

になる。だが、その多数ユーザーを混在させて動作している 1 つの物理サーバー群の内部は、米国系パブリッククラウド事業者の優秀な少数人数の仮想化技術基盤を熟知したプログラマによって、ユーザーごとに、正しく分離されている。彼らプログラマたちは、CPU の共用においては米国インテル社、AMD 社等の CPU 仕様に基づく Intel VT 等と呼ばれる技術で論理的分離がなされる。この部分が、ハイパーバイザと呼ばれるプログラムであり、その具体的実装、ノウハウと動作原理は、各社の企業秘密になっていて、決して公開されない程度に、重要なものである。また、物理ディスクの共用においては、物理ディスク上にファイルシステム類似概念を作り出し、そのファイルシステム類似構造上に、ファイル的概念としての仮想ディスクを設置するが、それらの各仮想ディスクのファイルは、ユーザー組織ごとにアクセスコントロールがなされていて、そのアクセスコントロールは、前記のような米国系パブリッククラウド事業者の優秀な少数人数のセキュリティを熟知したプログラマによって、コードとして実装されているのである。その具体的実装、ノウハウと動作原理も、各社の企業秘密になっていて、決して公開されない程度に、重要なものである。」

行政管理職 X 「君のいう複雑・高度な技術について、私には細部が分からなかったが、大まかには理解した。君の主張したいことは何か？」

行政デジタル人材 Y 「要するに、米国系パブリッククラウド事業者において多数ユーザーを混在させて動作している 1 つの物理サーバー群を物理的に観察すると、確かに分離がなされておらず漏えいの危険があるように見えるが、論理的には、その懸念はないからどうぞ安心してほしい、ということである。われわれ技術者の視点から、ガバメント用クラウドを実質的に評価すると、ガバメント用クラウドは、従来のような物理的なデータセンタにおいて、通常はラック間を物理的に分離し、あるいは少なくとも物理サーバー間を分離して、物質的に分離してきたことと同等程度に、われわれ自治体と他の自治体または国あるいはサーバーを混在利用している民間の無関係なユーザーたちとの間で、強度な分離が提供されているから、漏えいを予防するためのシステム技術上の担保があり、違憲となるリスクはない、ということである。」

行政管理職 X 「確かに、従来型システムでも、われわれ自治体は必ずしも庁舎内のサーバー室にサーバーを置くことなしに、民間データセンタを借りて、その中に専用のサーバーを置いて、それを民間業者に有償で運用してもらっていた。民間データセンタでは、ラックの壁とか、少なくともサーバーの外壁に護られて、他の同一のデータセンタを利用する他の顧客との混在的単一施設利用状況下であっても、われわれの有する市民個人情報が外部に漏れるリスクはほとんどなかった。唯一あるとすれば、当該民間データセンタを共用利用している他人、または不法に侵入した他人が、われわれのサーバーラックの鍵を無断で開き、サーバーを物理的に持ち出す行為は物理的に可能であったが、そのような犯罪者がそのような行為を行なうためには法律に違反しなければならず、そのペナルティはとても大きいから、そのような犯罪者によるそのような犯罪が出現するリスクは極めて低く、具体的危険が生じているということもいえなかった。このような理論により、従来の自治体システムにおいて、民間データセンタを利用することは、たとえその中の物理ディスクに住民のプライバシー情報が含まれていたとしても、合憲であったのである。この構造に対して、是非ともちょっと違憲を主張したいと考える市民が攻撃を行なうためには、(i) 自治体の庁舎内に住民の個人情報を含むサーバーを置く場合と、(ii) 民間データセンタに住民の個人情報を含むサーバーを置く場合とで、(i) よりも (ii) のほうが危険で、プライバシー情報の保護に欠けるという旨を、その市民は主張しなければならなかった。だが、われわれは、(i) 庁舎の室内にサーバーを置くよりも、(ii) 民間データセンタにサーバーを置くほうが、むしろ防犯上セキュリティが高く、漏えいのおそれが少ないと、主張することができる状態になっていて、そのような市民による主張は脅威ではなかった。よく思い出せば、そういうふうな理論は、確かに昭和の終わりごろから平成の中頃にかけて、各自治体内で管理者と技術者とが熱心に議論してきた事柄であり、いま、とても懐かしく感じるものである。そして、自治体のサーバーの設置管理を民間業者に任せることも、昭和の時代から行なわれてきたのである。その民間業者の役員または従業員の中には、外国人も含まれていたかも知れない。彼らはアクセスしようとすればいつでもわれわれの自治体の住民データに容易にアクセスすることができたであろう。彼らは技術

者だから、いかにロギングや監査やアクセス制御の仕組みを具備したとしても、それらは結局彼らが設置するものであり、自ら解除あるいは回避することができるというリスクがあった。このような議論は長年自治体庁舎内で優秀な職員たちとの間で秋の夜長に延々と行なわれてきたのである。そしてわれわれが当時達した結論は、次のとおりであった。民間事業者との間には NDA (機密保持契約) があり、また、そもそものサーバー運営管理の契約上の債務としても当然に、彼らはメンテナンス目的以外の理由で、データにアクセスしたり、さらには、これを第三者にコピーして提供したりするというようなことは無い程度に、人的にも、法的にも、信頼関係が存在している。単に業者に外国人が含まれているというだけでは、個人情報の漏えいの危険が具体的に存在するということは言えないから、違憲リスクはない、という結論だった。このような過去の議論を、今ようやく、思い出したのである。なるほど君の言うとおり、確かに、従来型システムを民間データセンタに委ね、物理的な分離対策を施した上で、民間人に管理を委ねる場合と比較して、ガバメント用クラウドを利用して論理的な分離対策を施した上で、米国系パブリッククラウド事業者の外国人を含む取締役や従業員に管理を委ねる場合は、論理的にみて、大きな違いはなく、違憲リスクはなさそうである。この点まで理解を進めることができたことについて感謝をする。」

行政デジタル人材 Y 「管理職の方に、最新の技術に関する理解をしていただいて良かったと思う。」

行政管理職 X 「ところで君は先ほどから分離、分離というが、ちょっと従来手法とガバメント用クラウドの手法の本質を比較してみよう。民間データセンタ内の行政システムにおけるラック隔壁の、または少なくともサーバー隔壁の分離というものを取り上げて、いまいちどその分離の性質について考えるとしたら、その分離の本質は、物権的分離か、債権的分離か、いずれだろうか。」

行政デジタル人材 Y 「物権的分離である。」

行政管理職 X 「なるほど、物権的分離というものは、何に依存しているのか。」

行政デジタル人材 Y 「物理法則である。根本原理としては、時空間の構造、マクロには、分子間力とか、剛体の性質とか、物質材料の性質というような様々な法

則である。より常識的には、固体金属で作られた板によって囲まれた領域は、他の物体を通過させることがない確率が極めて高いという現象である。」

行政管理職 X 「物理法則は、安全であるか。変化することはないのか。」

行政デジタル人材 Y 「物理法則は、宇宙創成時間もない時においては、ミクロなレベルで次々に変化し、現代のマクロ系が形成されたと考えられるが、その後の約 138 億年以上は、変化していないと考えられる。少なくとも、国会の決議とか、外国関係とか、技術企業の意思といった、人の意思によって、変化することは決してない。」

行政管理職 X 「物理法則の根本的原理が時空間の構造によるものとして、それは何によって支持されているのか。」

行政デジタル人材 Y 「数学法則であると考えられる。しかし、これについては争いがある。数学法則というものが物理法則と独立して存在し得るかいう問題が存在するのである。」

行政管理職 X 「数学法則は、安全であるか。ことごとく変化してしまうことはないのか。」

行政デジタル人材 Y 「数学法則が変化するリスクがあるかどうかは、争いがある。しかし、その前に、そもそも物理法則が数学法則に沿って動作することの論理的証明が、実はなされていないという問題が、存在する。なぜ物理法則がほとんど数学法則に沿って動作するのか、その理由が不明であり安心できないというものである。一説には、数学法則と物理的法則との間の確実な連結が担保される法的保証 (注: ここでいう法とは、人定法的な法でなく、自然法的な法のことである。) は存在しないというものがある。そして、人間原理により、数学法則による予測可能性がかなりの精度で担保された物理法則に従う物理世界の実装上においてのみ、われわれのような知性が発生しないか、すくなくとも、このような高度複雑な理論を述べた行政文書を記述し始めることはないという説がある。この説は、数学法則と物理法則は互いに関係になく存在し、それらが偶然一致する物理現象空間においてのみ生命が発達するというものである。その結果、生命が知性に発展し、たとえば、この行政文書に示される難儀な文章的代物がその中で生成されたということになる。」

行政管理職 X 「君は、この行政文書に示される難儀な文章的代物といったが、それは一体何か。」

行政デジタル人材 Y 「今まさにわれわれの議論の会話で先ほどから互いの口から語られる言葉があらかじめ記載されているこの PDF または印刷済用紙としての行政文書のことである。」

行政管理職 X 「われわれは、実在する 2 人の人間であって、自由意思に基づいて先程から自由な会話を行なっているのであり、われわれの会話に対して何らかの文書が先に存在して内容が確定されている訳ではないと思う。」

行政デジタル人材 Y「いや、直接的にわれわれ 2 人の目には見えないのだが、われわれの思考と議論は先ほど言及した行政文書に文字として確かに先に記録されているのである。」

行政管理職 X 「われわれは、その事実を、確認、検証することはできるか。」

行政デジタル人材 Y「できない。それは、この仮想的区間の外部の事象である。ある法則に基づいて動作している時空間上の現象があるとして、その現象において振る舞う主体が、その時空間システムそのものの構成原因となっているより基盤的実装をのぞき見て、それを観測することは理論上不可能であると考えられるのである。このような概念は、まさに、パブリッククラウド事業者の提供する仮想基盤の VM のゲスト OS 内のみの利用を許容されたユーザーが、その仮想基盤そのものの実装の模様やその安全性を確認、検証することはできないという、ガバメント用クラウドに関するセキュリティ担保に関する重要な議論に結びつくのである。」

行政管理職 X 「なるほど。そのような比喩によってようやく仮想化の本質が理解できてきたので大いに感謝をする次第である。クラウドシステムにおける仮想マシン (VM) とその基盤システムとの関係およびわれわれが注意深く観察し評価しなければならないそれらのセキュリティの堅牢性に関する重要性を理解することができた。ところで、仮にそうであっても、この口頭での議論が自由意思に基づくものでなく、あらかじめ行政文書に記載されているとおりに発話されているという事実の存在はね認めがたい。私は、それには憤慨を感じるのである。」

行政デジタル人材 Y「それを確認する手段は存在しない。VM の内側から、VM

そのものを観察することはできないし、その安全性も、セキュリティも、検証することはできない。今われわれの口頭から出るこの文言があらかじめ記載されているこの文書の著者の思想や合理性について、それらが一応健全であり、危険なものではないかどうかは、その仮想空間の内側に存在する過ぎない我々は、どう逆立ちしても、検証することは、できないのである。」

行政管理職 X 「仮に我々の口頭での議論が仮想空間上にのみ存在していて、その仮想空間の実体を作り出している主体がエミュレーションしているとしたならば、我々 2 人が独立した意思を持っていて議論を重ねているとしても、外形的に次々に表現されてゆく議論の内容だけでなく、我々 2 人の内面の精神構造までも、その仮想空間の実体を作り出している主体によって、いつでも観察され、読み取られ、場合によっては改竄(ざん)されることも、あり得るのだろうか。」

行政デジタル人材 Y 「それはあり得るし、システムの中にいる我々 2 人がそのことを事前にも事後にも通知を受けることは、決してない。だから、我々は決してそのことに気が付かないと考えられる。ユーザーは、仮想空間の中に一度追いやられてしまったならば、その仮想空間システムを繰り出す特権的基盤システムの実装主体により 100% 支配管理された状態になるのである。他人の作ったクラウドシステムを重要で秘匿性の高い目的で利用しようとすることの、最大のリスクは、ここにある。」

行政管理職 X 「君のいう危険はまったくそのとおりだが、君がその見解を主張するというのはなかなか驚くべきことである。君は米国系パブリッククラウド事業者の利用をいわば強引に推進する立場のように見えたのだが、そうであれば、米国系パブリッククラウド事業者を利用することは、仮想空間システムを作り出している実体を信頼する必要があるが、その信頼は確認することができないという理論からは、米国系パブリッククラウド事業者の利用に対して否定的な結論に傾くことになるはずである。君はこの矛盾をどのように説明するのか。」

行政デジタル人材 Y 「それについては、私は、仮に、行政的には、米国系パブリッククラウド事業者を完全に信頼することができないとしても、個人的には、彼らに日本国中のさまざまな国民資源を注入して彼らの巨大化を図ることは、公益に

資すると考えるのである。だが、この議論は個人的見解なので、われわれの公的な意思決定には援用できない。さて、話が脱線したので、元に戻すべきである。とにかく、これまでの実験観測上、物理法則は数学的法則の派生物であるか、あるいは、それが設計上の法的構造であるかあるいは人間原理に基づく事実状態であるかは別として、少なくとも現に十分堅牢な連結を有しており、それは 138 億年くらいの長い間は信頼できたから、これからも信頼できると、本日の時点では、一応、仮定するのである。」

行政管理職 X 「だが、別の可能性として、数学法則よりも物理法則が先に存在し、物理法則中に組み込まれている事実的現象の 1 つが数学法則であると考えることはできないのか。」

行政デジタル人材 Y 「まさにその点でも争いがあると思われる。先ほどの時空間の構造が形成された際にその形成の結果として数学法則が形成された可能性はもちろんあるが、むしろ数学法則が先に存在していて、それを元に物理法則を演じる現象世界が形成されたという可能性もあり、いずれが正しいのかは、分からない。」

行政管理職 X 「数学法則と物理法則の先後関係が問題となるとして、そもそも『先後』という言葉を用いるには、物理法則の一部として存在するはずの時空の概念における時間というシステムが形成されていなければならないから、先後という概念をここで持ち出すとしたら、物理法則のほうが先に形成されたという必要があり、そうでなければ論理的矛盾に陥るのではないか。」

行政デジタル人材 Y 「いや、そうとは限らないのである。あなたは今、『論理的矛盾』といったが、まさにその『論理的矛盾』について議論する際には、少なくとも、『論理的』操作が必要である。今ここで論理操作について考えてみると、それには、『正しい』と『誤り』ということを示す情報としての 0 か 1 かを示す『ビット』が存在する必要があり、このビットに対して、1 ビット入力操作としての NOT、2 ビット入力操作としての AND および OR が必要である。これらが合わさって XOR が形成されるといえる。だが、これについても争いがある。XOR 操作だけが先に存在していて、XOR を組み合わせて AND、OR および NOT が形

成されたという説も存在し得る。いずれにせよ、こういうビット処理が取扱い可能になって初めて、論理が可能になり、矛盾の指摘が可能になる。ビット処理は数学法則のうちかなり根幹の部分であるブール代数的処理である。そうすると、物理法則と数学法則のいずれが先かの論理を持ち出すには少なくとも数学法則が先に存在していければならないといえるのである。」

行政管理職 X 「それは、数学法則というハードウェア上に、論理法則というソフトウェアが形成されているのか、あるいはその逆か、という問題がある、という意味で合っているか。」

行政デジタル人材 Y 「細部には注意が必要だが、だいたいその理解であっている。パブリッククラウド的技術表現でいうと、一方がバーチャルマシン (ただし Intel VT のようなハードウェア仮想化技術を活用した VM ではなく、QEMU の完全仮想化モードにおける CPU エミュレーションにより実装されている VM) のホスト側ソフトウェアであり、もう一方がゲスト側ソフトウェアであり、どちらがホストで、どちらがゲストかという問題である。」

行政管理職 X 「数学法則と物理法則が両方同時に形成されたとか、むしろそれらは単に同一の実在の側面を異なる形式で表現したものに過ぎないということも可能か。」

行政デジタル人材 Y 「その理論は、もちろん成り立たせることは可能で、誠に創造的なものである。だが、それを仮定すると、通常は、職業上、厄介な問題が生じてしまうのである。すなわち、A というシステムの基盤が B というシステムである (B の上に A が乗っている) というように考えたならば、A というシステムの責任者としては、B というシステムが A というシステムに前置して存在し、それが一見短期間でも安全で安定しているという事実を示すことで、通常程度の議論能力を有する人からの安全性の指摘に対しては、A というシステムの安全性を、B というシステムの安全性を暗黙的に仮定することにより、示すことができるのである。A と B との間で責任分界点が存在し、異なる 2 個の管理主体が A と B を管理している構造にすれば、そのような一見安全であるという言い逃れを行ないたい A の管理責任者にとっては、なお、好都合である。B の安全性は B のほうの

問題であり、A としては知らん、というように言えるためである。A からみて B の安全性は契約によって担保されていればよいという考え方である。まあだいたいは、実のところ、ガバメント用クラウドにおける米国系パブリッククラウド事業者の利用の動機は、このような心理状態を実現したいというなかなか魅力的な方向性に牽引される力に支持されて形成されてきたものである。その最大の利点は、『説明がスムーズにできる』、というものである。だが、B の側に脆弱性が存在するが、これは A から検証不能となってしまうという、システムの本質上の問題は解決されていない。しかし、A の担当者としては、本質的問題よりも、職業上の安全性のほうが重要である。少し脱線するが、実は A が B の安全性に懐疑を生じさせる否定的情報を得ていて、B のリスクを認識・容認している場合、A の責任者のほうの職業上の安全性は損なわれるのである。この場合、A は、責任分界点の向こう側である B との間の契約関係の存在により、B の安全性を盲信していることはできない状態に追いやられてしまう。この理論において、われわれ行政機関のユーザーシステムが A、われわれがこれからみていく米国系パブリッククラウド事業者のクラウド基盤システムが B である。さて、ガバメント用クラウドの話はすこし置いておくことにしよう。われわれの先ほどの議論は、より根本的な、物理世界と数学世界に関する話であった (ガバメント用クラウドというものは所詮はその物理世界ないし数学世界の空間の内側に存在するものであった)。今 A に前置して安定した B が存在するという主張をするとき、数学法則と物理法則の片方が A、もう片方が B に当てはまると説明すれば、A または B のいずれかしか取り扱わない学者の視点では、まことに『説明がスムーズにできる』のである。そして、実は、1 人の学者においても、ある時は自らの領域が A である (仮想空間内のユーザーシステムである) と主張し、別の時には自らの領域が B である (仮想空間を作り出す基礎システムである) と主張するように、絶えず揺れ動く心理現象が、みられるのである。自らの学問領域の基礎の安定性を指摘されそうになったら、前者の主張をすればよい。自らの学問領域をより一層権威付け、その重要性を強調し、聴衆を感嘆させたくなったら、また、予算が欲しくなったら、後者の主張をすればよい。だが、こういう、一面しか見えない学者は、『A と B が同時に形成されたはずだ』という驚くべき理論を

繰り出すことはとてもできないのである。結局のところその学者は 1 つの専門領域面についてしか十分に理解しておらず、その点が露呈してしまうからである。」

行政管理職 X 「またしても君の説明は長いが、おかげでクラウドシステムの構造とリスクについての理解が進んだ気がする。ところでなぜこうも話が脱線するのか。」

行政デジタル人材 Y 「それはあなたが色々と質問をするからである。」

行政管理職 X 「私は、管理職であり、忙しい。ここは行政機関であるから、質問に対しては、自らの職分の責任範囲内でのみ、3 行くらいで完結に答えればよろしい。」

行政デジタル人材 Y 「いや、決してそういう安易な風にはいくまい。さまざまな物事には、ある問題に関連して、ある職業的領域を包含する責任分界線を越えて、その奥深くに別の問題が関連しており、それはどんどんと連なっていき、長い視点でみると、循環構造が見出されることもあるのである。このような全体的観察的視点をもたずに、その都度狭隘な職業領域の文脈のみに着目し、物事をひとまず解決したかのように取り繕ってしまうことこそが、現在の高度複雑化する社会における行政機関において、以前よりも効果的な結果を出すのに苦労する羽目になっている原因である。われわれの尊敬する米国の伝説的行政人材や、その他、たとえば、今活躍されているような米国系パブリッククラウド事業者の優秀な少数人数の仮想化技術基盤を熟知したプログラマやその経営者たちは、狭隘な単一職業領域における責任分界線の内側のみの思考にとどまることなく、その線を越えた自由な思考を再現なく辿って踏み込んでいくことにより、現代の強いアメリカ合衆国の銀盤的な基盤と、コンピュータやインターネット、AI 等の技術基盤を、次々に、米国内に形成させることに成功しているのである。このような歴史的事実を考えると、日本の最大の人材母体である行政機関においても、まさに、我々が尊敬する米国の伝説的行政人材や、現代の米国系パブリッククラウド事業者の人材たちの有する思考の特性と同様に、特定の領域に留まらず、全体を俯瞰的に闊歩していき、複雑で相互の依存関係が強い鎖鬚（さしゅ）でメッシュ状に連なっている複数のばね問題を、全体的、同時的に解決してゆくことを、通常の行動ルーチンとして、習慣付ける必要があるの

である。そのためには、もちろん、長年時間がかかると考えられるが、少なくとも、その正しい道のりの入口において歩み始めることを開始しなければ、決して、到達は不可能である。このように考えるとき、あなたの言う、『ここは行政機関であるから、質問に対しては、自らの職分の責任範囲内でのみ、3 行くらいで完結に答えればよろしい。』という指導は、あたかも、これから始まる長い日本の進化発展の、いうなれば、未開拓の関東平野の荒野における入口付近にある安全門を出たあたりで、3 里 (里とは、約 4㎞ のことである。) くらい歩いては、また恐くなって戻ってくるというような行動をとるべきであるということを、示しているということになるのである。それは、よくないことである。そのような 3 里的考え方が原因で、われわれ日本は、ついに、現代世界における人材不足と、国際競争力の低下を招いてしまっているのである。これを解決するためには、これからは、どのような問題についても、連続的にかつ遠方まで分け入って考える習性を、今、いよいよ身に付けなければならない時節に、ついに、差し掛かっているのである。」

行政管理職 X 「それはそうだが、もう少しポイントにまとめ、圧縮することはできないのか。物事は、何でもシンプルに解決できるはずだ。」

行政デジタル人材 Y 「それには、限度がある。荘子にもいうように、普通の人にとっては日々わずかな時間をかけて食事を用意すればよいが、これから千里の旅をする人にとっては、三ヶ月くらいは、食料の用意に時間をかける必要があるのである[①]。コンピュータを活用して問題を解決するということは、千里の旅に出るようなものであるから、多くの物事を理解しなければならない。多くの物事は、複雑な構造を伴って生じるものであるが、それの法則を見てシステム的に整理できることは事実であるとして、その整理と圧縮の程度には、限界が存在するのである。また、理論上の限界に加えて、その情報の受領者である側も、物理現象に基づいて動作する人間の頭脳であることから、受領側がその頭脳の稼働速度の範囲内で理解することができる表現形態に対象となる物事を変形させて保存する場合において、その結果としての文字および図の量はどうしても冗長にならざるを得ないのである。

[①] 荘子 (内篇) 逍遥遊篇

アリストテレスによると、その冗長さの度合いは、ある物事に対して、適量が存在し、過度に圧縮し過ぎても、冗長にし過ぎても良くないというのである。その結果形成された文字情報の集合体が、書籍や論文というものであり、これまで、不要なものを捨て、重複を排除し、現在の世の中の物事を理解できる程度に減縮させても、すくなくとも巨大なコンクリート構造物に支持される図書館に収めようにも収まりきれない分量になっている。これは人間があえてみだりに複雑な構造を作り出しているというのではなく、そもそも社会上必要となる学問的物事の本質が、もともと、複雑な構造をしているためである。人類社会が発展し、さまざまな技術や社会制度が形成されるにつれ、知識という氷山の水面下からいよいよ解氷されて出てくるものの複雑さの度合いは、次々に高まっていくのである。それを複雑なものとして、そしてまた、決して限界を超えてシンプル化することができない性質のものとして、いったんはありのままに受容した上で、それを統合的に社会の現実的問題解決のために利用する行為こそが、現代行政活動の本質である。あなたのいう、ポイントにまとめて圧縮せよというのは、人類の知見の詰まっている図書館の膨大な学術書群をシンプルにして数冊にまとめることができるはずだという主張と同義である。そのようなポイントにまとめた圧縮を強制するという行政的風味を生み出そうとするあなたの主張は、行政の本質的活動能力をいたずらに阻害するおそれがある。」

行政管理職 X 「それでは、言葉や文字ではなく、代わりに、図やパワーポイントを用いて、わかりやすく、短縮することはできないのか。」

行政デジタル人材 Y 「あなたのいう、図やパワーポイントを用いて短縮するというアイデアが仮に正しければ、前述のような、人類の知見の詰まっている図書館の膨大な文字を中心とする学術書群を、図やパワーポイントを用いれば、かなり圧縮できるという考え方である。それには無理があると考えられる。複雑な情報は、今のところ、文書にシリアライズするしか方法がない場合が多い。それに、複雑な概念は、その表現に一定の精密さが必要であり、その精密さを維持する範囲における適切な圧縮率は、すでに文章が記される時点で、限界近くまで、行なわれているのである。それに対してさらに時間をかけたとしても、圧縮率は対数的にしか増加

しないであろう。」

行政管理職 X 「そうであったとしても、人間が取り得るかなり高度な知性と、行政分野において用いられるべき知性とは、異なるのではないか。行政に必要な知性レベルは低く抑え、言葉や文字ではなく、図やパワーポイントを用いて短縮する程度の水準で処理できたほうがスムーズではないだろうか。」

行政デジタル人材 Y 「まさにその考え方が、近年の日本の行政における問題解決を、また、より広くいうと、日本におけるさまざまな組織における問題解決をも、阻んでいるのである。人材不足、国際競争力の低下などといった問題の原因は、まさに、あなたのいうその単純化の考え方によるものである。いまここで、行政について考えると、確かに、夜警国家的な最小限の行政を目指すのであれば、あなたのいう通りかも知れない。しかし、日本の主権者は、20 世紀以降は、夜警国家ではなく、豊富な活動機能を担う行政を実現するようにわれわれに命じてきたのである。豊富な活動を行なう行政は、当然、巨大な高コスト行政となる。その支払われる行政コストのうち人件費は、行政に集まってくる高度な人材の知性に対する使用料金である。人件費以外のコストは、その高度な活動において必要となる外部調達物品や役務の使用料である。日本の主権者はそのように考えてわれわれ行政に対して多額のお金を毎月支払ってくれている。行政というものは、社会において高度で複雑な難儀な他で解決困難な問題が次々にしわ寄せされてくるときに、これを現実的コストの範囲内で法定の範囲内で解決することが期待されている機関である。それとの引換え対価として、主権者は、多額の税金を行政に寄託してくれているのである。したがって、われわれのような高コスト行政においては、行政に集まっている人たちは、何よりもまず、学問を盛んにして、国内において最も高い水準の知性を形成維持し、次に、それを活用して、寄せられる高度な問題を現実的コストの範囲内で最大限に解決しなければならない。それができないのであれば、高コスト行政の存在理由が失われるのである。あなたのいう、行政に必要な知性レベルは低く抑え、言葉や文字ではなく、図やパワーポイントを用いて短縮する程度の水準で処理できたほうがスムーズであるという考え方では、現在の大きな行政機構の存在意義を維持することは、到底、困難となってしまう。行政に必要な学問レベルを低下

させ、図やパワーポイントを用いて短縮する程度の水準にしたならば、行政は、最小限の機能しか実現できなくなる。それは現在の日本の方針に反している。」

行政管理職 X「それは確かにそのとおりだ。それに、昔をよくよく思い出すと、日本の行政においては、最も高度複雑な物事を理解できる人材が揃っていたはずだ。ところが、特に、最近の行政に集まってくるコンピュータ関連領域の人材のレベルが、なぜ、今、それなりの水準に留まるのか、これは、大きな謎であった。だが、今ようやくその原因発見の糸口がつかめたかも知れないという、大いなる希望が再び灯火を回復し始めたのである。すなわち、コンピュータ関連領域の行政人材においては、パワーポイントを用いて議論を短絡化するというアイデアが普遍的に流行していることが、その原因かも知れない。パワーポイントというのはコンピュータのソフトウェアであるから、コンピュータを使いこなす人々がパワーポイント文化に真っ先に偏向してしまうということも、うなずける話である。このようにして、組織的思考能力の低下は、行政に入ってくるコンピュータ領域人材の行動習性によって、ますます拍車がかかっている可能性がある。この問題を解決するためには、やはり、伝統的な文書に基づく行政、学問的知識に基づく行政を、復活させる必要がありそうだ。コンピュータ関連領域の行政人材こそ、それを率先してやるべきだ。」

行政デジタル人材 Y 「全くその通りだ。さて、そろそろ、話を元に戻すべきである。脱線前のもともとの議論は何であったか。」

行政管理職 X 「行政のコンピュータシステムのサーバーコンピュータが、従来型の庁舎やデータセンタに設置されている場合は、そこで取り扱われる情報が物権的に他者と分離されているという話だったはずだ。そして、その分離は物理法則によって実現されており、物理法則は安定していて、138 億年くらい変化していない、というようなえらく高尚な話題だったはずだ。」

行政デジタル人材 Y 「確か、そのような話だった。」

行政管理職 X 「そうであれば、行政のコンピュータシステムのサーバーコンピュータが、従来型の庁舎やデータセンタに設置されている場合、おおいに安心できるのである。138 億年という信頼は、じゅうぶんな長さである。われわれの行政

機関が今後数百億年も存続することは不可能だからである。」

行政デジタル人材 Y 「いや、その長さは物理法則の安定性を示すものであり、物理法則に基づいて成立している個々の物質、たとえばラック外壁やサーバー筐体の金属板などの物質が維持される長さを示すものではないことに、注意を要するのである。ところで、今あなたは、『われわれの行政機関が今後数百億年も存続することは不可能だ』と言ったが、その根拠は何か。」

行政管理職 X「われわれの行政機関の活動は、太陽に依存しているためである。そこで、太陽の寿命が問題となる。独立行政法人国立科学博物館の見解によって、太陽の寿命はおそらくあと 50 億年くらいと定められたのである[①]。」

行政デジタル人材 Y 「いや別に太陽の寿命が独立行政法人の発表によって定められたということはない。むしろ独立行政法人は太陽が生み出したものである。それに、われわれ行政機関の存続は、太陽以外にもさまざまなものに依存しているし、より早期の段階で太陽活動の変化が生じ行政機関の維持に影響が生じる可能性も高い。だが、われわれ人間社会と、それを支える行政機関は、いずれは、太陽活動に依存しない領域で延命することができる可能性もあると考えられる。そうすれば、われわれの行政機関が今後数百億年も存続することも、十分考えられるのである。よって、われわれの行政機関が今後数百億年も存続することは不可能だというあなたの見解には、誤りがある。」

行政管理職 X 「しかし、それを可能にするためには、人間社会は、遅くとも太陽寿命の期日が到来する日の前日までにおいて、地球外に退去し、活動の幅を、宇宙の空間上に対し、ますます広範囲化する必要があるのではないか。」

行政デジタル人材 Y 「その退去実施日は、前日ではなく、当日でも差し支えはないであろう。だが、それは大きな問題ではない。基本的にはあなたのいう通りである。地球外に安全に退去して活動を維持する必要がある。そして、そのためにはコンピュータ技術と AI 技術の発展が必要不可欠である。それらの発展がなければ、地球外に安全に退去して活動を維持するために必要な固定資産的装置群の組成

① https://www.kahaku.go.jp/exhibitions/vm/resource/tenmon/space/sun/sun02.html

や制御はほとんど不可能であるためである。」

行政管理職 X 「すると、コンピュータ技術と AI 技術の発展が、われわれの行政機関が地球を安全に退去し今後数百億年以上も存続することに対して必要不可欠であるということになるが、そのコンピュータ技術や AI 技術の発展は、どのようにして成されるのか。」

行政デジタル人材 Y 「近時は、米国系パブリッククラウド事業者のリソースを中心に成されている。たとえば、現代型の AI 技術には GPU と呼ばれる半導体を大量に並べて並列動作させる必要があるが、これらは、米国系パブリッククラウド事業者のデータセンタに立ち並ぶサーバー配列群上に分散配置されているのである。これらの米国系パブリッククラウド事業者のクラウド基盤を活用して生成型 AI 技術を大いに進化発展させたものが、たとえば、2022 年頃から注目を集めている、OpenAI 社の Chat-GPT である。」

行政管理職 X 「なるほど。そのような大規模 AI 技術を進化発展するために、米国系パブリッククラウド事業者の大規模リソースの存在とその拡大が人類史上重要な要素となることは分かった。しかし、そのことと、われわれ行政機関の米国系パブリッククラウド事業者の利用行為との間では、何らかの関係はあるのか。」

行政デジタル人材 Y「直接的な関係はないが、間接的には、大いに関係がある。人類の大規模 AI 技術を進化発展するためには、米国系パブリッククラウド事業者の大規模リソースが拡大する必要があり、そのため、人類のさまざまな部分の資源、すなわち一次的には金銭を、米国系パブリッククラウド事業者にどんどんと支払い、彼らが膨大な半導体投資を行なえるようにする必要がある。これを人類史的に観察すると、われわれ国民主権者は、日本の行政機関に米国系パブリッククラウド事業者に対してガバメント用クラウドとしての一括契約を行なわせ、その経路を用いて、国民の金銭資源を集中的に米国系パブリッククラウド事業者に対してコントリビュートし、よって、人類の大規模 AI 技術を進化発展することに大きく寄与しているということもできるのである。そして、AI 技術の発展は、先の議論でみられたように、われわれ行政機関が太陽寿命を越えて地球外に安全に退去して今後数百億年も存続するために必須の条件である。よって、米国系パブリッククラウド

事業者に国および地方自治体の多額のお金を集中させて支払い、これにより彼らにエネルギーを集中させることは、日本国内の複数のシステム事業者に分散的にお金を支払うよりも、われわれ行政機関の存続にとって、良い結果につながるのである。実は、私は行政技術者として、このような大局的観点により、米国系パブリッククラウド事業者を個人的に応援していて、その目的で、次々とさまざまなシステムをできるだけガバメント用クラウドに移行することを推進しているのである。」

行政管理職 X 「君のいう理論は、確かに因果のつながりがまったくないという訳ではないが、社会的に相当性を有する因果関係があるようには見えないし、むしろサイエンスフィクションのように聞こえるから、市民や議会を説得するために十分ではない。それにまた、君の述べた理論すなわち上に記載されている突飛で長大な文言は、常識的なものではなく、明らかに生成系 AI が生成した文面のような風味が感じられるのである。」

行政デジタル人材 Y 「確かにこのような議論を突き詰めると我々の人間的思考が実は生成系 AI の思考であるのか、我々も結局は生成系 AI と類似した思考パターンしか取り得ないのかという、存在意義にかかわる深淵な苦難が生じるのである。」

行政管理職 X 「確かにその苦悩が表面化するから、この話はやめにしよう。」

行政デジタル人材 Y 「やめにしよう。」

行政管理職 X 「それでちょっと話を元に戻す必要がある。今われわれは、従来手法とガバメント用クラウドの手法の本質を比較していたところであった。民間データセンタ内の行政システムにおける他のデータセンタ利用者との分離の本質は、物権的分離であるという結論であった。そこから 138 億年がどうであるというような議論が始まり、それがもとで、混乱が生じたのである。ただ今、われわれはようやく元の道に戻ってきたところである。さて、データセンタでの分離と比較して、君がいう、ガバメント用クラウド上での分離の本質は、物権的分離か、債権的分離か、どちらだろうか。」

行政デジタル人材 Y 「債権的分離である。」

行政管理職 X 「その債権的分離の確保は、何に依存しているのか。」

行政デジタル人材 Y 「これは、2 つのものに依存している。(i) 第一に、米国系パブリッククラウド事業者の取締役や従業員たちの中の少数の、クラウド上の VM 基盤等をプログラミングできる高度な能力を有するプログラマたちの腕である。(ii) 第二に、米国系パブリッククラウド事業者の取締役や従業員たちが、ガバメント用クラウド上のデータを、決して、意図的に他人に引き渡すことがないという信頼である。」

行政管理職 X 「それらは、従来型データセンタにおける物権的分離を担保している力、すなわち先ほど出てきた 138 億年云々というような安定した物理法則と同じくらい、安定していて、強力か。」

行政デジタル人材 Y 「いや、とても弱く、何かあるとすぐにでも崩壊しそうな力に過ぎない。」

行政管理職 X 「それでも、それらが崩壊する平均間隔が、われわれ行政機関のこれまでの平均存続間隔よりも長ければ良いというものであろう。」

行政デジタル人材 Y 「残念ながら、今のところ、それは全く期待できない。日本の行政機関のこれまでの平均存続間隔と比較して、米国系パブリッククラウド事業者の寿命は、かなり短いと考えられる。米国における、現代型パブリッククラウドの誕生は、2007 年頃であり、未だ 16 年しか経っていない。他方、われわれ行政機関は、少なくとも明治以降でみても、150 年以上の継続がある。現代型パブリッククラウド事業者の平均存続間隔は、われわれ行政機関の平均存続間隔のだいたい 10 分の 1 くらいに過ぎない。」

行政管理職 X 「われわれは、米国系パブリッククラウド事業者の取締役や従業員たちの中の少数の、クラウド上の VM 基盤等をプログラミングできる高度な能力を有するプログラマたちの技術力が、十分に高いことを証明しなければならない気がする。そうでなければ、米国系パブリッククラウド事業者において、われわれ行政機関の平均存続間隔と比較して極めて短い間隔で、分離機構が崩壊し、情報の漏えいが生じる事象が発生する現実的危険性があるといえることにはならないか。」

行政デジタル人材 Y 「それはそうかも知れないが、あなたは、その理論をいまここで持ち出すことはできない。なぜならば、先にあなたは、『われわれから検証

不能な部分であり、ここにセキュリティ上のリスクが存在し得る。』とした上で、『本日は、技術的能力の側面についての議論はひとまず留保する。』、と述べたからである。そして、米国系パブリッククラウド事業者の取締役や従業員たちの中の少数の、クラウド上の VM 基盤等をプログラミングできる高度な能力を有するプログラマたちの技術力を疑うべきか否かという点は、まさに技術的能力の側面についての議論であり、本日あなたはこれを取り上げないことに同意した。だから、今、この点をあなたがこれ以上追及することは、できないのである。」

行政管理職 X 「確かにそのとおりだ。そのセキュリティ問題については、別の機会に考察をする必要がある。」

行政デジタル人材 Y 「もう深夜になってしまったから、今日は帰ってよろしいか？」

行政管理職 X 「もちろん、よろしい。」

行政デジタル人材 Y 「それではもう帰宅しようと思う。実は、明日は土曜日であるが、私は、朝から登庁して、現行システムを休止させ、いよいよ、ガバメント用クラウド上に仮想マシンを立ち上げ、その仮想マシンに現行システムの民間データセンタ上にあるシステムの VM 上の仮想ディスクを移行しようと思っている。ところがどうやら VM 基盤が異なるので、仮想ディスクのイメージ形式が異なる。そこで、dd というツールを用いてディスクをイメージ化した上で、イメージファイルを直接送り込む作業を、3 人くらいで、行なうことを教案している。ただ、それはブートディスクも含むから、ガバメント用クラウド上の IaaS VM 上で起動するかどうか心配であるから、もう帰宅して休もうと思っている。その仮想マシンや仮想ディスクは、米国系パブリッククラウド事業者の単一のサーバー群において、複数のユーザーによって混在されて保管処理されるが、もちろん、先に述べたとおり、論理的に互いに分離されているのであるから、ガバメント用クラウドにシステムを移行した後も、同一の米国系パブリッククラウド事業者を利用する他のユーザー組織との間で、データが混合するリスクを考えることなく、枕を高くして、眠ることができるのである。」

行政管理職 X 「ちょっと待たれよ。明日、ついに、ガバメント用クラウドに、

システム移行を行ない、これにより、住民の個人情報を米国系パブリッククラウド事業者のクラウド上で保存・管理する行政活動を、現実に、開始するというのか。」

行政デジタル人材 Y 「そうだ。」

行政管理職 X 「先ほど、議論の途中で脱線する前に出ていた、住基ネット事件最高裁判例に係る合憲性の問題については、すでに十分検討を済ませているのか。」

行政デジタル人材 Y 「その問題の議論は、さきほど済ませたはずだ。ガバメント用クラウドにおけるわれわれ自治体の専用クラウド領域は、論理的に他のユーザーと隔離され、国からも、県からも、他の自治体からもアクセスできないようになっている。もちろん、無関係の他人からも、すなわち、世界中のいずれの第三者からも、アクセスできないようになっている。データにアクセスできるのは、米国系パブリッククラウド事業者の取締役や従業員等のうち、メンテナンス行為のために必要がある技術者たちだけである。これは、従来型システムで民間データセンタにサーバーを置き、これの管理を民間業者の取締役や従業員等に委ねた場合と等価であり、本質的に新たな脅威は存在していない。こういう議論だったはずだ。」

行政管理職 X 「確かに、そこまでは議論が完了していて、問題はなさそうだということになった。しかし、今ひとつ心配事がある。」

行政デジタル人材 Y 「その心配事とは、一体は何であるか。」

行政管理職 X 「ヨーロッパの先進国で最近おおいに問題となっている、米国クラウド法 (CLOUD Act: Clarifying Lawful Overseas Use of Data Act) と呼ばれる、2018 年 3 月 23 日に米国で成立した米国国内法の問題である。」

行政デジタル人材 Y 「なぜ米国クラウド法がそこまで問題なのか。」

行政管理職 X 「先に君は、ガバメント用クラウドにおけるわれわれ自治体の専用領域に置いたデータには、われわれ自治体自身と、米国系パブリッククラウド事業者の取締役および従業員によるメンテナンス行為以外では、決して誰もアクセスできないと言った。ところが、米国クラウド法の第 18 編 121 章 2703 条によると、米国連邦政府または米国州政府は、いつでも、われわれ自治体のクラウド領域内に保存されている、われわれの市民の個人情報にアクセスできることになる。ガバメント用クラウドに移行する予定の、税務記録、健康保険記録、生活保護情報、

就学情報、障害者情報、健康管理情報、失業保険情報、図書館貸出履歴、等の個人の内面に関わるような機微な個人情報を処理・管理するシステムのデータ領域に、アクセスできることになる。米国連邦政府または米国州政府は、第三者である。そうすると、住基ネット事件最高裁判例基準の (3) に抵触し、個人情報が第三者に漏えいする具体的危険が生じることになる。」

行政デジタル人材 Y 「あなたは、米国クラウド法に基づいて、米国連邦政府または米国州政府が、われわれの自治体の住民に関する情報を取得する現実的可能性が存在し、それが脅威であると考えるのか。」

行政管理職 X 「いや、そうではない。私は、個人的には、米国連邦政府または米国州政府を信頼している。しかし、われわれが懸念しなければならないのは、米国連邦政府または米国州政府によるそのようなデータ取得行動の有無とは全く別の問題として、いつでもその可能性がある米国系パブリッククラウド事業者のサーバーに住民のプライバシー情報を保存するという行為について、われわれの住民や議員の方々から、住基ネット事件最高裁判例に照らし、憲法違反であると指摘され、場合によっては、訴えられる可能性がある点にある。そして、この問題は、個人情報の問題と、日米関係の問題という、2 つのセンシティブな問題が同時に重なっている問題であり、稀にみる大きな問題に発展し得るのである。大きな問題として過度にこの問題が世間で取り上げられたならば、ガバメント用クラウドへのスムーズな移行と、行政のデジタル化の進捗が、妨げられる危険が大きくなる。そういった事態に陥らないようにするためには、あらかじめ、合憲性を検討しておく必要があるし、指摘をされた場合には、間もなく、合理的で抜けのない返答を用意しておかなければならない。」

行政デジタル人材 Y 「なるほど。その心配は確かにあるが、これまで他の自治体でガバメント用クラウドに関連してそのような合憲訴訟が発生していないことからみて、心配する必要はないのではないか。」

行政管理職 X 「これまで市町村におけるガバメント用クラウド利用に関連して、米国クラウド法によって権利が侵害されるリスクを排除するために、市民が自治体によるガバメント用クラウド利用を違憲として提訴していない理由は、簡単であ

る。日本の裁判所は、具体的違憲審査制を採用しているので、具体的な争訟原因がなければ、違憲の訴えをすることはできない。すなわち、ガバメント用クラウドに未だ住民のデータが保存されていない限り、住民は、訴訟をすることはできないのである。」

行政デジタル人材 Y 「それは厳密には正確ではない。未だ住民データがアップロードされていなくても、アップロードされる具体的予定が存在すれば、妨害予防請求権によって、提訴されるリスクがあるのではないか。」

行政管理職 X 「それはそのとおりかも知れない。妨害予防請求権については、また後で議論することにしよう。だが、未だこの合憲問題に係る議論が世間ではほとんど発生していない理由は、もう 1 つある。実はこちらのほうがより本質的原因なのだが、日本では、市民も、議員も、また、マスメディアも、米国クラウド法の問題の重大性に気付いていないのである。」

行政デジタル人材 Y 「他国の状況はどうか。」

行政管理職 X「日本以外の先進国では、これはすでに大きな問題となっている。ヨーロッパ先進各国ではこの問題は GDPR との関係で重要視され①、ヨーロッパの行政組織は、米国系パブリッククラウド事業者への依存をやめる方向で動き出している②。たとえば、ドイツの経済エネルギー大臣も③、EU 委員会の委員長までも④、その方向性を公言している。中国は、もともと米国に依存する気はなさそうだから、自国内でクラウド技術を生み出していて、問題を解決できそうである。ロシアは、そもそも、経済制裁により、米国系パブリッククラウド事業者を利用しづらいから、問題はない。このような訳で、問題に全然気付いていないのは、日本くらいのものである。」

行政デジタル人材 Y 「日本において、未だ国民、議員、マスメディアがこの問

① https://policyreview.info/articles/analysis/mitigating-risk-us-surveillance-public-sector-services-cloud
② https://www.enisa.europa.eu/publications/cybersecurity-research-directions-for-the-eu2019s-digital-strategic-autonomy/
③ https://www.zdnet.com/article/eu-turns-from-american-public-clouds-to-nextcloud-private-clouds/
④ https://www2.deloitte.com/xe/en/insights/technology-management/cloud-sovereignty-three-imperatives-for-the-european-public-sector.html

題に気付いていないのであれば、それらの問題が起き上がって大規模に討論が開始される前に、そそくさと、ガバメント用クラウドへの移行を全部済ませてしまえば、一度完了したものを戻すことは困難であるというような事実状態の尊重の理論で、問題を回避できるのではないか。」

行政管理職 X 「実のところ、国はそのような考え方で、問題が大きく生じる前に、いちはやくガバメント用クラウドへの完全移行を完了させたいと考えてきたようだ。これは、われわれ自治体にとっては、確かに、追い風である。だが、その戦略では、3 つの問題が発生してしまう。第一に、ガバメント用クラウドへのデータ移行が完了した状態でシステムを運用していたところ、市民の 1 人が、米国クラウド法の存在を原因として、市を訴えたとしよう。その結果、日本において住民の提訴により違憲判決が出たとする。判決に従い、その住民のデータだけ、安全な方法で、米国クラウド法の影響から隔離して処理するには、膨大なコストが発生するのである。」

行政デジタル人材 Y 「なるほど。確かに、勝訴した住民だけを特別扱いしてデータを分けると、それだけで膨大なコストがかかるのか。」

行政管理職 X 「そのとおりだ。そこで、第一のコストを下げるために、もうすべてのシステムをオンプレミスに戻すとか、米国系パブリッククラウド事業者以外のクラウドに戻すというようなことを行なう必要が生じる可能性が高い。だが、それは急な話なので、対応するのに時間とコストがかかるのである。これが、第二の問題である。われわれ自治体における IT 人材の育成は十分うまくいっているとはいえず、むしろ 2030 年を目指してどんどんと IT 技術に関する基本的知識と能力を有する人材は減少しつつある。これに対する対策として、ガバメント用クラウドの利用が促進されているのだが、そうすると、ますます能力が低下するという、悪循環に陥っているのである。最近の自治体 IT 人材のレベルは、自庁舎内にサーバーを自ら立てることすらできない不健康状態であると聞く。これが、重大な経営問題として、日本のほとんどの自治体をこれから悩ませる問題として普及するのである。これは、あたかも歩くと筋肉痛になるから、それを避けるためにずっと寝ていると、足腰が弱っていき、ついには、寝たきりになり、ますます足腰が弱り、つ

いには自力で歩行困難となる、という具合である。そういう時に、憲法問題が生じたから急に米国系パブリッククラウド事業者の利用を止めよというように言われると、問題を是正するために、莫大なコストが発生することが予想されるのである。」

行政デジタル人材 Y 「なるほど。しかし、市町村ごとに、市町村を訴える住民が発生するか否かは、確率論の問題だと思う。たとえば、われわれの市はたとえば今後 10 年以内に 10% の確率で訴えられるとする。その場合にシステムを急いで是正するコストは 5 億円とする。その場合は、われわれの市は、それを払えば良いのではないか。何とか支払えるであろう。そして、90% の確率では、訴えられない。期待値を考えると、この場合、発生する損害の期待値は、5 億円 × 10% = 5,000 万円くらいである。」

行政管理職 X 「君は、住民訴訟制度を知っているか。」

行政デジタル人材 Y 「知っている。地方公共団体の首長や職員の違法または不当な行為または怠る事実に基づく地方公共団体の損害を、その首長や職員に賠償させる制度である。」

行政管理職 X 「住民訴訟制度を用いて訴訟をしてきた住民が、われわれ 2 人に対して、ガバメント用クラウドに住民情報を保存することについて、米国クラウド法を原因とする違憲リスクがあると認識・容認していたにもかかわらず、適切な処置を怠った結果、その後に違憲判決が出たことによりシステムを急に是正するための追加コストとして 5 億円の支出が必要となったということを証明したら、われわれ 2 人の判断に重大な過失があったとして、5 億円が請求されることになる。これは、われわれ 2 人にとって、個人的に、とても危険ではないか。」

行政デジタル人材 Y「確かに危険である。確かにその可能性が存在する。だが、ガバメント用クラウドを通じて米国系パブリッククラウド事業者を使用することを指示してきたのは、国の側だから、仮に違憲問題が発生したら、国が責任をとってくれるのではないか。」

行政管理職 X 「いや、国としてはそのような "指示" は一切していないと否認するに違いない。国は、地方自治の本旨に基づき、あくまでもガバメント用クラウ

ドを利用することを選択肢の 1 つとして提示したのであり、意思決定はあくまで地方公共団体の側の問題だと言うだろう。」

行政デジタル人材 Y 「しかし、国のほうでも国の事務にガバメント用クラウドを利用するわけで、その際に国のシステムにも国民の情報が大量に格納される場合もあるから、国の職員がガバメント用クラウドの利用を決定したことについて、後で損害が発生したならば、地方公共団体におけるわれわれ 2 名と同じような立場で、その責任者である職員や閣僚が重過失として責任を負わされるリスクもあるのではないか。そう考えると、国としてもガバメント用クラウドの利用にはかなり慎重になるということが予想されるのではないか。」

行政管理職 X 「このことについて、大変興味深いのは、地方公共団体では住民訴訟制度が整備されているが、国のほうではそのような制度がないという点である。国家賠償法では、一応は、国は、損害の原因となった行為 (重過失としての誤った判断) を行なった職員や閣僚に対して求償することができるとされているが、その求償をするか否かは、あくまでも国が決定できる。国民には、その請求をするよう訴える権利がない。だが、これと比較して、地方公共団体については、住民は、その請求をするよう訴える権利がある。これは大きな違いである。このことにより、基本的に、国の閣僚や職員は思いきった判断がしやすくなる傾向がある一方で、地方公共団体の首長や職員は慎重な判断をしようとする傾向がある。国と地方との間の温度差は、実は、このような点から生じるのである。国は、滅多なことでは公務員個人に求償できないのである。このことは、地方公務員のための賠償責任保険商品が存在するのに、国家公務員のための責任保険商品が存在しないという事実からも、明らかである。」

行政デジタル人材 Y 「なるほど。国のほうではとても急進的に次々に物事が決まるが、地方自治体のほうはとても慎重に物事を決めていき動きが比較的ゆっくりとしている現象をみて、その温度差がなぜ発生するのか、昔から疑問だったのだが、その根本的原因として、住民訴訟権の有無があるということか。」

行政管理職 X 「まあそういうことである。この観点からデジタルガバメントに関する国に関わる各個人の行動を見ていくと、明確な温度差が見出されて、誠に興

味深いものである。」

行政デジタル人材 Y 「なるほど。そういえば、最近、国のほうで開かれたという、ガバメント用クラウドやネットワークに関する委員会のようなところで、国のほうは随分と急進的な方法を提案したそうで、他方で構成員たちのほうからは、あまり急いでやると危ないのではないかということで、ずいぶん慎重な意見が出てきたそうである。国は急進的で、委員のほうはずいぶん慎重である理由は何だろうか。」

行政管理職 X 「国の意見は、国と雇用関係にある閣僚や公務員が出す意見だから、先ほどの理論でいうと、それによって損害が国に生じても、重大な過失または故意がある場合に限り、かつ国が求償した場合にだけ、個人賠償が課せられるのである (国家賠償法 1 条 2 項)。他方、委員は国との間で委任関係が成立しているから、これは専門家としての善管注意義務というのが課せられていて、重大な過失だけでなく、普通の過失についても責任を問われて、賠償させられるリスクがあるのだ (民法 644 条)。しかも、国と雇用関係がある閣僚や公務員は、国家賠償法で、第三者からの直接賠償請求が制限されるが、国と委任関係がある委員は、発言に過失があったならば、第三者から不法行為責任を直接追及されるリスクがあるのだ (民法 709 条)。」

行政デジタル人材 Y 「なるほど、だから委員はガバメント用クラウドについて結構慎重な意見を出し、国のほうはかなり猪突的な意見を出すということになるのか。」

行政管理職 X 「そうだ。それに関してもう一つ、興味深い現象がある。大臣は国会議員だが、国会議員は憲法 51 条によって、国会でいかなる演説、討論または表決を行なっても、責任が追及されない、とされている。過失があっても同じである。もちろん、選挙民に対する政治責任は問われるが、より重要な、国や損害を受けた被害者に対する民事賠償責任は、全く問われないのである。」

行政デジタル人材 Y 「なるほど。そうすると、ガバメント用クラウドに関係する物事はもちろんのこと、たいていの政策というものは、(a) 意思決定の内容の法的責任を問われ得ない議会での議論がもっとも急進的で、いってしまえば、かなり

いい加減であり、かなり好きなことを言って良く、(b) 次に個人責任が重過失に限られかつ求償される心配が少ない国の公務員がそれなりに急進的で、(c) 続いて、住民訴訟のリスクがある地方公共団体の公務員はいよいよ慎重であり、(d) いよいよ過失だけでも責任を問われかねない善管注意義務を有する国の委員会の構成員が最も慎重で注意深い、というような、注意深さの序列が構成されるということになる。これは制度的、必然的に常にこのようになってしまうのであり、個人の特質などが与える影響は限定的のようだ。」

行政管理職 X 「深く考えると確かにそのような結論になる。」

行政デジタル人材 Y 「だが、『国会議員や大臣はかなりいい加減であり、好きなことを言っていれば良い』などというような陰口をここで言うのはちょっと危険ではないか。ここで言っているこの内容が文書化されてどこかにでも載せられたとしたら、権力的な国会議員や大臣にいずれ読まれて不利益を受けてしまうかも知れないではないか。ちょっと発言には注意しなければならない。われわれは、そういう批判的思考を持たないように注意しなければならない。」

行政管理職 X 「それは問題の本質を突いている。まさに、『見られているかも知れない』という状態が、そのような健全な自由的思考に影響を与えるというリスクが、まさに、米国クラウド法の元で、米国系パブリッククラウド事業者が提供するガバメント用クラウドを利用することによって生じるリスクなのである。主権者の情報がいつでも外国に監視されて取得されているという心理的状態は、監視されているかもしれないという側の行動に深刻な影響を与えるのである。これは、われわれの民主的意思決定権、すなわち国としての自己決定権をおびやかすのである。1791 年に発表されたベンサムのパノプティコンの話は、有名であろう。ところで、具体的に、まさに今のこのつまらない会話がいちいち文書化され国会議員や大臣の方々が入手して読むとは到底思えないから、本日の議論については、問題はない。」

行政デジタル人材 Y 「いや、先にも私が主張したとおり、このことはいかように工夫してもわれわれ 2 人の目には見えないのだが、われわれは口頭により自由意思に基づきこの会話を発しているように見えて、実はそうではなく、その思考と議論は、紙あるいは PDF の上の文書に、文字として、確かに、発言より先に固定

的に記録されているのであると考えられるのである。」

行政管理職 X「先に議論した話の蒸し返しである。その証拠はないではないか。この話はやめにしよう。」

行政デジタル人材 Y 「やめにしよう。それに、先ほどの、政策において人々によって慎重度合いにむらが出て温度感に不統一性が生じるというよくある行政的混乱問題は、個々の国会議員や大臣や公務員や委員に責任があるわけではなく、法律で決まっているのでどうしようもないことだ。法律による行政の原理というものは、行政の者は定まった法律に従うしかないという法理である。しかし、それでも、何とか方法はある。我々 2 人はちょっと前述の保険に入るなどして大胆な行政デジタル化改革などやっていこうではないか。つまりその保険に入っていさえすれば、われわれ職員がガバメント用クラウドを利用して、米国系パブリッククラウド事業者のサーバーに住民の情報が載ったシステムを次々に移行していったとして、違憲判決が出て多額のコストがかかったとしても、住民訴訟を起こされても個人的にはそれなりに安全だということで、合っているか。」

行政管理職 X 「それはまあそうかも知れないが、それは問題の本質的解決になっていない。第一に、保険というのは金銭問題を解決するだけで、損害を実際に解決することにはならない。第二に、住民のデータが米国クラウド法によって他人(米国連邦政府または米国州政府の捜査官等) に取られたら、その漏えいは、もう元には戻せない。被害者である住民に形式的に損害賠償を支払ったとしても、住民が侵害された憲法 13 条の『個人情報をみだりに第三者に開示されない自由』は、本質的に、回復不可能である。第三に、米国クラウド法に基づいてデータが第三者に次々に取られていくと、やがてその第三者に強大な権力が発生してしまう。その第三者の強大な権力は、われわれ日本国民の主権をおびやかすリスクがある。それは避けなければならない。第四に、主権者の情報がいつでも外国に監視されて取得されているという心理的状態は、われわれの民主的意思決定権、すなわち国としての自己決定権をおびやかすのである。先ほどの話である。第五に、国民からわれわれ行政に対するデジタルガバメントに係る信頼が決定的に失われ、回復困難となる。実際に、住基ネット事件訴訟が原因で、この国のデジタル化が随分と長引いたではない

か。先にも述べたことであるが、ガバメント用クラウドにおける米国クラウド法との関係の違憲問題は、国内における個人情報の管理の問題と、日米関係の問題との両方に重なり合う、希有な重大問題で、それが表面化したときに生じる波乱や疑心暗鬼は、とてつもなく大きく、長続きする。この第五による損害が、一番大きい。だから、これを避け、スムーズなガバメント用クラウドへの移行を実現するためには、米国クラウド法の引き起こす違憲問題を、あらかじめ、解消していくほかない。」

行政デジタル人材 Y 「米国クラウド法については、すでに国会でも議論されていて、次のような国会答弁があったはずだ。すなわち、日本政府または日本の地方公共団体の有するクラウド上のデータに関し、米国政府から米国系パブリッククラウド事業者へのデータ提供命令があった場合、日本政府または日本の地方公共団体の有する国民の個人情報が米国政府に提供されることを避けるため、米国系パブリッククラウド事業者の異議申立てや日本政府への事前の通知を求め、そのような通知があったならば、日本政府が米国系パブリッククラウド事業者と協議し、適切に対応する、という答弁だ (第 204 回国会 参議院 内閣委員会 第 17 号 2021/5/11、第 208 回国会 衆議院 内閣委員会 第 12 号 2022/03/25)。だから、米国クラウド法に基づく開示命令が出ても、米国系パブリッククラウド事業者が米国政府に異議申立てをしてくれることが期待できるし、日本政府への通知があることも期待でき、住民のプライバシー情報が第三者 (米国政府) に漏えいするリスクは、ほとんどないのではないか。」

行政管理職 X 「確かに、日本政府と米国系パブリッククラウド事業者との間の契約で、事業者に対して、必ず異議申立てを行なうという契約上の義務を課すことはできる。ところが、データ開示命令は、捜査令状または行政召喚状でなされるので、異議申立てを行なったとしても、覆る可能性はとても低いのである。捜査令状については、一度米国裁判所による司法審査を経て発付されるので、重大な誤りがない限り、覆らないであろう。行政召喚状は、米国裁判所による審査なしで米国の行政機関が発付できてしまうが、それについては、もちろん異議申立てにより司法審査がなされる。だが、米国連邦最高裁判所は、米国の行政機関による召喚状による行政調査の権限は、その権限を過度に制限すると行政機関がその法的責任を遂行

できなくなるおそれが高いことから、広範囲な権限を認めている。」

行政デジタル人材 Y 「それでも、米国裁判所は、われわれ日本人の憲法 13 条の権利、すなわちプライバシー権利を尊重して、異議申立てを十分真剣に取り扱ってくれる期待が持てるのではないだろうか。」

行政管理職 X 「残念ながら、そういうわけにはいかないのだ。もちろん、米国憲法修正第 4 条には、捜査機関に対するプライバシー権は保障されるとある。だが、これについては米国最高裁による判例が出ていて、米国非居住の外国人には憲法上の権利として保障されないということになっているのだ。米国捜査官がメキシコでメキシコ人の被告人の自宅を捜索して入手した文書について争われた事件 (United States v. Verdugo-Urquidez, 494 U.S. 259 (1990)) で、そのような結論が出てしまった。」

行政デジタル人材 Y 「それでは、日本政府が米国系パブリッククラウド事業者経由で米国政府からのデータ開示命令が出たことの通知を受けたら、すぐに日本政府が米国に、データ開示命令を破棄するよう、直接頼むことはできないのか。」

行政管理職 X 「それには 2 つの問題がある。第一に、米国当局は、データ開示命令の発布をする際に、その旨をデータ取得対象者に通知することを禁止する命令を合わせて米国裁判所から取得することができる。この場合、米国系パブリッククラウド事業者は、日本政府に通知をすることができなくなってしまう。それに違反すると、司法妨害罪や裁判所侮辱罪に問われるので、米国系パブリッククラウド事業者の取締役または従業員は、必ず従わざるを得ないであろう。第二に、仮に通知を受けることができたとして、日本政府が米国政府に対して外交的に "協議" しても、これは無意味であると考えられるのである。データ開示命令は米国の裁判所を通じて発付されるが、米国においてはもちろん三権分立が徹底しているから、いくら日本政府が米国政府に外交ルートを通じて依頼をしても、それは米国裁判所に対して効果がない。」

行政デジタル人材 Y 「しかし、国会答弁では、次のことも確認されたはずだ。すなわち、日本政府と米国系パブリッククラウド事業者との契約上、一切の紛争は "日本の裁判所が管轄" し、"日本法を準拠法" とする、というものである (第 204 回

国会 参議院 内閣委員会 第 17 号 2021/5/11)。これで安心ではないのか。」

行政管理職 X 「これでも、全く安心できない。日本政府と米国系パブリッククラウド事業者との契約をたとえ日本法に準拠させたとしても、また、たとえ専属的合意管轄を日本の裁判所としたとしても、それは契約者である日本政府と米国系パブリッククラウド事業者との間の民事上の関係を規定するに過ぎない。米国クラウド法は、米国連邦政府または米国州政府と米国系パブリッククラウド事業者との間の公法上の関係を規定する法であり、この 2 者の法的関係と、米国系パブリッククラウド事業者と契約者との法的関係とは、全く独立した、別々の関係である。だから、この管轄や準拠法の意味は、データ開示命令を阻止するために意味がないと思われる。」

行政デジタル人材 Y「それでも、国会答弁では、次のことが確認されたはずだ。すなわち、米国クラウド法は、米国政府に無制限なアクセスを認めるものではなく、米国のための犯罪捜査という極めて限定された場合において、米国の裁判所が発する米国の令状等に基づき、米国系パブリッククラウド事業者に対して開示命令が行なわれるに過ぎないから、脅威は限定的であると考える、というものだ (第 208 回国会 衆議院 内閣委員会 第 12 号 2022/03/25、第 210 回国会 衆議院 内閣委員会 第 7 号 2022/11/11)。これで安心ではないのか。」

行政管理職 X「これもなお、全く安心できる材料にならない。まず、米国では、犯罪捜査のための令状発付は、きわめて頻繁に行なわれていて、連邦裁判所だけでも 1 年間で 32,282 件の通知遅延型捜査令状が申請され、99.5% が裁判所によって認められている。次に、司法審査を経ない行政召喚状についても、年間約 4,000 件が発付されている。2022 年の下半期だけ見ても、たとえば、米国 Microsoft Corporation は、米国政府から合計 4,908 件ものデータ開示請求を受けている。87% について契約者情報またはデータを検索し、その結果 (結果が存在しない場合は、その旨) を回答している。法令に準拠しないとして回答を拒否したものは、わずか 13% の 644 件に過ぎないのである。決して限定的で例外な事象であるとはいえない。たとえば、ある日本人が、米国内で横領、詐欺、脱税、テロ、あるいは薬物の不法摂取等の犯罪を行なったと疑われている状況を考えてみると

よい。その日本人は日本に帰国してしまっているが、米国捜査員としては、彼が後日また米国にやって来たときに訴追することを予定しており、刑事証拠を収集したいと考えたとする。米国捜査員としては、その日本人に関する犯罪の証拠となり得る情報 (たとえば、税務記録、健康保険記録、健康管理情報、図書館貸出履歴等のシステムの情報) を、日本国政府のガバメント用クラウド上に記録されている、日本政府または日本の地方公共団体のクラウド領域上のこれらのシステムのデータを取寄せることが最良であると判断したとする。すると、その日本人のデータは、日本政府またはわれわれ自治体の許可なく、そして、一切の日本の裁判所の令状審査もなく、全くの他人である、米国連邦政府または米国州政府の捜査員に取得されてしまうことになる。加えて、その日本人のデータが、他の日本人のデータと一体・不可分なデータベースファイルに入っている場合、その無関係の他の日本人のデータも合わせてデータベースファイルごと取得されてしまう可能性がある。」

行政デジタル人材 Y 「いよいよ心配になってきた。しかし、国会答弁では、次のことも確認されたはずだ。すなわち、万一、米国クラウド法に基づく命令があった場合は、"外国主権免除法に基づく主権免除の適用" を米国に求めることで、開示を阻止できる、というものだ (第 210 回国会 衆議院 内閣委員会 第 7 号 2022/11/11)。この、『外国主権免除法に基づく主権免除の適用』という画期的な手法により、何とかなるのではないか。」

行政管理職 X 「それについては、先日よく調べてみたのだが、どうもその政府答弁の言っていることは、実は外国主権免除法の話ではなく、米国法第 18 編 121 章 2703 条 (h) の "Comity Analysis" (国際礼節に基づく法的解釈) の手続を意味しているようだ。まず、政府答弁のいう外国主権免除法 (Foreign Sovereign Immunities Act) の趣旨は、民事訴訟に限定した概念であり、米国クラウド法が実現する刑事訴訟手続上のデータ開示命令については、全く無意味だと思われるのである。主権免除の適用という概念は、米国判例法上、連邦または州は、政治的または統治的性質を有する行為から生ずる結果について不法行為責任を問われることがない、という理論である。これが 1812 年の判例 (Schooner Exchange v. McFaddon, 11 U.S. 116 (1812)) によって拡大されて、外国政府も、同様の免除が認められるよ

うになった。だが、米国クラウド法には、この理論が使えない。そこで、日本政府としては、米国法第 18 編 121 章 2703 条 (h) の "Comity Analysis" の規定を用いる必要があるが、そのためには、日米間で、あらかじめ、第 2523 条に基づく行政協定を締結しておく必要がある。今のところ、その行政協定は締結されていない。よって、2022/11/11 の国会答弁で説明されている方法では、開示を阻止できないと思われるのである。」

行政デジタル人材 Y 「それでは、米国クラウド法の対象となる以上、現行のガバメント用クラウド上で住民のプライバシー情報を仮想ディスクやデータベース上に保存することで、日本においては、その住民に対して、違憲状態が生じてしまう可能性があるということか。」

行政管理職 X 「そのとおりである。住基ネット事件最高裁判例 (最判平成 20 年 3 月 6 日) は、個人情報をみだりに第三者に開示されない自由は憲法 13 条によって保障されると認めている。米国クラウド法に対する懸念において、『第三者』とは、米国連邦政府または米国州政府のことである。『みだりに』とは、君も先に言及していたが、同判例の表現を借りれば、『法令等の根拠に基づかずに又は正当な行政目的の範囲を逸脱して』、という意味である。ここでいう『法令等』とは、日本国の法令等のことである。米国クラウド法による米国当局によるデータの取得は、明らかに、日本国の法令等の根拠に基づくものではない。むしろ、行政機関の保有する個人情報の保護に関する法律 6 条 (安全確保の措置) 1 項、8 条 (利用及び提供の制限) 1 項 という日本国の法令に違反した状態が生じる。」

行政デジタル人材 Y 「しかし、住基ネット事件最高裁判例では、第三者に対して、われわれ行政機関の側が能動的にデータを提供することが問題となったもののはずだ。今回の米国クラウド法の問題は、それとは異なるのではないか。われわれ行政機関のクラウド領域に置かれているデータが、米国クラウド法によって無断で第三者 (米国連邦政府または米国州政府) によりコピーされるものだから、われわれ行政機関の側は、あくまでそのような不正なアクセスの被害者であり、能動的に米国当局にデータを提供した訳ではない。われわれ行政機関はその不正なデータコピーに関して何ら能動的な行為を行なっていないので、憲法違反に問われることはない

のではないだろうか。」

行政管理職 X 「何ら能動的な行為を行なわず、単に第三者による行為による被害が発生するがままに放置することを、『不作為』という。不作為は、確かに責任を問われない場合もある。しかし、作為との同価値性があれば、作為と同じように評価されるであろう。具体的には、(i) 結果が予見可能であり、かつ、(ii) 作為可能性があり、(iii) 作為が容易であれば、作為と同じように評価されるであろう。(i) について、すでに上記のとおり米国クラウド法に関する議論をわれわれは行なっているので、予見可能性を満たす。(ii) 米国クラウド法による不正データ送信問題を発生させないようにするためには、単に米国パブリッククラウドを用いるガバメント用クラウドを利用しないようにすれば良い話であり、作為可能性がある。加えて、(iii) 作為はとても容易である。米国パブリッククラウドを用いるガバメント用クラウドを利用する以外のシステム移行方法は多数存在する。そもそも今問題となっているわれわれのシステムは、これまで自ら構築運用するサーバーで動作していたものであり、これをあえて明日ガバメント用クラウドにデータコピーにより引っ越ししようとしている所であった。この状態で、米国クラウド法に関連する問題を今われわれが認識・容認している以上、米国クラウド法に基づく日本法に準拠しない (日本の主権者の視点でみた評価としての) 不正なデータ抽出が行なわれたならば、われわれ行政機関の責任は免れることができないと思われる。」

行政デジタル人材 Y 「なるほど。確かにそれはそのとおりだが、ここで今一つ疑問が生じるのである。つまり、㋐ われわれ行政機関が国民の個人情報をガバメント用クラウドとしての米国系パブリッククラウド事業者のサーバーに置いた時点ですでに国民はわれわれに違憲訴訟を起こすことができるのか、それとも、㋑ その後いよいよ米国クラウド法に基づいて第三者 (米国当局) がデータをわれわれのサーバーから抽出した時点ではじめてその対象となった国民はわれわれに違憲訴訟を起こすことができるのか、という疑問である。」

行政管理職 X 「それは、プライバシー権に関して、㋐ 妨害排除請求権のみが認められるか、それとも、㋑ 妨害予防請求権も認められるかという問題である。プライバシー権について妨害予防請求権の存在を否定された判例はなく、最近の判例

では、存在を認める傾向にある。住基ネット事件最高裁判例では、もともと控訴審で妨害排除請求権が認容されたので、最高裁では妨害予防請求権利の主張は審理対象となっていなかったので、明確ではない。しかし、マイナンバー利用差止等請求控訴事件判例 (仙台高等裁判所令和 3 年 5 月 27 日) は、事案事態は棄却したものの、プライバシー権に対する妨害予防請求権の構成を認めている。プライバシー権以外の人格権としては、志賀原発運転差止請求事件控訴審判例 (名古屋高等裁判所平成 21 年 3 月 18 日) も、『個人の生命，身体及び健康という重大な保護法益が現に侵害されている場合，又は侵害される具体的な危険がある場合には，その個人は，その侵害を排除し，又は侵害を予防するために，人格権に基づき，侵害行為の差止めを求めることができる』旨を認めている①。北方ジャーナル事件最高裁判例 (最判大昭和 61 年 6 月 11 日) も、プライバシー権ではなく名誉権を対象として、出版物の発行前の差止めとして、妨害予防請求権を認めている。このように、通常の人格権またはプライバシー権侵害であっても、妨害予防請求権は認められる傾向にあると考えられる。加えて、米国クラウド法に関して考察すると、前述したとおり、米国クラウド法の手続上、米国当局は米国系パブリッククラウド事業者に対して、ガバメント用クラウドに対するデータ強制取得に際して、その事実を契約者である日本政府に事前通知することを禁止する命令を発布することができてしまう。この場合、ガバメント用クラウド上に機微なプライバシー情報を記録されている日本の国民、そして、日本政府や地方公共団体も含めて、日本人は、米国当局による、日本法上違法なデータ取得に気付くことすら困難となる。データ取得がなされたことの通知を受けることができない状況においては、㋐ 妨害排除請求権の行使は事実上不可能であり、そのため、国民としては、㋑ 妨害予防請求権を行使して、あらかじめデータ開示からの予防措置を国または地方公共団体に求めるしかないという状態になるのである。このようなことから、米国クラウド法に関連しては、㋑ 妨害予防請求権が認められると考えられる。」

行政デジタル人材 Y 「そうすると、われわれ地方公共団体としては、ガバメン

① マイナンバー訴訟における「私生活上の自由」, 斉藤邦史, 情報法制研究 第 10 号, 2021/11

ト用クラウドを利用できないことになってしまうのではないか。」

行政管理職 X 「いや、これから議論することとなる、適切な対策を施せば、その心配はなくなるから、安心してよい。政府答弁にもあるように、仮に米国政府がデータを取得できてしまったとしても、米国政府がその内容にアクセスできないように、暗号化措置を事前に講じているので、米国政府へのデータ漏えいの危険は防止できるのである (第 204 回国会 参議院 内閣委員会 第 17 号 2021/5/11、第 208 回国会 衆議院 内閣委員会 第 12 号 2022/03/25)。」

行政デジタル人材 Y 「暗号化というものは、米国系パブリッククラウド事業者の提供するクラウド側での暗号化処理で十分か。」

行政管理職 X 「いや、クラウド側の暗号化では不十分であり、クライアント側での暗号化が必要である。なぜならば、クラウド側での暗号化は、契約者データの一部分としてのその暗号鍵がクラウド上に電子的に保管されているので、米国連邦政府または米国州政府は、米国クラウド法に基づき取得したデータが暗号化されてした場合、次は、契約者データの一部分としてのその暗号鍵データの取得を行なうことができてしまうであろう。この 2 つのデータが取得されれば、米国連邦政府または米国州政府は、取得した暗号化データを、彼らの有する普通のコンピュータで完全に解読できてしまう。米国クラウド法は、米国系パブリッククラウド事業者に対してデータの復号化を義務付けていないので、米国当局としては、この方法で、自ら復号化するしかないのである。その結果、日本国民のプライバシー情報を米国当局に取得されてしまい、やはり憲法違反、行政機関の保有する個人情報の保護に関する法律違反となってしまう。だから、クラウド側での暗号化が必須である。」

行政デジタル人材 Y 「結論としては、われわれ地方公共団体は、ガバメント用クラウドを利用する際には、必ずクライアント側での暗号化を行ない、米国連邦政府または米国州政府が米国クラウド法に基づいていかなる努力をしても米国系パブリッククラウド事業者の提供するガバメント用クラウド用のコンピュータ群上に保存されている情報から元の平文を解読することが現実的時間内に決してできないという状態を維持すれば、ガバメント用クラウドの利用行為は合憲となる、しかし、暗号化が不十分であれば、違憲となる、という考え方で安全か。」

行政管理職 X 「だいたいはそれで安全だと思われる。ただし、注意点が数点ある。第一に、暗号アルゴリズムは、政府推奨暗号リスト[①]に記載されている十分な強度を有するものに限るべきである。第二に、暗号鍵は、十分な長さを有し、推測不能なものにする必要がある。第一または第二を怠り、たとえば、DES を用いて暗号化しただけでは、米国連邦政府または米国州政府は、米国クラウド法に基づいてダウンロードしたわれわれ地方公共団体のデータを容易に復号化することができるから、その状態となっているだけで、違憲状態となると考えられる。第三に、これが肝心な点であるが、暗号鍵データは盗まれないようにするとともに、絶対に紛失しないように、確実に保管していなければならない。鍵を紛失してしまうと、全データへのアクセスが不可能となる。これは、鍵をクラウド側で保管してもらえることによる紛失対策利益とのトレードオフであるが、米国クラウド法に対抗するためには、決して鍵をクラウド側で保管させてはならないので、この鍵を絶対に紛失しないようにするという負担は、やむを得ない負担である。もっとも、鍵を A4 用紙で数枚印刷しておいて、『捨てるな』等と書いて、庁舎内の数ヵ所の金庫と、できれば他に安全な場所 1 箇所以上に保管しておけば、すべての紙を紛失しない限り、自ら復号が不能となるリスクはほとんど避けることができ、安心である。」

行政デジタル人材 Y 「よく理解することができた。それに、この長大複雑な議論は昨夜に開始されたものであるが、その議論の果てにおいて、今、庁舎の窓から少し外の暗闇を睥睨したところ、ついには、先ほど議論した太陽寿命の件にも呼応したのか、ようやく夜明けが向こう側からやってきたようであり、夜中に帰宅しまた早朝に登庁する手間も省けたのであり、これはその点においても、誠に便利で有益な議論であった。そして、もうすぐ朝がきたら、だいたい 3 人がかりでガバメント用クラウドに既存のシステムのデータを移行しようと予定していたその予定作業の実施において、必ず IaaS のゲスト OS 内の作用として仮想ディスク上にクライアント側暗号化を施し、その暗号鍵は決して当該クラウド上に残存させないようにすることによって、米国クラウド法に基づく米国連邦政府または米国州政府

① https://www.cryptrec.go.jp/list.html

によるデータ開示命令が米国系パブリッククラウド事業者に対して発付されても、決して彼ら第三者にはデータを復号化することができないように最大限留意するとともに、これにより、住基ネット事件最高裁判例基準に従って合憲な状態を維持し、議員、住民、マスメディア等の良識を有する方々から、ガバメント用クラウドを利用していることに関して米国クラウド法に関する違憲状態が生じるのではないかというような指摘に対しても、大手を振って、堂々と、われわれは大丈夫である、権利侵害が発生しないように対策を行なっていると説明することができる状態を維持したいと思う。これは、日本国憲法に定めのある、憲法遵守義務を全うするための当然の仕事であることはもちろんのことであるが、それに加えて、憲法前文に記載のあるように、自国の主権を維持し、他国と対等関係に立とうとする全力をあげた責務としての、重要な経綸行為の開始点が、コンピュータ技術に係る側面については、やはり、われわれ地方公共団体をその健全な精神の中心的発達場として、いよいよ、開幕成長してゆくことになるのである。」

第 3 節　住基ネット最高裁判例の違憲判断基準にみるガバメント用クラウドのリスク

行政機関において、コンピュータやネットワークを用いて市民の個人情報を取り扱う際に欠かせないのが、住基ネット事件最高裁判例 (最判平成 20 年 3 月 6 日) である。同訴訟では、従来、自らの住む市町村長にのみ預けてあるはずの個人情報 (住民基本台帳における氏名、生年月日、性別、住所の 4 項目) およびこれに住民票コードを合わせた 5 項目、ならびに転入・転出履歴情報を、市役所が他人 (他の市町村、都道府県、国) にコンピュータネットワーク (住民基本台帳ネットワークシステム、以下「住基ネット」) を経由して提供することが、憲法 13 条の幸福追求権によって導出されるプライバシー権の侵害にあたり違憲であるか否かが争われた。最高裁は、個人情報をみだりに第三者に開示されない自由は憲法 13 条によって保障されることを改めて認めた。その上で、住基ネットに関しては、次のような事実認定および法的判断に基づき、合憲とした[①]。

(1)　住基ネットを経由して他の行政機関に開示され得る個人情報は、「氏名」、「生年月日」、「性別」、「住所」および「転入・転出履歴」である。これらの個人情報は、個人の内面に関わるような秘匿性が高い情報ではなく、本人確認のために従前から行政機関をまたがって事務処理に利用されてきた。住基ネットを介してこれらの事務処理を行ない、「住民票コード」を付番して併せて処理に利用したとしても、「個人に関する情報をみだりに第三者に開示又は公表するもの」とはいえない。

(2)　個人情報は、市町村から、住基ネットおよび都道府県サーバーを経由して、「全国サーバー」に、送信され、保存される。この「全国サーバー」は、指定情報処理機関 (現在の J-LIS) に設置されている。そして、指定情報処理機関の職員が、情報を他人に漏えいした場合は、公務員の守秘義務違反に該当し、刑罰の対象となる。このような法制度上の予防の仕組みが具備

① https://www.courts.go.jp/app/files/hanrei_jp/933/035933_hanrei.pdf

されている (注: 指定情報処理機関の職員は、みなし公務員である。地方公共団体情報システム機構法 21 条参照)。

(3) 住基ネットのシステム技術上、個人情報が容易に漏えいする具体的な危険はない。

(4) 上記 (2) の法制度と (3) のシステム技術上の不備はなく、住基ネットの個人情報が法令等の根拠に基づかず又は正当な行政目的の範囲を逸脱して第三者に開示または公表される具体的危険が生じているとはいえない。

したがって、国民の個人情報を扱う行政事務のデジタル化において、住基ネット事件最高裁判例の上記基準 (1) ～ (3) の前提のいずれか 1 つでも欠けるだけで、裁判所が違憲判断に傾くリスクが増大する。われわれは、国及び地方公共団体のシステムのうち、国民の個人情報を扱う部分をガバメント用クラウドで運用する場合において、これをパブリッククラウド事業者のパブリッククラウドサービスに預ける際に、上記前提 (1) ～ (3) のいずれかに欠陥が生じないように、最大限の注意を払わなければならない。

ガバメント用クラウドにおいてパブリッククラウド事業者を利用する場合における問題を分析する際には、3 つの問題に分類することが有用である。(a) 国内の行政機関相互のデータ提供問題と、(b) 一極集中型のパブリッククラウドを利用することによるデータの第三者への漏えいリスク軽減法の問題と、(c) 外国のパブリッククラウド事業者が当該外国政府からの命令によってデータを提供してしまう問題の 3 種である。以下で、それぞれ検討をする。

(a) 国内の行政機関相互のデータ提供問題

国や地方公共団体は、これまで、自らが完全に支配管理するコンピュータシステムを用いて、例えば、「住民基本台帳」、「戸籍情報」、「税務記録」、「健康保険記録」、「生活保護情報」、「就学情報」、「障害者情報」、「健康管理情報」、「印鑑登録印影データ」、「失業保険情報」、「図書館貸出履歴」などの個人情報を処理してきた。これらの個人情報は、住基ネット事件最高裁判例で示された前提 (1) の「個人の内面

に関わるような秘匿性が高い情報ではなく、本人確認のために従前から行政機関をまたがって事務処理に利用されてきた」情報を超える、極めてセンシティブな個人情報を多く含む。仮にこれをパブリッククラウド化した場合においても、単にそれぞれの国や地方公共団体 (これらは別々の法人 = 行政主体である) が自らのクラウド領域を完全に排他的に支配・管理する限りにおいては、各行政主体はこれらの情報をいかなる時点でも第三者に開示している訳ではないといえるので、第三者への情報の提供の問題、すなわち違憲リスクは生じないように見える。

次に問題となるのは、仮に国が、地方自治体と併せたボリュームディスカウントを狙って、多数の自治体分を合わせてガバメント用クラウドの大規模リソースについてパブリッククラウド事業者と一元的に契約をして調達し、これを各地方自治体に国が有償で再販する関係を採用する場合、一見すると、国が地方公共団体のデータを取得しているように見えるので、住基ネット事件最高裁判例基準 (1), (2) 上、地方公共団体がガバメント用クラウドに個人情報をアップロードした時点で違憲になるというリスクである。しかし、この問題は、すでに国によって発見されつつある契約上の工夫で一応カバーできると考えられる。すなわち、この場合、国が、全体的管理権限を各地方自治体の管理領域に対して決して行使することができない旨の明文の契約が、単に国の一方的宣言だけでなく、国、各地方自治体、および納入元のパブリッククラウド事業者との間のすべての関係性に渡り、法的に完全に有効な不備のない (国による勝手な権限行為を可能とする例外を「一切」認めない = 国の閣僚や国職員による地方自治体の管理領域への勝手なシステム権限行使が、刑罰によって厳罰に処せられる十分な根拠となる) 契約が締結されており、これを担保する法制度も合わせて立法がなされているのであれば、各行政主体のクラウド領域は、少なくとも他の行政主体 (特に、国) との関係においては、国や各地方自治体がそれぞれ別々にパブリッククラウド契約を締結したのと同等のセキュリティが確保されているということができ、違憲リスクは生じないように見える。ただし、ここで十分に注意しなければならないのは、住基ネット事件最高裁判例基準 (2) の確実な遵守が必要であるという点である。国による、ガバメント用クラウド上の、地方自治体のデータに対する勝手な閲覧権限行使を、厳格に法律に基づいて禁止する、法制度上の措置

が必要である。繰り返しになるが、単に、国が、「パブリッククラウド事業者から契約に基づいて受領した管理者権限を、決して行使しない」とか「管理者権限を行使するために必要な多要素認証の QR コード情報を第三者に預け、自らは必ず消去する」旨を、一方的な声明やガイドライン、民事上の契約に記載する等では不十分である。判例に基づき、法制度上、これを担保する立法がなければ、それをしておく (これにより、違反があった場合は、必ず違反者や責任者が処罰される状態とする) 必要があるという点である。このようにして、違憲状態と判断されるリスクを下げておく必要がある。

このように、国が一元的に用意するガバメント用クラウドに、複数の行政機関が、「住民基本台帳」、「戸籍情報」、「税務記録」、「健康保険記録」、「生活保護情報」、「就学情報」、「障害者情報」、「健康管理情報」、「印鑑登録印影データ」、「失業保険情報」、「図書館貸出履歴」などのセンシティブな個人情報を一元的に保存する場合であっても、それらの管理支配領域が、行政機関相互に (特に、国から地方公共団体に対して) 決してアクセス不能であり、これが法制度上も担保されている限りは、少なくとも、行政機関相互の関係上は、住基ネット事件最高裁判例基準における (1), (2) と同等の状態が満たされており、違憲リスクは生じ難いように見える。従前は個別の行政機関の電算室内に分散して設置されていた物理的なサーバーコンピュータやディスクが、物理的には少数のクラウドサービス事業者のシステムに一極集中するものの、論理的には従来と全く変わらない仮想的分離がなされていれば、従来と何ら変化がない状態であると説明することが可能であるためである。イメージでいうと、とても巨大な合同データセンタ倉庫を国が安価で借りて、その中を金網ケージで仕切り、それぞれの金網ケージの鍵を各地方自治体に渡し、合鍵は決して国で保持せず、完全に各領域を地方自治体に占有させ、その中に各地方自治体がサーバーコンピュータを並べるのと同じ状態であるためである。

(b) 一極集中型のパブリッククラウドを利用することによるデータの第三者への漏えいリスク軽減法の問題

住基ネット事件最高裁判例基準によると、単に (a) の問題が解決されたからと

いって、違憲状態が解消される訳ではない。大量の個人情報が詰まった全国の国と自治体の行政システム群が、一極集中的にパブリッククラウド化された状態に対してのセキュリティ上のリスクが高まっていくと、今度は、住基ネット事件最高裁判例基準における (3) 技術上の不備のリスクに際し、違憲状態となるリスクが、その一極集中度合いに応じて、どんどんと、増大していくことになる。これを解決する必要がある。パブリッククラウドサービスの基盤ソフトウェアには、オンプレミスの基盤ソフトウェアと比較して、原理上、多数の未発見の脆弱性が存在するリスクが存在し、ソフトウェアのコードの流出等の比較的ひんぱんに発生する現象が原因で、これらが一気に顕在化した場合、高度なサイバー攻撃者がパブリッククラウドサービスの特権領域を侵害し得る可能性が高い。このような脆弱性は、パブリッククラウド事業者の雇用する少数の特権的プログラマの注意不足 (これは、現在の技術水準では、十分に予防することも、検出することも困難である) により、始終作られて、次々に基盤ソフトウェアのプログラムコードに埋め込まれてゆくが (オンプレミスの基盤ソフトウェアと異なり、コードが公開されないので、これは、ほとんど発見されないから、増大する一方である)、その脆弱性を悪用した大規模サイバー攻撃は、10 年 ～ 20 年単位で発生し得る。そして、このようなパブリッククラウドサービスの特権的基盤部分に対する大規模サイバーインシデントの発生は、単なる一ユーザーとしての契約者である日本政府によっては、全く左右することができない事柄となるのである。全く衆人環視がなされていない、秘密のパブリッククラウドサービスの基盤ソフトウェアを開発する少人数の精鋭プログラマの腕に、極めて属人的に責任が集中し、彼ら少数の頭脳に依存している状態になっているためである。ところが、彼ら少数の頭脳の多くは外国人であり、日本国民や日本政府によって民主的に選ばれた訳ではなく、彼らに対しては、日本国の主権者による民主的統制が全く利かない。これが、従来の、日本の各行政主体の職員が自ら構築運営してきたオンプレミスのサーバーコンピュータを利用する場合と、パブリッククラウドサービス基盤を利用する場合との、大きな違いである。このように、日本政府や各地方自治体は、従来と異なり、パブリッククラウドサービスを本格的に利用し始めたら、もはや、それ以降は、大規模サイバーインシデントの発生をいかように努力しても全くコントロ

ールできない状態に陥る。しかし、このことに対する対策は容易である。そのようなパブリッククラウドサービスの欠陥が一度でも現実化・表面化してしまったときに備えて、裁判所によって、われわれの判断が元となり、住基ネット事件最高裁判例基準 (3) に比して、地方公共団体によるガバメント用クラウドの利用が違憲であったと認定されないようにするためには、われわれは、予め、パブリッククラウドサービスに保管するすべてのデータ (仮想ディスクイメージ等) を、クライアント側での暗号化等、技術的に容易にとり得る手法により、確実に予防することを、ガバメント用クラウドの利用上の要件として明確化・義務付けする必要性がある。このような簡単・確実な予防策については、資料 ③ に具体的に記載している (なお、このような技術的安全手法でどうしても予防できないような構造となっている一部の情報システムは、やむを得ず、パブリッククラウド化を避け、各行政主体の物権的な完全支配領域、すなわち、オンプレミス的なサーバーや、プライベートクラウドに設置しなければならない。しかし、そういったものは、ごく例外であり、大抵のシステムは、パブリッククラウドサービスに設置する際にクライアント側での暗号化等の対策を適切に施すことについて、技術上の問題はないと考えられる)。

(c) 外国のパブリッククラウド事業者が当該外国政府からの命令によってデータを外国政府に提供してしまう問題

行政クラウドにおけるパブリッククラウド利用に関連し、上記の問題 (a), (b) は、すでに本会議においても、また過去のさまざまな場所においても、一定程度議論がなされてきた模様である。ところが、われわれが未着手の大きな問題がもう 1 つ存在する。それは、外国のパブリッククラウド事業者が当該外国政府からの命令によってデータを提供してしまうという問題である。米国クラウド法の問題は、この問題である。

前述の (a) の、国が借り受けた巨大なデータセンタ倉庫のイメージで比喩すると、次のような解説が可能である。国と地方自治体との間では堅牢な金網ケージによって互いが隔てられることで、1 つの倉庫を複数の行政主体が共同利用しても安全であると考え、これにより、住基ネット事件最高裁判例に照らして、合憲性が

維持できていると楽観視してきた。倉庫は、もちろん、日本国内に存在し、日本の排他的な主権が及ぶ範囲であると、われわれ行政主体は、信じていた。ところが、実はその倉庫主は外国人であり、その外国人が、その母国の、仲の良い別の外国人(外国政府の職員)に、「捜査」という大義名分で命じられて、次々に、外国政府の職員を、夜中に、その倉庫に出入りさせることができるというのである。倉庫主は、倉庫の入口の鍵はもちろんのこと、日本の国や地方自治体が個別に互いを分離している金網ケージの鍵も解錠することができ、その中にあるデータを、悠々と、見廻って、色々と欲しい情報また朝になったら気付かれずにそそくさと去って行くのである。

いうまでもなく、いかなる外国政府も、日本の各行政主体とは全く異なる法人であり、かつ、日本国憲法における国民主権原理のコントロール下にない、「他人」である。いかなる外国において、いかなる法が制定させ施行されていたとしても、その法の立法過程について、日本の主権者は一切関与していない。また、そのような夜中のこそこそとした外国人による倉庫出入り行為について、当該外国においていかなる権威がある裁判所がいかなる判断を下したからといって、その裁判所の裁判官の判断には、日本の主権者からみて、何ら正統性はない。日本の行政主体が、日本の主権者の財産(個人情報)を安全に保管するための倉庫として、誠に無防備な倉庫を借りていたという過失を後から知った日本の主権者たちは、とても怒り、国政に対する支持が失われるおそれがある。日本の裁判所による違憲判決も出てしまうかも知れない。日米間の国際問題に発展し、貴重な財産である日米関係を損なうリスクもある。そして、日本の主権者は、いざ事が発生した後に、色々と調べるうちに、ついには、このリスクを認識しつつ議論していなかったのは、なんとわれわれ専門家であることを突き止め、日本の主権者の怒りは、いよいよ、われわれ専門家に向けられることになるのである。このようなリスクが、明らかに存在する。われわれは、これを避けなければならない。したがって、この問題を今注意深く検討し、予防を行なう必要がある。

現在、ガバメント用クラウド計画において問題となり得る最大のリスクは、米国クラウド法である。日本の行政主体による米国系パブリッククラウド事業者のクラ

ウドコンピューティング基盤利用に際し、米国クラウド法に基づき、米国連邦政府または米国州政府の捜査官による令状取得により、それらのデータがそのような米国政府職員に取得されてしまい、分析の対象とされてしまうリスクである。これにより、国民がわれわれ行政主体に保管を委ねている個人情報が、「他人」であるこれらの米国連邦政府または米国州政府の捜査官に対して取得され、分析されてしまうリスクである。このリスクが現実的に直ちに発生し得るかどうか、かつ、現実化に際して、日本国政府または地方自治体が、当該外国 (米国) に対して、日本国の法体系と日本国の司法審査権の支配に基づき、これを差止めることができる法制度上の具備が、日本国内および米国との関係において、確実になされているかどうかという点が、日本の主権者の関心事であると思われる。万一、米国クラウド法に対応するための技術上および法制度上の対策が十分に講じられていない状態で、ガバメント用クラウドとして米国パブリッククラウドが利用された場合は、住基ネット事件最高裁判例基準 (2) ～ (4) に照らすと、違憲とされる可能性が極めて高くなる。そこで、このようなリスクがあるかどうかを検討するためには、まず、米国クラウド法の中身を読み込んで、その仕組みをある程度理解する必要がある。次に、このようなリスクへの対処を行ない、合憲状態を維持するために必要な技術的対策方法を策定し、実行する必要がある。

第 4 節　米国クラウド法の仕組み

「米国クラウド法」 (CLOUD Act: Clarifying Lawful Overseas Use of Data Act) は、2018 年 3 月 23 日に米国で成立した、米国国内法である。ヨーロッパの先進国各国においては、最近、行政クラウドサービスの基盤として米国のパブリッククラウドサービスを利用する場合、米国クラウド法が重要な問題となっている。

ところが、日本国内では、そもそも米国クラウド法とは具体的にどのような構造となっており、何を規定しているのか、何が問題なのか、という最も根本的な部分の情報すら、日本人は、これまで、ほとんど確認、議論していないように見える。米国クラウド法について議論するのであれば、まず、同法の条文 (原文) にあたらなければならないのは、当然のことである。ところが、未だ日本語訳すら存在しないようであり、理解が困難である。

著者は、米国クラウド法を読むために、米国の法体系に初めて接した。そのため、ここよりも下の内容は、様々な点で不完全または誤りを数多く含む可能性がある。誤りがあれば、ご指摘をお願いしたい。

【米国法におけるクラウド法】 まず、米国法は、連邦法と州法があるが、米国クラウド法は、連邦法に属する。連邦法は、連邦議会で制定される。連邦法は、第 1 編から第 54 編までで構成される。米国クラウド法は、第 18 編「刑法および刑事訴訟法」に含まれている。米国法は、編ごとに条文番号が連番で付いているようである。第 18 編は、第 1 部から第 5 部までから成り、第 1 条から第 6005 条まで成る。条番号は、部をまたがって付いている。すなわち、ある編の内部では、条文番号はユニークである。編と条文番号があれば、法文を一意に特定できて便利である。日本のように、長い法律名を書く必要はなさそうである。第 18 編では、部ごとに 1000 条単位で番号がアロケーションされており、すべての部は「1000 の倍数 + 1」で始まる。これは、コンピュータのアドレス的 (配列番号的) になっていて、大変興味深い。例えば、第 1 部は 第 1 条から第 2725 条まであり、第 2 部は第 3001 条から始まる、という具合である。先人の知恵で、条数が増えることを見越して、1000 の倍数ごとにページングしているようなのである。それでは、ある編の中のある部の途中に、後から条文を差し込む際に、どうやっているのか。日

本で「第 3 条の 2 の 2」のような具合でパッチを充てる方法はあるのだろうか。よく見ると、たとえば、第 40 条と第 41 条の合間にどうしても 1 条を挿入したいという場合には、第 40A 条という番号、すなわち、「A」というアルファベットを末尾に無理矢理付けた番号を付けて、挿入がなされていた。この具合で、第 40B 条、第 40C 条という風に次々と増えていくようである。それでは、さらに、第 40A 条と第 40B 条との間に条をどうしても挿入したい場合にはどうするのか調べようとしたが、第 18 編を目を皿のようにして眺めてもそういう場合は見つけられなかった。これはより重大な問題として後日また調べてみることにしようと考えている。なお、第 40A 条のように大文字で書くパターンと、第 40a 条のように小文字で書くパターンが混在しているようである。色々な立法担当者の趣味で適当にやっているようにも見える。

さて、第 18 編は、日本法風に呼ぶと、第 1 部は「刑法」、第 2 部は「刑事訴訟法」、第 3 部は「刑事収容施設及び被収容者等の処遇に関する法律」、第 4 部は「少年法」、第 5 部は司法取引制度、という具合に並んでいる。問題となっている米国クラウド法は、おおむね、第 18 編第 1 部の「刑法」の第 121 章「電子データの保存および取引記録へのアクセス法」に含まれている。日本法でいうと、刑事訴訟法における捜査の章の手続の一部と通信傍受法の一部に該当するような部類である。したがって、本来は第 18 編第 2 部の「刑事訴訟法」に含まれるべきだが、歴史的経緯から、第 18 編第 1 部の「刑法」に含まれているようである。その歴史的経緯は、ぱっと法文を読んだ感じでは、おそらく、刑法の中にまず日本の不正アクセス禁止法や電気通信事業法に該当するような、不正アクセスや盗聴を禁止する処罰規定が 1986 年ごろに追記され (第 2701 条)、これにより、第 18 編第 1 部第 121 章「電子データの保存および取引記録へのアクセス法」という章が新設されたことに始まるようである。そして、この不正アクセスに対する例外規定として、捜査令状、裁判所命令状または行政召喚状がある場合における例外が次々に追加されたようである。そのような規定が後からどんどんと追加されていき、第 18 編第 1 部第 121 章は、もともと刑法的だったものが、いつの間にか、日本における刑事訴訟法や通信傍受法の手続法のように、お化けのように成長していったものであるように見える。

米国クラウド法 (2018 年 3 月 23 日) は、第 18 編第 1 部第 121 章「電子データの保存および取引記録へのアクセス法」の多くの部分を改訂、追記する形で制定されたようである。米国クラウド法の法文自体は、米国議会の Web サイトの議事録で見ることができる[①]。しかし、これは日本の法令改定と同様のあの読みにくい差分表記であり、これだけを読んでも意味はよくわからない。元から存在する第 18 編第 1 部第 121 章全体を、「U.S. Code」と呼ばれる六法全書のようなものの上で読んで始めて、ようやく、意味がわかるようになっている。ちょうど外国人が日本の国会の Web サイトに掲載されている法律改正案を読んでも全く意味が分からないのと同じである。

米国クラウド法を構成する、第 18 編 121 章 「電子データの保存および取引記録へのアクセス法」について、その趣旨を日本語にしてまとめてみたものを以下に記す。注意として、以下は正確な日本語訳ではなく、パブリッククラウド事業者や、これに対して裁判所捜査令状や裁判所命令状、または行政召喚状の発行を申請する米国連邦政府または州政府の職員の視点で見て必要な部分のみを抜き出した抜粋である。また、元々の法文はクラウドサービス事業者のデータのみでなく電気通信事業者の取り扱う通信記録も含むものであるが、今回はその点は省略して、クラウドサービス事業者に関する部分だけ抜き出して、分かりやすいように記載している。なお、条文上は、クラウドサービス事業者は、"Remote Computing Service" の "Provider" と記載されている。"Remote Computing Service" の定義は、「電気通信回線を介したコンピュータによるストレージまたはデータ処理サービスの公衆提供役務」とされている。

【米国クラウド法の主要部分の日本語要約】

第 18 編 121 章 (電子データの保存および取引記録へのアクセス法)
第 2703 条 契約者に係るデータの開示義務
(a) 略
(b) クラウドサービスのデータ

① https://www.congress.gov/bill/115th-congress/house-bill/4943/text

(1) 政府機関 (注: 条文によると、米国政府の省庁およびすべての州政府または政治部門とされる。) は、クラウドサービス事業者に対して、以下のいずれかの手順により、(2) に係るデータ内容の開示を命じることができる。

(A) 捜査令状の発付を受けている場合は、クラウドサービス契約者に対する通知を行なう必要はない。

(B) 以下のいずれかの場合は、クラウドサービス契約者に対する通知を行なう必要がある。ただし、第 2705 条により通知を延期させることができる。

(i) 連邦法または州法により認められた行政召喚状、または連邦裁判所または州裁判所による裁判所召喚状がある場合。

(ii) 後掲の (d) に係る裁判所命令を取得する場合。

(2) 上記 (1) は、当該サービスにおいて保存または維持される下記各号の有線または電気通信サービスに対して適用される。

(A) クラウドサービス契約者の委託を受け、クラウドサービス契約者からの受信データまたは受信データに基づいたコンピュータ処理によって作成されるデータに係るサービス。

(B) クラウドサービス事業者がデータの保存またはコンピュータ処理の実施以外の目的でそのデータ内容にアクセスすることが契約者によって許可されていない場合においては、クラウドサービス契約者に対して純粋にストレージまたはコンピュータ処理を提供するサービス。

(c) 略

(d) (b) または (c) における裁判所命令は、管轄権のある裁判所であればどの裁判所でも発行できる。政府機関は、対象データが進行中の調査に関して関連性がありかつ重要であると信じるに足る合理的根拠を示す必要がある。クラウドサービス事業者は、裁判所に異議申立てが可能である。異議申立てがあった場合、裁判所は、開示請求される情報や記録の分量が著しく多大であるか、そのような命令に従うことが当該クラウドサービス事業者に著しい負担を生じさせる場合は、当該命令を破棄するか、または変更することができる。

(e) 本章に基づきデータを政府にデータを開示するクラウドサービス事業者は、訴訟から免除される。裁判所の命令、捜査令状、召喚状、法的認可または証明に基づいてデータを開示したことについて、クラウドサービス事業者、役員、従業員、代理人またはその他データの開示の実施者、施設の提供者または支援者に対して、いかなる裁判所に対しても訴えることはできない。

(f) 略

(g) 略

(h) 外国の判断の尊重

(1) 定義

(A) 「適格外国政府」とは、米国と第 2523 条に基づく行政協定を締結しており、かつ、電気通信サービスやクラウドサービスに関して以下の (2) および (5) と実質的に同等な手続法を制定する国をいう。

(B) 「米国人」とは、米国市民、米国永住権者、大部分の社員が米国市民または米国永住権者である権利能力なき社団および米国で設立された法人をいう (第 2523 条)。

(2) 破棄または変更を求める異議申立て

(A) クラウドサービス事業者は、以下の各号のいずれにも該当すると認める合理的な理由がある場合、裁判所に対し法的手続を破棄または変更することを求める異議申立てを行なうことができる。

(i) 対象となるクラウドサービス契約者が「米国人」でなく、かつ、米国内に居住していないこと。および

(ii) 開示の実施により、クラウドサービス事業者が適格外国政府の法律に違反する重大な危険が発生すること。この申立ては、クラウドサービス事業者が命令を受けた時から 14 日以内に提出されなければならない。この破棄を申立てる権利は、その他の破棄または抗弁に係る法的基礎を損なうものではないが、「適格外国政府」に関連する法への抵触を理由に破棄を申立てる唯一の根拠である。

(B) 裁判所は、(A) の申立てを受領した場合、政府機関側に対して反論の機会を与える。

裁判所は、以下の各号のいずれにも該当すると認定した場合に限り、必要に応じて法的手続を破棄または変更するものとする。

(i) 義務付けられようとする開示が「適格外国政府」の法律に違反すること。

(ii) 総合的に判断した結果、正義の利益のために、法的手続を変更または破棄すべき状況であること。

(iii) クラウドサービス契約者が「米国人」でなく、かつ、米国内に居住していないこと。

(3) 裁判所は、上記 (2) (B) (ii) を判断するにあたり、下記の各号を適切に酌量しなければならない。

(A) 開示を要求しようとしている政府機関の調査上の利益を含む米国の利益。

(B) 本来禁止されている開示を防止しようとする「適格外国政府」の側の利益。

(C) クラウドサービス事業者に課される矛盾した法的要求の結果、当該事業者またはその従業員が処罰される可能性、程度およびその処罰の性質。

(D) 対象となるクラウドサービス契約者の所在地および国籍、米国との結びつきの性質および程度、外国政府からの捜査要請 (第 3512 条) に基づく場合は契約者と当該外国政府とのつながりの性質および程度

(E) クラウドサービス事業者と米国との関係性

(F) 開示請求情報の調査上の重要性

(G) 開示対象の情報について、より迅速で、効果的かつ過度でない他の手段の可能性。

(H) 外国政府からの捜査要請 (第 3512 条) に基づく場合は、その要請元外国政府の捜査上の利益。

(4) クラウドサービス事業者は、裁判所が第 2705 号 (a) (2) で示されている不利益な結果を予防するために直ちに開示する必要があると判断した場合をのぞき、異議申立て係属中は、対象データを保存することで足り、直ちに開示する必要はない。

(5) 「適格外国政府」との相互主義 (逆方向の手続) に関する規定。

第 2705 条 通知の延期

(a) 通知の延期

(1) 政府機関は、第 2703 条 (b) に基づく通知について、以下の場合は、通知の延期をすることができる。

(A) 政府機関が裁判所命令を請求する場合、第 2703 条 (b) に基づく通知を最大 90 日間延期する命令を求めることができる。裁判所は、下記 (2) に規定される不利益な結果をもたらす可能性があると判断した場合には、この申し出を認めるものとする。

(B) 政府機関が行政召喚状または裁判所召喚状を取得した場合、召喚状の存在を通知すると下記 (2) に規定される不利益な結果をもたらす可能性がある旨を「政府機関の責任者」が書面にした場合は、第 2703 条 (b) に基づく通知を最大 90 日間延期することができる。

(2) 上記 (1) における不利益とは、次のいずれかを意味する。

(A) 個人の生命身体の安全に対する危険。

(B) 刑事訴訟を免れるおそれがある場合。

(C) 証拠の破壊または改ざんがなされるおそれがある場合。

(D) 証人となる者への脅迫のおそれ。

(E) その他、調査を著しく困難とし、または裁判を不当に遅延させること。

(3) 政府機関は、上記 (1) (B) の書面の申請な写しを保管しなければならない。

(4) 通知の延期は、裁判所による命令、または政府機関による必要性の証明により、さらに延長できる。ただし、それぞれの延長の期間は、90 日以内とし、下記 (b) への該当を要件とする。

(5) 上記 (1) または (4) の通知の延期期間が満了した場合、政府機関は、対象のクラウドサービス契約者に、下記の内容を記載した書面を送達するか、書留郵便または普通郵便で交付しなければならない。

(A) 法の執行に係る調査の性質を合理的かつ具体的に記載する。

(B) 以下の情報。

(i) クラウドサービス事業者が、対象のクラウドサービス契約者のために保持する情報が当該政府機関に提供されたことおよびその日時。

(ii) 通知が延期されたものであること。

(iii) 当該通知の延期の根拠となる認定または決定を行なった政府機関または裁判所はどこか。

(iv) この法律のいずれの規定により、その通知の延期が認められたのか。

(6) 本款における「政府機関の責任者」とは、警察本部または地方警察事務所の警部、警部補またはこれに相当する職員、または検察庁本部または地方検察庁の検事長、第一級検事補またはこれに相当する職員を意味する。

(b) 政府によるデータアクセス対象者に対する通知の禁止命令

政府機関は、第 2703 条に基づき情報開示命令を求めるに際して、第 2703 条 (b)(1) の規定に基づくと通知が不要な場合、または、第 2705 条 (a) に従ってかかる通知を遅延させることができる範囲において、捜査令状、召喚状または裁判所命令が向けられたクラウドサービス事業者に対し、裁判所が適切と考える期間内は、捜査令状、召喚状または裁判所命令の存在を外部に通知しないよう命じる裁判所命令を申請することができる。裁判所は、捜査令状、召喚状または裁判所命令の存在をデータアクセス対象者に通知することが以下の結果を招く合理的理由があると判断した場合は、そのような命令を下すものとする。

(1) 個人の生命身体の安全に対する危険。
(2) 刑事訴訟を免れるおそれがある場合。
(3) 証拠の破壊または改ざんがなされるおそれがある場合。
(4) 証人となる者への脅迫のおそれ。
(5) その他、調査を著しく困難とし、または裁判を不当に遅延させること。

第 2708 条 行政救済の独占性

この章に係る憲法違反に対する救済および制裁は、この章で規定されている行政救済策を、唯一の司法上の救済策とする。

第 2713 条 データ保存と開示の要求

クラウドサービス事業者は、当該事業者が所有、保管、管理する電子データおよび契約者に関する記録その他の情報を、当該データ、記録またはその他の情報の所在地が米国内であるか米国外であるかにかかわらず、本法律に基づき、保存、バックアップ、または開示する義務を履行しなければならない。

このように、米国クラウド法を日本語に要約してみると、これは、急に親しみやすい条文としてわれわれの前に姿を現わすのである。大体の内容は、日本の刑事訴訟法における裁判所による捜査令状、または行政による捜査事項照会書の規定とよく似ている。このような具体的な条文を読めば、クラウド法、クラウド法と言って何か得体の知れないお化けが出たかのように恐れる必要はない。原文を読めば、誰でも、どのようなリスクがあるのか具体的に分かる。

前述のとおり、クラウド法は 2018 年 3 月 23 日に米国で成立したが、これは既存の第 18 編 121 章を改訂するものであった。クラウド法の趣旨は、

"Clarifying Lawful Overseas Use of Data Act" という標題のとおり、米国から見て外国にあるデータに米国連邦政府または米国州政府がアクセスすることを合法化するための規定を挿入することである。クラウド法のうち、最も重要な部分は、上記の日本語要約の最後の第 2713 条である。この条は、(米国主権下にある) すべてのクラウドサービス事業者は、外国に物理的に所在するクラウドサーバー上の契約者データを政府に対して差し出すことを義務付けるものである。クラウド法が制定される前は、米国連邦政府または米国州政府が、米国系パブリッククラウド事業者に対して、米国外のサーバーに保存されている顧客のデータを提出させることが可能かどうか、明確でなかった。2016 年の Microsoft Corporation 対米国連邦政府訴訟[①] (政府の捜査令状が無効であることの確認を目的とした訴訟) では、米国連邦控訴裁判所 (日本の高等裁判所に相当) は、第 18 編 121 章の保護法益は契約者のプライバシー権であり、保護されるデータの所在地が外国にある場合は、司法共助条約に基づいて提出を求める必要があるとして、捜査令状は無効と認め、連邦政府を一旦敗訴させた (2016 年 7 月 14 日)。これに対して連邦政府側が連邦最高裁判所に上告していたところ、2018 年 3 月 23 日に米国クラウド法が成立してしまった (これにより、訴訟は却下された) というものである。米国クラウド法成立により、米国の管轄下にあるパブリッククラウド事業者は、Microsoft 事件のような場合においては、米国連邦政府または米国州政府が、裁判所を通じて捜査令状または裁判所命令状を取得し、あるいは、政府機関が直接行政召喚状を発行したならば、パブリッククラウドサービスの契約者のデータを政府に引き渡す義務があることが、ついに、初めて、法文に明記されたのである (第 18 編 121 章 2713 条)。

米国クラウド法の効果と、米国連邦政府または米国州政府によるクラウドサービス事業者への開示請求の手続については、上掲の法文趣旨のとおりであり、極めて明快である。米国系パブリッククラウド事業者は、日本のデータセンタ内の対象データが保存されているクラウド基盤に管理者特権を用いてリモートアクセスし、遠隔操作で、データ本体を、光ファイバ回線を経由して米国本土まで転送し、米国本

① Microsoft Corp. v. United States, 829 F.3d 197 (2016).
https://www.leagle.com/decision/infco20160714063

土でそのデータを米国政府機関にコピーして引き渡さなければならなくなった。第 2703 条 (b) (1) によると、このデータ提出命令は、(A) 裁判所を通じて取得する捜査令状、(B) (i) 行政召喚状、または裁判所召喚状、(ii) 裁判所命令、のいずれかの取得により可能となる。米国に所在するパブリッククラウド事業者の社員がこれに従わないと、提出命令の目的が刑事捜査である場合は司法妨害罪 (第 18 編第 73 章第 1512 条 (c)) に問われ最大 20 年の拘禁刑に処せられるおそれがあり、また、裁判所の令状または命令に違反すると、裁判所侮辱罪 (第 18 編第 21 章第 401 条) に問われ最大 6 ヶ月の拘禁刑に処せられるおそれがある。このような間接強制により、パブリッククラウド事業者の社員は、命令に従って顧客データを強制的に開示させられることになる。

ガバメント用クラウドが米国系パブリッククラウドの基盤上に構築された場合、この米国クラウド法が存在する以上、上記の手続のとおり、たとえそのデータが物理的に日本国内のデータセンタに存在したとしても、米国連邦政府または米国州政府の権限のある職員は、日本の各行政機関が有する日本国民の個人情報を含むデータ (たとえば、IaaS の VM の仮想ディスクイメージ) を強制的に取得することが可能となる。これは強制的取得であるので、日本国政府の承諾も、実際の当該クラウド領域のユーザーである行政機関 (地方公共団体等) の承諾も不要である。また、後述するとおり、事前の通知なくデータが取得されることが可能な法制度となっており、この場合、日本政府または日本の地方公共団体には、米国および米国系パブリッククラウド事業者に対して異議申立ての機会がそもそも与えられていない。加えて、事後の通知も延長することが可能であり、事実上、データが米国政府によって強制取得されたことすら気付かない状態が継続し得るのである。

このように、米国クラウド法の対象となり得る米国系クラウドサービス上にガバメント用クラウドが構築され、これを日本政府または日本の地方自治体が利用し、日本国民の個人情報が保存された場合、住基ネット事件最高裁判例の基準に照らすと、場合によっては、憲法違反となる現実的リスクが発生する。住基ネット事件最高裁判例基準 (3) は、システム技術上個人情報が容易に漏えいする具体的危険がないことを合憲要件として明確化した。米国クラウド法によると、前述のとおり、

システム技術上、個人情報を含むクラウド上のユーザーデータがいつでも米国連邦政府または米国州政府の職員によって容易に取得されてしまうこととなる。米国連邦政府または米国州政府は、日本法上、これらのデータの取得行為について、何らの正当性を有さない他人 (第三者) である。そうすると、個人情報を含むデータが、そのような「第三者」にいつでも容易に取得され得る状態となっていることとなり、これでは、基準 (3) を満たさなくなり、違憲となるリスクが生じるのである。

第 5 節　ガバメント用クラウドに係る米国クラウド法対抗手法を述べた国会答弁（2021 年、2022 年）の提案手法の分析

上述の米国クラウド法の問題について、日本国の議会では、過去少なくとも 3 回にわたり (衆議院で 2 回、参議院で 1 回)、議員から政府に対して質問があり、討論が行なわれたようである。その議事録の抜粋、趣旨の要約を以下にまとめた。なお、もともとの議事録が極めて長大なものであるため、抜粋の過程で、字句や表現は文脈に沿う形で一部修正しているが、意味に変化はないように注意している。なお、政府側の答弁内容において、後の検討に用いるため、① ～ ⑤ の番号を振っている。

1　米国クラウド法に関する国会答弁の要約

【第 204 回国会 参議院 内閣委員会 第 17 号 2021/5/11[①]】

議会 (241)「日本国内のデータセンタであれば、クラウド事業者が米国資本であっても、米国による執行管轄権は完全に排除されるのだろうか？ 2018 年 3 月に、米国クラウド法が成立している。これによると、たとえ日本国内のデータセンタであっても、米国が管轄権を有する米国系パブリッククラウド事業者については、米国当局の執行管轄権がある、ということになるのではないか？」

政府 (242)「米国クラウド法について調べたところ、データが米国外にある場合でも、米国による犯罪捜査において米国裁判所が発付する令状があれば、米国政府が米国の管轄権に服するプロバイダーに対して、(当該米国外に保存されている) データの提供を求めることが可能であるようだ。」

議会 (243)「そうすると、(日本の) 国内法が優先されることを含めた法規制、あるいは、クラウド事業者との確約、文書上の取り決めが求められるのではないだろうか？」

政府 (244)「① 仮に (米国政府による米国系パブリッククラウド事業者への) 要請 (開示命令) があった場合でも、無断で日本政府の情報が提供されることを避け

① https://kokkai.ndl.go.jp/#/detail?minId=120414889X01720210511&spkNum=241

るため、クラウド事業者の異議申立てや日本政府への (事前の) 通知を求めることで、対策が可能である。② また、(米国政府に) 情報が提供されても、(米国政府が) その内容にアクセスできないように暗号化措置を講じることで、対策が可能である。」

議会 (245)「やはり、日本国内法が優先されるという何らかの明示された米国系パブリッククラウド事業者との取り決めや、米国との関係で、日本政府に (事前の) 通知なく (米国系パブリッククラウド事業者に) 情報提供を求めることはないという約束が必要である。政府もその危険性、危惧を認識しているではないか。」

政府 (246)「契約を検討している米国パブリッククラウドは、政府情報システムのためのセキュリティ評価制度である ISMAP に登録されたサービスである。③ 契約上は、一切の紛争は日本の裁判所が管轄し、日本法を準拠法とする予定である。(だから、安心である。)」

【第 208 回国会 衆議院 内閣委員会 第 12 号 2022/03/25[①]】

議会 (114)「米国クラウド法によると、米国政府が要求すれば、(日本のデータセンタにある米国系パブリッククラウド事業者の保管する) 日本人の個人情報が米国政府に開示される可能性がある。この場合、日本政府が米国企業に対して開示を阻止することはできないのではないか？」

政府 (115) 「④ 米国クラウド法は、米国政府に無制限なアクセスを認めるものではなく、(米国のための) 犯罪捜査という極めて限定された場合において、(米国の) 裁判所が発する (米国の) 令状 "など" に基づき、(米国法上) 適切に手続が行なわれ、米国系パブリッククラウド事業者に対して情報提供の要請 (開示命令) が行なわれるというものだと思う。① 万一こういった要請 (開示命令) があった場合、米国系パブリッククラウド事業者から日本国政府に (事前の) 通知が行なわれて、当該事業者等と協議の上、適切に対応するというふうにしている。② さらに、日本国政府はデータを暗号化を行ない、仮に誰か (米国政府) がデータを取得しても、

[①] https://kokkai.ndl.go.jp/#/detail?minId=120804889X01220220325&spkNum=114

(米国政府は) その内容を読み取ることができない措置を講じている。」

議会 (116)「いろいろ政府の方でも対策を講じていただいていることは分かった。」

【第 210 回国会 衆議院 内閣委員会 第 7 号 2022/11/11[①]】

議会 (100)「2018 年に米国で施行された米国クラウド法においては、米国政府は、米国内の本拠地を持つ企業 (米国系パブリッククラウド事業者) に対して、米国外に保存されているデータを合法的に閲覧、差押請求を行える可能性がある。仮に米国捜査当局からガバメント用クラウド上の日本国民に対するデータの開示が求められた場合は、開示しなければならないのか？ それとも、日本の主権を主張できる (開示を拒絶できる) のか？ 確認をしたい。」

政府 (101)「④ 米国クラウド法は、米国政府に無制限なアクセスを認めるものではなく、(米国のための) 犯罪捜査という極めて限定された場合において、(米国の) 裁判所が発する (米国の) 令状 "等" に基づき、事業者に対して開示要請 (開示命令) が行なわれるものである。そのため、ガバメント用クラウドについては、そもそも当該データ提供の要請 (命令) が行なわれることは想定し難い。⑤ しかし、万一米国クラウド法に基づく要請 (命令) があった場合は、米国系パブリッククラウド事業者から日本政府に (事前の) 通知が行なわれ、外国主権免除法に基づく主権免除の適用を米国に求めることで、開示が行われないものと考えている。」

議会 (102)「ありがとうございました。」

2 政府による米国クラウド法に係る対策提案手法の整理

上記議事録における政府答弁をまとめると、日本のガバメント用クラウド (あるいは、その前の政府共通プラットフォーム) に関わる米国クラウド法に関する日本国民

① https://kokkai.ndl.go.jp/#/detail?minId=121004889X00720221111&spkNum=100

の個人情報保護が米国政府によって米国クラウド法を用いて取得されてしまう危険は、以下のような提案手法 ① ～ ⑤ によって予防または排除できる (したがって、ガバメント用クラウドにおいて米国系パブリッククラウド事業者を利用しても、個人情報保護の問題は発生しない) という理論が見えてくる。提案手法 ① ～ ⑤ は、いずれも、上記議事録の要約の本文中の番号に対応している。

【提案手法 ①】 日本政府または日本の地方公共団体の有するクラウド上のデータに関し、米国政府から米国系パブリッククラウド事業者へのデータ提供命令があった場合、日本政府または日本の地方公共団体の有する国民の個人情報が米国政府に提供されることを避けるため、米国系パブリッククラウド事業者の異議申立てや日本政府への事前の通知を求め、そのような通知があったならば、日本政府が米国系パブリッククラウド事業者と協議し、"適切に対応" する。(第 204 回国会 参議院 内閣委員会 第 17 号 2021/5/11、第 208 回国会 衆議院 内閣委員会 第 12 号 2022/03/25)

【提案手法 ②】 仮に米国政府がデータを取得できてしまったとしても、米国政府がその内容にアクセスできないように、"暗号化措置" を事前に講じているので、米国政府へのデータ漏えいの危険は防止できる。(第 204 回国会 参議院 内閣委員会 第 17 号 2021/5/11、第 208 回国会 衆議院 内閣委員会 第 12 号 2022/03/25)

【提案手法 ③】 日本政府と米国系パブリッククラウド事業者との契約上、一切の紛争は "日本の裁判所が管轄" し、"日本法を準拠法" とする。(第 204 回国会 参議院 内閣委員会 第 17 号 2021/5/11)

【提案手法 ④】 米国クラウド法は、米国政府に無制限なアクセスを認めるものではなく、米国のための犯罪捜査という極めて限定された場合において、米国の裁判所が発する米国の令状 "等" に基づき、米国系パブリッククラウド事業者に対して開示命令が行なわれるに過ぎないから、脅威は限定的であると考える。(第 208

回国会 衆議院 内閣委員会 第 12 号 2022/03/25、第 210 回国会 衆議院 内閣委員会 第 7 号 2022/11/11)

【提案手法 ⑤】 万一、米国クラウド法に基づく命令があった場合は、米国系パブリッククラウド事業者から日本政府に事前の通知が行なわれるであろう。この場合、"外国主権免除法に基づく主権免除の適用" を米国に求めることで、開示を阻止できる。(第 210 回国会 衆議院 内閣委員会 第 7 号 2022/11/11)

上記議事録をみる限り、3 名のいずれの国会議員の先生方も、日本のガバメント用クラウド (あるいは、その前の政府共通プラットフォーム) に関わる米国クラウド法に関する日本国民の個人情報保護に係る問題を指摘したが、政府の答弁において説明された提案手法 ① ～ ⑤ により、一応、納得されたという流れになっている。

このように、今のところ、米国クラウド法に関しては、国会において大きな問題とはなっていない。しかしながら、仮に ① ～ ⑤ の対策内容が、問題を解決するために不十分であると認識されれば、これは、再び、国会等で、大きな問題になり得る。したがって、われわれは、上記の国会議事録において示された政府側の提案手法 ① ～ ⑤ の対策内容を、今すぐ、より精密に確認し、不十分な点がないかどうか、慎重にこれを検討する必要がある。万一、提案手法 ① ～ ⑤ に不十分な点があれば、国会等で改めてこれが指摘されるより前に、われわれは、再度対策を施し、今後の指摘に対して万全の体制で応じるべきである。

3　検討

それでは、以下で、提案手法 ① ～ ⑤ について慎重に検討をしていくことにしよう。

(1) 【提案手法 ①】日本政府または日本の地方公共団体の有するクラウド上のデータに関し、米国政府から米国系パブリッククラウド事業者へのデータ提供命令があった場合、日本政府または日本の地方公共団体の有する国民の個人情報が米国政府に提供されることを避けるため、米国系パブリッククラウド事業者の異議申立てや日本政府への事前の通知を求め、そのような通知があったならば、日本政府が米国系パブリッククラウド事業者と協議し、"適切に対応" する（第 204 回国会 参議院 内閣委員会 第 17 号 2021/5/11、第 208 回国会 衆議院 内閣委員会 第 12 号 2022/03/25）

この提案手法が有効であるかどうかを検討するためには、米国政府に対する米国クラウド法に基づく日本のガバメント用クラウド上のデータ開示命令が出た場合、(a) 米国系パブリッククラウド事業者に対してデータ開示命令に対する異議申立てを契約上義務付けることができるか、(b) 当該異議申立てがなされれば、それは日本の裁判所で正しく審理されることが保障されるのかそれとも米国の裁判所で審理されてしまうのか、(c) 当該異議申立てが仮に米国の裁判所で審理されるとして命令の破棄は確実に認められるのか、(d) 異議申立てをするために、データ開示命令が出た後開示の実施までに十分な期間を前置して契約者 (日本政府) に対して米国系パブリッククラウド事業者から確実に事前通知を受けることができる法的担保があるか、(e) 仮に事前通知を受けたとして日本側が米国系パブリッククラウド事業者と "協議" することに意味はあるのか、の (a) ～ (e) についてそれぞれ分析を施す必要がある。

(a) 米国系パブリッククラウド事業者に対してデータ開示命令に対する異議申立てを契約上義務付けることができるか

日本政府と米国系パブリッククラウド事業者との契約において、「米国クラウド法に基づくデータ開示命令があった時は、米国に対して、必ず異議申立てを行なう」ことを日本政府が事業者に対して義務付けることはできると思われる。これは単に米国当局から米国系パブリッククラウド事業者に対して開示命令が発付されたことを停止条件とする、その都度の、異議申立ての行為 (たとえば、異議申立書を裁判所に提出する行為) を契約上の債務として通常の作為義務として課すことであり、不法な行為を強いるものではないので、契約上は有効である。異議申立ての根拠は、米

国法第 18 編 121 章 2703 条 (d) に規定されているので、データ開示命令の正当性の有無について米国系パブリッククラウド事業者がその裁量で異議申立てを行なうか否かを決定することを明示的に禁止し、"必ず" 異議申立てをしなければならない旨を契約上規定すればよい。

(b) 当該異議申立てがなされれば、それは日本の裁判所で正しく審理されることが保障されるのかそれとも米国の裁判所で審理されてしまうのか

仮に (a) で日本政府が米国系パブリッククラウド事業者にその都度の異議申立てを義務付けたとして、米国系パブリッククラウド事業者がこれに従って毎回異議申立てをしたとしよう。異議申立てが行なわれただけでは、もちろん、全く意味は生じない。異議申立てによって、米国政府によるデータ取得を阻止するためには、その異議申立てが認められ、米国法第 18 編 121 章 2703 条 (b) (1) (A) の捜査令状の取消しまたは無効、あるいは (B) (i) の行政召喚状または裁判所召喚状もしくは (B) (ii) の裁判所命令の取消しまたは無効、が裁判所によって裁決される必要がある。問題は、「裁判所」とは日本の裁判所を指すのか、それとも、米国の裁判所を指すのかという点である。

行政機関に対する個人情報をみだりに第三者に開示されない自由は、日本国憲法 13 条で保障される権利であり、また、日本国の法律に基づいて保障される権利である。住基ネット事件最高裁判例基準 (3) の「個人情報の漏えい」を阻止し、また、行政機関の保有する個人情報の保護に関する法律 6 条 (安全確保の措置) 1 項、8 条 (利用及び提供の制限) 1 項で規定されている保護の状態を維持するためには、そのような異議申立ては、必ず、日本法に基づいて、日本の裁判所で審理されなければならない。なぜならば、米国の裁判所で審理され、異議申立てが認められるか否かが決定されたとしても、それは、米国の主権者がデータ開示を決定しているに過ぎないから、その決定には日本の主権者からみて、何ら正統性はないためである。

しかし、実際には米国クラウド法に基づくデータ開示命令に対する米国系パブリッククラウド事業者による米国に対する異議申立ては、米国法に従い、米国の裁判所でのみ審理されてしまうこととなる。データ開示命令が米国の主権の及ぶ領域内で適法に行なわれる以上は、米国裁判所の管轄権が及ぶためである。そして、異議

申立てに対する米国の裁判所によるいかなる決定があったとしても、その米国の裁判官たちは、日本国憲法の下で日本の主権者によって任官されたものでない以上、その決定に基づいてデータ開示命令が履行されれば、それは日本に対する主権侵害となる。よって、(a) で述べた異議申立てを必ず義務付けることのみによっては、日本政府または日本の地方公共団体が国民に対して保障しなければならない行政機関に対する個人情報をみだりに第三者に開示されない自由権に対する第三者(米国) からの侵害に対する予防措置を講じているということができず、住基ネット事件最高裁判例基準 (3) の「個人情報の漏えい」を阻止し、また、行政機関の保有する個人情報の保護に関する法律 6 条 (安全確保の措置) 1 項、8 条 (利用及び提供の制限) 1 項で規定されているセキュリティの保護を提供していることにならない。ただし、例外として、異議申立てが行なわれれば、必ず米国裁判所によって命令の破棄が確実に認められる法制度的な保障が存在するのであれば、話は別である。これについては、(c) で後述する。

(c) 当該異議申立てが仮に米国の裁判所で審理されるとして命令の破棄は確実に認められるのか

上記 (b) により、米国クラウド法に対する米国系パブリッククラウド事業者による異議申立ては、常に米国の裁判所で審理されるとして、仮にそのような異議申立てがあれば必ずデータ開示命令の破棄が認められるのかどうかが重要である。もしそうであれば、(a) で述べた契約上の異議申立ての義務付けを施すだけで、確実に日本国民の個人情報の保障が提供されるためである。

しかしながら、実際には米国系パブリッククラウド事業者の異議申立てによる命令の破棄が認められる可能性は極めて低い。逆に、ほとんどの場合、米国系パブリッククラウド事業者の異議申立ては、米国裁判所によって、却下されることになると考えられる。

そもそも、米国クラウド法に基づいて米国連邦政府または米国州政府が米国系パブリッククラウド事業者に対して開示命令を出す際に必要な書類は何であろうか。これは、第 18 編 121 章 2703 条に詳しく規定されている。捜査令状、行政召喚状、裁判所召喚状、または 2703 条 (d) で特別に規定されている裁判所命令の

4 種類である。この中で特に重要となるのが、捜査令状と行政召喚状の 2 つである。以下、それぞれについて見ていく。

まず、第 18 編 121 章 2703 条 (b) (1) (A) で規定されている捜査令状について、これはだいたいどの程度の割合が司法判断を通過するのであろうか。これは、連邦裁判所についてのみであるが、統計データがある。例えば、2021 年には 32,282 件の捜査令状が捜査機関から連邦裁判所に申請されたが、そのうち、実に 99.5% が、裁判所によって認められているのである① (ただし、Delayed Notice Search Warrants と呼ばれる、被疑者に対して事前の通知を行なわずに発付される捜査令状の統計データである)。これは、ほとんど 100% に近い数字である。日本においても捜査令状の申請はほとんど認められるようであるが、米国でも同じ模様である。そして、これは一度司法審査を経て適法なものとして発付された捜査令状であるから、明白な違法がある場合をのぞき、異議申立てをしたところで、覆えすことはほとんど困難である。

次に、第 18 編 121 章 2703 条 (b) (1) (B) (i) の行政召喚状であるが、この行政召喚状というものは、捜査令状よりもさらに容易に利用される命令書である。これは、連邦法または州法に根拠がある限り、行政機関は、司法審査を経ずに簡単に発付できる命令書である。日本における行政調査権と同じようなものだと思われる。米国連邦最高裁判所は、米国の行政機関による召喚状による行政調査の権限は、その権限を過度に制限すると行政機関がその法的責任を遂行できなくなるおそれが高いことから、広範囲な権限を認めているのである②③④。

行政召喚状は、司法判断を経由せずに、米国連邦政府または米国州政府が発付することができるが、異議申立て等により司法審査を経て取消しまたは無効にすることが可能である。ここで、憲法修正 4 条 (捜査に対する市民のプライバシー権) に対する違憲審査基準が問題になる。審査基準が厳格審査であれば、日本政府が米国系パブリッククラウド事業者に日本国民のプライバシー権利を理由として異議申立て

① https://www.uscourts.gov/statistics-reports/delayed-notice-search-warrant-report-2021
② United States v. LaSalle Nat'l Bank, 437 U.S. 298, 313 (1978)
③ United States v. Powell, 379 U.S. 48, 57 (1964)
④ Oklahoma Press Publishing Co. v. Walling, 327 U.S. 186, 209 (1946)

を求めた結果、米国裁判所は、行政召喚状を無効化してくれることが期待できる。ところが、実際には、これは絶望的である。米国連邦最高裁判所の判例[①]は、米国の行政機関による召喚状による行政調査の権限に係る、憲法修正 4 条 (捜査に対する市民のプライバシー権) による違憲審査基準について、厳格な基準を採用せず、「合理性の基準」を採用しているためである。具体的な司法審査基準として、(i) 行政調査の目的が合法であること、(ii) 召喚状で開示を要求される情報が目的に関連するものであること、(iii) 行政機関はその召喚状で認めている情報を未だ入手しておらず召喚状発付の必要性があること、(iv) 行政機関が召喚状を発付する際に必要な行政手続を履行したこと、の 4 点が判示されている。これはもう、ほとんど形式的審査といって良いものである。このように、米国最高裁は、行政召喚状の発付について、行政調査を行なおうとする米国行政機関の裁量を、最大限に認めてしまうのである。

上記のように、米国連邦政府または米国州政府の行政機関が、日本政府のガバメント用クラウド上のデータを対象として、データ開示を命ずるための捜査令状あるいは行政召喚状を発付することは極めて容易であり、これが行政機関によって次々に申請ないし発付されたならば、その都度、捜査令状については 99.5% もの確率で司法審査を通過してしまい、行政召喚状についてはゆるやかな違憲審査 (合理性の基準) によってやはり司法審査を通過してしまうことが、明らかになった。これにより、われわれは、とても心配になる。しかしながら、まだ希望はある。歴史的にみると、米国の裁判所は、政府による人権侵害を、憲法に基づいて積極的に阻止してくれることについて市民の信頼が厚い裁判所である、という評判があるではないか。そこで、われわれ日本人は、日本政府のガバメント用クラウド上のデータを対象として、いよいよ、米国行政機関による捜査令状あるいは行政召喚状の発付による米国クラウド法に基づくデータ開示命令が発付された場合において、パブリッククラウド事業者を経由して、憲法修正 4 条 (捜査に対する令状主義と市民のプライバシー権の保障) に対する侵害、すなわち憲法違反を理由として、米国裁判所に対して

① Securities and Exchange Com'n. v. Jerry T. O'Brien, Inc., 467 U.S. 735, 741-42 (1984)

開示命令の破棄を申立てれば、憲法審査によってこれを認めてくれるかもしれないという最後の希望をもって、米国に対して、抗告をしてみることになるのである。ところが、この最後のわずかな希望は、またもや、米国連邦最高裁判所判例によって打ち砕かれるのである。米国最高裁は、米国捜査官がメキシコでメキシコ人の被告人の自宅を捜索して入手した文書について、適法な捜査令状を取得せずプライバシー権 (米国憲法修正第 4 条) を侵害し違憲であるとして証拠からの排除を被告人が求めたことに関し、「問題は、米国憲法修正第 4 条が、非居住外国人が所有し外国に所在する所有物に対して、合衆国捜査官による捜索・押収に適用されるかどうかである。裁判所は、憲法修正第 4 条は、適用されないと判断する。」と明確に判示している①。

このように、米国連邦最高裁判所によると、米国外に住む日本人の人権である、捜査に対するプライバシー権 (米国憲法修正第 4 条、日本国憲法 13 条、35 条) は、米国政府に対しては、保障されないことになってしまっている。プライバシー権が米国裁判所に認められるのは、米国内の居住者か、または、米国市民に限られるのである。この問題は、米国クラウド法成立後、ヨーロッパにおいて GDPR との関係で問題とされ、大きく取り上げられている②。

よって、米国連邦政府または米国州政府の行政機関が、日本政府のガバメント用クラウド上のデータを対象として、データ開示を命ずるための捜査令状あるいは行政召喚状を発付したことについて、直ちに異議申立てが行なわれたとして、これが米国の裁判所で審理されても、データ開示命令の破棄が確実に認められるとは到底いえず、むしろ、明白な誤りや不合理性がある場合をのぞいては、ほとんどの場合で、異議申立ては棄却されることになると思われる。

米国クラウド法は、第 18 編 121 章 2703 条 (d) において、もう一種類の興味深い異議申立て原因を明文的に認めている。「裁判所は、開示請求される情報や記録の分量が著しく多大であるか、そのような命令に従うことが当該クラウドサー

① United States v. Verdugo-Urquidez, 494 U.S. 259 (1990)
② https://policyreview.info/articles/analysis/mitigating-risk-us-surveillance-public-sector-services-cloud

ビス事業者に著しい負担を生じさせる場合は、当該命令を破棄するか、または変更することができる。」という部分がそれである。「命令に従うことが当該クラウドサービス事業者に著しい負担を生じさせる場合」は命令の破棄または変更が可能であるとしたとき、その「著しい負担」として何が認められるか。例示として、「開示請求される情報や記録の分量が著しく多大である」場合が、明文で記載されているので、これに類するような著しい負荷が生じる場合であれば認められそうである。ところで、仮に米国系パブリッククラウド事業者と契約者との間の契約上、「データ開示命令には従わないこと」という契約があったとして、その契約に違反すると多額の違約金が課せられるという状態においてデータ開示命令に従わせられることが、「命令に従うことが当該クラウドサービス事業者に著しい負担を生じさせる場合」に該当するかどうかが、重要な問題となる。もしそのような契約上の義務付けが、第 18 編 121 章 2703 条 (d) の「負担」として認められたならば、それは、ガバメント用クラウドに関しては、日本政府にとってとても有利である。なぜならば、日本政府と米国系パブリッククラウド事業者との間の契約で、「データ開示命令には従わないこと」という契約をしておけば良いということになるためである。ところが、これは、実際には機能しないと思われる。それは 2 つの理由によると思われる。第一に、それは米国裁判所および米国法の視点からは単なる米国クラウド法の公法上の義務に対する脱法行為であり、認められないという理由が想定される。第二に、これが後述するより重大な問題を引き起こすものでもあるが、第 18 編 121 章 2703 条 (e) により、米国クラウド法に基づくデータ開示命令に従ったパブリッククラウド事業者に対しては、民事上の完全免責が与えられているのである。免責になる以上は、「著しい負担」は発生しないという判断となってしまうものと思われる。むしろ、「命令に従うことが当該クラウドサービス事業者に著しい負担を生じさせる場合」の部分に今一度より力強く注目すると、むしろ、これはガバメント用クラウドを運営する日本政府にとって、国民のプライバシー保護上で不利な結果を生じさせるのである。たとえば、ガバメント用クラウド上に、あるデータベースファイルがあるとしよう。このデータベースファイルには 3 人くらいの日本国民の情報がたまたま記録されているとしよう。このうちわずか 1 名

が、米国連邦政府または米国州政府の捜査員によって疑われている被疑者であるとする。データベースファイルはバイナリデータであり、その内容は、十分な負担をかけて分析すれば (データフォーマットの意味を理解した上で分析をすれば)、被疑者 1 名の情報のみを抽出できるとする。だが、その作業をも、米国政府側が、米国系パブリッククラウド事業者に依頼するとなると、それはまさに、「命令に従うことが当該クラウドサービス事業者に著しい負担を生じさせる場合」に相当するおそれが生じるのである。1 個のデータベースのバイナリファイル全体のデータコピーは、一瞬であり、そのコストとしては数円くらいしかかからない。だが、1 個のデータベースのバイナリファイルを意味的に分析し、3 人の個人情報のうちから 1 人を抽出する作業は、安く見積もっても、数十万円はかかるであろう。場合によっては、データフォーマットが特殊であるとか、古いバージョンのソフトウェアを用意しなければならないとして、数百万円が必要になる場合がある。このような著しい負担がかかるのを避けるため、第 18 編 121 章 2703 条 (e) の規定は、米国政府は、余分で無関係な 2 人分のデータをも含んだ 3 人分全部のバイナリデータベースファイルのコピーを要求する合理的な根拠となってしまうのである。予め無関係と分かっている残りの 2 人分のデータを含めたバイナリファイルをコピーさせることが、それらの 2 人分の令状主義に係るプライバシー権 (米国憲法修正第 4 条) を侵害するリスクがあるが、その 2 名のいずれも米国非居住者であり、かつ米国人でなければ、前述の米国最高裁判例に基づき憲法上の同条の人権は認められないので、米国の視点からは支障はなく、全く問題は生じないということになってしまうのである。

(d) 異議申立てをするために、データ開示命令が出た後開示の実施までに十分な期間を前置して契約者（日本政府）に対して米国系パブリッククラウド事業者から確実に事前通知を受けることができる法的担保があるか

米国系パブリッククラウド事業者からの米国連邦政府または米国州政府に対するデータの開示は、事実上の行為であり、一度開示されたら、取消すことが不可能となる。そうすると、米国連邦政府または米国州政府の行政機関が、日本政府のガバメント用クラウド上のデータを対象として、データ開示を命ずるための捜査令状

あるいは行政召喚状を発付した場合、米国クラウド法に基づく異議申立てを行なうには、当然、そのデータ開示命令が出た後、異議申立ての準備に要する十分な期間が前置され、そのデータ開示命令が発付された事実が、当該米国系パブリッククラウド事業者から日本国政府 (および、ユーザーが日本の地方公共団体である場合は、その団体) に事前通知される必要があることになる。なぜならば、仮に事前通知がなければ、日本政府および日本の地方公共団体が異議申立てを行なう契機が存在せず、異議申立ては不可能であるためである。

そこで、日本政府が、米国系パブリッククラウド事業者との間の契約において、米国連邦政府または米国州政府から米国系パブリッククラウド事業者に対するデータ開示命令が出た場合は、開示の実施までに十分な期間を前置して契約者 (日本政府) に対して米国系パブリッククラウド事業者から確実に事前通知をする義務を契約上の債務として明記して事業者と契約することにより、事前通知の担保が確保できるかどうかが問題となる。これについて、米国クラウド法は、第 18 編 121 章 2705 条 (b) において、「政府によるデータアクセス対象者に対する通知の禁止命令」をデータ開示命令に添付して発付することができることが規定されている。その条件は、(1) 個人の生命身体の安全に対する危険、(2) 刑事訴訟を免れるおそれがある場合、(3) 証拠の破壊または改ざんがなされるおそれがある場合、(4) 証人となる者への脅迫のおそれ、および、(5) その他、調査を著しく困難とし、または裁判を不当に遅延させること、のいずれかに該当すれば良いこととなっている。そして、大抵の刑事捜査事案は、(2), (3), (5) の要件を満たす。例えば、米国連邦政府または米国州政府の捜査員が、米国内において日本人が犯罪 (たとえば、ある日本人が、米国内で横領、詐欺、脱税、テロ、あるいは薬物の不法摂取等の犯罪を行なったと疑われている状況を考えてみるとよい。) を行なったようだと疑っている事案を考えてみよう。その日本人はいったん日本に帰国してしまっているが、米国捜査員としては、彼について犯罪の合理的疑いの証拠を有しており、彼が後日また米国にやって来たときに訴追することを予定しており、刑事証拠を収集したいと考えたとする。米国捜査員としては、その日本人に関する犯罪の証拠となり得る情報 (たとえば、「税務記録」、「健康保険記録」、「健康管理情報」、「図書館貸出履歴」等のシステムの情報) を、

日本国政府のガバメント用クラウド上に記録されている、日本政府または日本の地方公共団体のクラウド領域上のこれらのシステムのデータを取寄せることが最良であると判断したとする。この場合、データ開示命令に係る捜査令状または行政召喚状は、米国系パブリッククラウド事業者に示さなければならない。だが、米国系パブリッククラウド事業者を経由して他人 (日本政府、日本の地方公共団体、または当該日本人等) にその捜査状況が伝わると、その日本人被疑者によって (2) 刑事訴訟を免れるおそれ (3) 証拠の破壊または改ざんをなすおそれ (5) その他調査を著しく困難としまたは裁判を不当に遅延させるおそれ が生じ得ることは明白である。これを予防するために、米国捜査員としては、米国系パブリッククラウド事業者に対して、第 18 編 121 章 2705 条 (b) の「政府によるデータアクセス対象者に対する通知の禁止命令」をデータ開示命令に添付して発付することとなる。

この「政府によるデータアクセス対象者に対する通知の禁止命令」は、米国行政機関が、米国裁判所に申請して発付してもらう手順となっている。したがって、この命令は裁判所命令である。米国に所在するパブリッククラウド事業者の社員がこれに従わないと、提出命令の目的が刑事捜査である場合は司法妨害罪 (第 18 編第 73 章第 1512 条 (c)) に問われ、最大 20 年の拘禁刑に処せられるおそれがあり、また、裁判所の令状または命令に違反すると、裁判所侮辱罪 (第 18 編第 21 章第 401 条) に問われ、最大 6 ヶ月の拘禁刑に処せられるおそれがある。このような刑罰による間接強制により、米国系パブリッククラウド事業者の社員としては、いかに日本政府が顧客としての大得意先であるとしても、データアクセス対象者である日本政府に対して、データ開示命令が発付されたことを通知することは不可能である。この問題の本質は、日本政府と米国系パブリッククラウド事業者との間の民事契約上は、日本法に準拠し、日本の裁判所の裁判権に服すると書いてあるかも知れないが、その米国系パブリッククラウド事業者と米国政府との間の公法関係は、米国法に準拠してしまっていることにある。これでは、いくら日本政府と米国系パブリッククラウド事業者との間で事前通知の契約が締結されていても、決して履行を期待することはできず、その契約は無意味である。無意味であるばかりか、民事契約上は、不能を強いることはできないので、日本法に基づいて解釈しても、その

契約は、無効とみなされるリスクもある。

そもそも、前述 (c) の検討結果により、たとえ異議申立てを行なうことができたとしても、これによりデータの開示命令を阻止することはほとんど不可能であるという結論が導かれている。それでも、一応、原理上は異議申立てを行なえば阻止できる可能性はゼロではなかったのである。だが、上記のように、データ開示命令が出たことの通知が命令によって禁止されることから、異議申立てを行なうことはそもそも不可能となる。これにより、データ開示を阻止できる可能性は、もはやゼロとなってしまったのである。

（e）仮に事前通知を受けたとして日本側が米国系パブリッククラウド事業者と”協議”することに意味はあるのか

前述 (d) により、そもそも、事前通知の担保は事実上確保できなさそうであることが判明した。仮にこのことを捨象し、事前通知を受けることができたとして、政府の答弁のように、日本側が米国系パブリッククラウド事業者と "協議" することについて、何らかの効果があるのだろうか。

効果は期待できない。なぜならば、米国系パブリッククラウド事業者としては、すでに米国連邦政府または米国州政府からデータ開示命令の発布を受けた状態に陥っているのであり、いかに日本政府と米国系パブリッククラウド事業者との協議が行なわれ、米国系パブリッククラウド事業者として大得意契約先である日本政府を慮る誠意があったとしても、やはり米国系パブリッククラウド事業者としては、司法妨害罪や裁判所侮辱罪に問われるペナルティ（これは、米国本土において、物理的強制力によって、当該米国系パブリッククラウド事業者の社員や経営者の個人の身体に対して直接的に加わる）を避けるため、命令に応じざるを得ないためである。日本政府の申し出の "協議"、より実質的にいうと、データ開示命令に従わないでほしいという懇願に応じなかったとしても、単に日本政府または日本の地方公共団体との間での契約上の債務不履行責任が、あるいはこれにより不法にデータを開示されることになる対象となる日本国民との間の不法行為責任が発生するのみである。これらは、単なる金銭賠償問題である。司法妨害罪や裁判所侮辱罪に問われるペナルティの重さと比較して、とても軽いものである。

これに加えて、米国系パブリッククラウド事業者は、次のような方法で、実際にはそのような日本政府または日本国民からの金銭賠償に対する執行を容易に免れることもできそうである。すなわち、仮に日本の裁判所において日本法に基づいて債務不履行または不法行為に係るの賠償義務が認定されたとしても、被害者が、米国系パブリッククラウド事業者にその賠償を実際に請求する際には、米国系パブリッククラウド事業者が財産を有する米国で執行する必要が生じる (日本にめぼしい財産がない)。ところが、この場合、米国裁判所はその執行を承認しないのではないかと思われるのである。なぜならば、米国裁判所の立場では、その請求原因は、米国系パブリッククラウド事業者が米国クラウド法に基づいて適法に請求に従った結果生じたものである。そして、第 18 編 121 章 2703 条 (e) には、米国クラウド法に従った米国系パブリッククラウド事業者に対して、完全な民事上の免責を与える旨の規定が存在しているのである。これは極めて強力な規定である。最も極端な場合として、次の極端なケースを想像してほしい。ガバメント用クラウドを経由して、日本国民 1.2 億人すべての機微な個人情報が、米国系パブリッククラウド事業者が日本政府との契約 (米国政府に対する無断のデータ開示をしないこと) を、意図的に守らず、米国政府からの司法妨害罪や裁判所侮辱罪等のペナルティをおそれ、米国政府に対して米国クラウド法に基づいてデータを開示したことについて、「他人にデータを漏えいした」として、国民 1 人あたり平均 10 万円の慰謝料の賠償請求が向けられたとしよう。それによって当該米国系パブリッククラウド事業者が日本政府または日本国民に対して負う賠償義務の総額は、12 兆円という、とても高額な金額となる。ところが、米国法を基準にすると、第 18 編 121 章 2703 条 (e) によって、その 12 兆円の賠償責任は、なんと、すべて免責されてしまうのである。そして、米国法の第 18 編 121 章 2703 条 (e) は公序規定であると米国裁判所によって認定されることが予想される。なぜならば、米国クラウド法は公法であるが、第 18 編 121 章 2703 条 (e) による免責保護が提供されない限り、米国クラウド法に事業者たちが自主的に従わなくなるおそれが高くなるため、これを予防しなければならないためである。この理論により、米国裁判所は、いかに日本の裁判所が日本法に基づいてプライバシー侵害に係る賠償責任を認定

したとしても、これを承認せず、被害は決して救済されない。

このようなことは、誰にでも容易に予想されることである。そのため、米国系パブリッククラウド事業者が、いざ、(i) 米国クラウド法への遵守と、(ii) 日本法および日本での契約の遵守 の相反する局面に立たされた時には、合理的に、(i) を選択することになる。(ii) の選択は、まず考えられないのである。日本側が、この状況において、米国系パブリッククラウド事業者との間で "協議" を行なえば (ii) を選択してくれるかも知れないと期待することは、まったく非合理であり、そのような期待を基礎として企画決定された、ガバメント用クラウドに関する判断は、誤った判断であるとみなされると考えられる。後世によって、一体誰が誤った判断をしたのか、是正できるときに是正しなかったのかということが、いよいよ、追及されるときがきたら、そのときは、2023 年当時の専門家たちが誤った判断をしたのだと批判されるであろう。われわれは、それを、避けなければならない。今ならばまだ予防できるのである。

まとめ

上記 (a) ～ (e) を整理してみよう。

まず、確かに (a) の異議申立ての契約上の義務付けは可能であるが、(b) により米国の裁判所で審理されてしまうことになり、日本の司法権が及ばず、プライバシー権の侵害の予防が不可能であることが分かった。そして、(c) により、米国クラウド法に係るデータ開示命令の捜査令状の司法審査通過割合も、行政召喚状の違憲審査基準も、極めてゆるやかであり、事実上の歯止めにならないこと、そもそも米国連邦最高裁は非居住者の外国人に対して令状主義に係るプライバシー権利を憲法上認めていないことが明らかとなった。加えて (d) により日本政府が期待している事前通知については、実際には米国クラウド法上禁止命令が発付される可能性が十分あり、禁止命令が出た場合は事前通知を受けることが不能となり、異議申立てがそもそも不可能であることが明らかとなった。(e) に関して、日本政府と米国系パブリッククラウド事業者との間の米国クラウド法に係る "協議" は、個人情報に対する権利侵害を防ぐために全く無意味であることが分かった。

このように、提案手法 ① は、実際には機能しない可能性が明らかとなった。そこで、われわれは、残された提案手法 ② ～ ⑤ に期待するしかない。

(2) 【提案手法 ②】 仮に米国政府がデータを取得できてしまったとしても、米国政府がその内容にアクセスできないように、"暗号化措置" を事前に講じているので、米国政府へのデータ漏えいの危険は防止できる。(第 204 回国会 参議院 内閣委員会 第 17 号 2021/5/11、第 208 回国会 衆議院 内閣委員会 第 12 号 2022/03/25)

これは、誠に素晴らしいアイデアである。提案手法 ① がすでに無力であることが判明した以上 (そして、後述するように、提案手法 ③ ～ ⑤ も機能しないと思われる以上)、我々は、もはや、この暗号化のアイデアを頼りにするしかないのである。

注意しなければならない点として、暗号化の手法が機能するためには、米国パブリッククラウドに保管されるすべてのデータは、確実に、クライアント側暗号化を施されている必要がある。そして、その暗号鍵は、決して米国パブリッククラウドのいずれかの領域に保管されてはならないことになる。なぜならば、仮に暗号鍵がいずれかの米国パブリッククラウド上に、平文で、または復号化可能な形式で、保管されていたとしたら、米国連邦政府または米国州政府の職員は、米国クラウド法を用いて、データと、暗号鍵の両方を容易に取得することができてしまうためである。このことについては、「資料③」のクライアント側暗号化で詳しく説明をした。だが、同資料は、前述のとおり、サイバー攻撃者を主たる脅威であると想定して記載したものである。同資料を作成した際には、米国クラウド法に際しては無頓着であった。今やわれわれは米国クラウド法がサイバー攻撃者と同等程度に脅威である (より厳密にいえば、米国クラウド法によって生じるガバメント用クラウドに対する脅威は直接的・具体的な脅威というよりも、日本国内において政治論争の原因となる抽象的な脅威である) ことを認識するに至った。日本国内において米国クラウド法を材料とする政治論争としてガバメント用クラウドを論難する識者の出現を想定し、その批判的視点における理論を予測してみよう。たとえば、IaaS を利用しており、仮想ディスク上を VM 上のゲスト OS で暗号化していると仮定する。その暗号化済み仮想ディスクと、その暗号鍵が、同じ米国パブリッククラウド上に置いてある場合、これは、サイバー攻撃者にとっても、米国クラウド法を用いてデータにアクセスする米国連邦

政府または州政府の職員にとっても、同様の価値がある。暗号鍵を用いて仮想ディスクを容易に復号化することができるためである。それでは、IaaS の利用において、たとえば、データを入れた仮想ディスクは米国系パブリッククラウド事業者 A の IaaS に置いてあり、その仮想ディスクをロードして暗号鍵を用いて復号化する設定となっている OS のシステムディスクを入れた仮想ディスクは米国系パブリッククラウド事業者 B の IaaS に置いてあると仮定しよう。この構成において、サイバー攻撃者を主たる脅威として考えた場合は、一応の安全性が確保されているように見える。なぜならば、サイバー攻撃者が A または B の一方を掌握する可能性は現実的に十分考えられるが、A と B の両方を同時に掌握する事態の発生はかなり低いためである。それに対する例外的状況を想定した反論は、サイバー攻撃者が B の側を掌握した場合、B の IaaS 上の OS 環境を実行すれば A の仮想ディスクにアクセスでき、かつ、これを復号化できてしまうという問題である。この本質は、B を掌握した攻撃者が、A を掌握していないときに、B を通じて A を掌握することができる現実的可能性が存在するかという点である。これはおそらく可能であろう。しかし、リスクは一定程度に軽減されているということができる。これと比較して、全く同じ構成において、米国クラウド法を用いてデータにアクセスする米国連邦政府または州政府の職員を主たる脅威として考えた場合は、A と B への分割は無意味となるのである。なぜならば、当該職員は、第 18 編 121 章 2703 条 (b) (1) の捜査令状または行政召喚状を、米国系パブリッククラウド事業者 A と B の両方に発行することにより、容易に A のデータを B に含まれる復号鍵によって解読することができてしまうためである。米国クラウド法は、米国系パブリッククラウド事業者に対してデータの復号化を義務付けるものではない。だが、米国政府職員自らが、米国クラウド法を用いてダウンロードした外国からの暗号化済みデータを、同じく米国クラウド法を用いてダウンロードした外国からの秘密鍵データを用いて複合することが可能である。われわれは、単に日本国内においてガバメント用クラウドに関する政治論争の原因となる抽象的な脅威としての米国クラウド法を想定するだけにおいても、A を米国系パブリッククラウド事業者に置くとして、B はそれ以外に置いて安全に分散していますといつでも表明する

ことができる程度の状態を維持してシステムを設計、維持しなければならなくなったのである。米国クラウド法の成立というものは、米国系パブリッククラウド事業者をどちらかというと好んで利用するわれわれに、意図せずにも、このような負荷を生じさせるものであった。

(3) 【提案手法 ③】 日本政府と米国系パブリッククラウド事業者との契約上、一切の紛争は "日本の裁判所が管轄" し、"日本法を準拠法" とする。(第 204 回国会 参議院 内閣委員会 第 17 号 2021/5/11)

国会答弁をみると、日本政府の側も、国会議員の側も、日本政府と米国系パブリッククラウド事業者との間の契約における準拠法および国際裁判管轄をいずれも日本とする対策を採れば、米国クラウド法に基づく開示命令に対する異議申立てに関する審査までも、準拠法および国際裁判管轄いずれも日本となるから、問題が解決されると考えているようである。

しかし、これは、準拠法および国際裁判管轄権に関する理解の混乱に基づく期待である可能性が高い。この提案手法は、米国クラウド法への対処としては、全く効果がないと考えられるのである。日本政府と米国系パブリッククラウド事業者との契約をたとえ日本法に準拠させたとしても、また、たとえ専属的合意管轄を日本の裁判所としたとしても、それはあくまでも契約者である日本政府と米国系パブリッククラウド事業者との間の民事上の関係を規定するに過ぎない。米国クラウド法は、米国連邦政府または米国州政府と米国系パブリッククラウド事業者との間の公法上の関係を規定する法であり、この 2 者の法的関係と、米国系パブリッククラウド事業者と契約者との法的関係とは、全く独立した、別々の関係である。よって、この提案手法を講じたとしても、米国系パブリッククラウド事業者が米国連邦政府または米国州政府から受ける米国クラウド法に基づくデータ開示命令に従わなければならない法的義務も、それに従わなかった場合に受ける可能性があるペナルティも、消滅または軽減させることができない。

(4) 【提案手法 ④】 米国クラウド法は、米国政府に無制限なアクセスを認めるものではなく、米国のための犯罪捜査という極めて限定された場合において、米国の裁判所が発する米国の令状 "等" に基づき、米国系パブリッククラウド事業者に対して開示命令が行なわれるに過ぎないから、脅威は限定的であると考える。(第 208 回国会 衆議院 内閣委員会 第 12 号 2022/03/25、第 210 回国会 衆議院 内閣委員会 第 7 号 2022/11/11)

この考え方は、大きく 2 つの理論によって構成されている。第一に、米国クラウド法によるデータ開示命令が発付されるのは「極めて限定された場合に過ぎない」という理論である。第二に、仮にそれが発付されるとしても、それは米国の裁判所が発する米国の令状 "等" に基づくものだから、司法審査を経ているので安心であるという理論である。ところが、この 2 つの理論はいずれも不十分であると考えられる。

第一の点について、捜査令状の発付状況を見てみる。米国における連邦裁判所の発付する捜査令状のみを見ても、① で前述したとおり、1 年間で 32,282 件の捜査令状 (2021 年の通知遅延捜査令状の件数である) が捜査機関から連邦裁判所に申請され、そのうち、実に 99.5% が、裁判所によって認められているのである。連邦裁判所による捜査令状だけでも年 3 万件が発付されているのだから、各州の裁判所の発付する捜査令状を含めると、膨大な数に上ると考えられる (各州の裁判所の捜査令状の数の統計を探したが、与えられた調査時間内には見つけることができなかった)。したがって、捜査令状だけみても、令状が発付される頻度は決して「限定的」とはいえない。これにより、第一の理論が成り立たなくなってしまう。また、99.5% もの令状が司法審査を通過している事実から、第二の理論も危うくなる。そもそもその司法審査というものは、日本国の裁判所による司法審査でなく、米国裁判所による司法審査である。これは日本国の主権者の立場から見て全く正統性がない。よって、もともと第二の理論で「司法審査を経ているため安心である」という理由は、本件に関して考えるときは実は無意味である。

第二の点について、国会答弁においては、「米国の裁判所が発する米国の令状 "等" 」との政府答弁が行なわれているが、この "等" のところには、行政召喚状が含まれるのである。なぜならば、米国クラウド法第 18 編 121 章 2703 条 (b)

(1) の (A), (B) により、データ開示命令は、捜査令状、行政召喚状、司法召喚状、あるいは裁判所命令のいずれかがあれば発布することができると明記されているためである。行政召喚状は、行政機関がいつでも裁判所を通さずに発付できる命令であることに、注意を要する。① で前述したが、これは司法審査を経ずに米国行政機関が発付することができてしまい、仮に無効を求める抗告を提起したとしても、極めてゆるやかな司法審査によってほとんどの場合は有効とされてしまう。そして、行政召喚状は決して珍しいものではない。統計によると、連邦政府レベルだけでも、年間約 4,000 件が発付されている[①] (行政召喚状はとても強力で濫用のおそれが高いので、議会は司法省に毎年の行政召喚状の発付件数の報告を求めている。年間約 4,000 件という数は、2001 年分の当該報告に記載されている統計情報である。議会の命令により、司法省が議会に報告した資料がインターネットに公開されているのである。2002 年以降の報告書は、何らかの理由でインターネット上に掲載されていないようである)。このように、行政召喚状について見ても、その頻度と違憲審査基準のゆるやかさから、第一の理論、第二の理論のいずれも成り立たないように見える。

ところで、米国系パブリッククラウド事業者のマーケティング資料では、あたかも、米国系パブリッククラウド事業者は滅多に米国政府からの要求に基づく個人情報やデータの開示は行なわないので安心して欲しいという旨の表記がなされている。しかし、実際には米国系パブリッククラウド事業者は米国政府からの数多くの要求に対応している。たとえば、2022 年の下半期だけ見ても、米国 Microsoft Corporation は、米国政府から合計 4,908 件ものデータ開示請求を受けている[②]。このうち、64% の 3,166 件で契約者情報等 (個人情報等) を回答しており、10% の 522 件でユーザーのコンテンツデータを回答しており、11% の 576 件でデータ不存在と回答している。すなわち、2022 年の下半期のみでも、米国政府からの 4,908 件のうち 87% について契約者情報またはデータを検索し、その結果を回答しているのである。法令に準拠しないとして回答を拒否したものは、わずか

① https://www.justice.gov/archive/olp/rpt_to_congress.htm
② Law Enforcement Requests Report, Microsoft Corporation, 2022
https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report

13% の 644 件に過ぎないのである。米国系パブリッククラウド事業者が米国政府に対してデータを開示することは、極めて頻繁に、膨大な件数について行なわれており、決して限定的で例外な事象であるとはいえない。

このように、米国クラウド法の脅威は例外的・限定的では決してない。日本人が米国当局によって被疑者として疑われている場合に、米国クラウド法に基づき捜査令状や行政召喚状が発付され、ガバメント用クラウド上に保存されている当該日本人の個人情報を含んだデータに関し、米国系パブリッククラウド事業者に対してデータ開示命令が発付される可能性は、とても高い確率で存在する。そして、繰り返しになるが、第 18 編 121 章 2705 条により、米国当局は、データが取得されたことの契約者への通知を禁止することを米国系パブリッククラウド事業者に命令することができるので、日本政府も、データを取得された日本国民も、データが取得された事実を知ることすらできない状態が起こり得る。

(5) 【提案手法 ⑤】万一、米国クラウド法に基づく命令があった場合は、米国系パブリッククラウド事業者から日本政府に事前の通知が行なわれるであろう。この場合、"外国主権免除法に基づく主権免除の適用" を米国に求めることで、開示を阻止できる。(第 210 回国会 衆議院 内閣委員会 第 7 号 2022/11/11)

この理論に関する議論は、2 つの部分に分かれる。第一に、米国クラウド法に基づく命令があった場合に、事前の通知を受けることができるか否かである。これについては、提案手法 ① (d) ですでにみたとおり、米国クラウド法第 18 編 121 章 2705 条により、事前の通知すら禁止されることが容認されているので、あまり効果が期待ができない。ただし、予め米国系パブリッククラウド事業者との間で約束を結び、日本政府が契約者となっているガバメント用クラウド用の米国系パブリッククラウド事業者との間の契約に関しては、常に「外国主権免除法に基づく主権免除の適用」を米国に求めるという契約書を締結することは、もちろん可能である。そこで、第二の議論として、「外国主権免除法に基づく主権免除の適用を米国に求める」ことに何らかの効果があるのかどうかを検討していこう。

(a)「主権免除」(sovereign immunity)とは何か

この政府答弁の理論の有効性を検討するためには、政府答弁のいう「主権免除」という概念、および「外国主権免除法」という法律について、それぞれ、詳しく調査研究する必要がある。そこで、まずは、一般法理論における「主権免除」という理論について調べてみる必要がある。

国際法 (慣習法) における「主権免除」(sovereign immunity) とは、国家免除 (state immunity) とも呼ばれる概念である。国家は外国裁判所の裁判権に服さないという国際法上の概念である①。これは、「対等な者は対等な者に対しては支配権を持たない」(ラテン語 "par in parem imperium non habe") という法諺に由来した概念である。ここで、主権免除を受けることができる「裁判権」には、一体どのような裁判権が含まれるのかが問題となる。一般に、裁判権は、民事裁判権と、刑事裁判権に大別できる。理論上は、広義の主権免除という概念には刑事裁判権も含まれ得る。しかし、国際法において、主権免除 (国家免除) という用語が用いられる場合、これは民事裁判権のみを含み、刑事裁判権を含まない。国連総会における国連国家免除条約が採択された際にも、同条約は「刑事手続には適用されない」ことが確認されている②。

(b) 米国における「主権免除」および「外国主権免除法」とは何か

米国における「主権免除」は、米国憲法学上から発達した概念である。これは、もともとは、連邦または州は、政治的または統治的性質を有する行為から生ずる結果について不法行為責任を問われることがない、という理論である③④。

すなわち、もともとの考え方は、各州は独自の主権を有しているため、州政府に対する訴えはその州の裁判所に提起しなければならず、連邦裁判所では州を訴えることができないというものである。米国憲法修正第 11 条は「合衆国の司法権は、その一州に対し、他州の市民、または外国の市民あるいは臣民によって提起あるい

---

① 新版 国際法講義, 波多野 里望, 有斐閣, P.98
② 国際法, 岩沢 雄司, 東京大学出版会, P.187
③ 法学 14 (1) アメリカの憲法判例に見る主権免除の理論, 高野 幹久, 関東学院, P.17
④ Black's Law Dictionary, Fifth Edition, P.1252

は訴追された普通法あるいは衡平法上のいかなる訴訟にも及ぶものと解釈してはならない。」と規定している。この考え方の延長上、外国も州と同様に主権を有するから、外国に対しても主権免除が認められるという理論が成立したようである。1812 年の米国最高裁判決が、米国において外国に対する主権免除を認めた最初の判例である[①]。その後長い間、米国では主権免除に関する明文法が存在しなかったが、米国裁判所は慣習法としてこれを扱ってきた。しかし、どのような場合に主権免除がなされるのか明確でなかったため、1977 年に米国連邦法である「外国主権免除法」(Foreign Sovereign Immunities Act) が制定された[②③]。外国主権免除法の全文は、第 28 編第 97 章の第 1602 条から第 1611 条までに規定されている。

米国の慣習法上の主権免除の概念においても、明文化された外国主権免除法の条文においても、いずれも、主権免除は民事訴訟のみが対象となる。刑事訴訟は、主権免除の対象とならない。

（c）米国クラウド法に関して、外国主権免除法に基づく主権免除の適用を米国に求めても無意味である

すでにみたように、米国クラウド法は、捜査目的における刑事訴訟の手続の一環として、米国連邦政府または米国州政府の捜査員等に、捜査令状または行政召喚状の発付によって、米国系パブリッククラウド事業者を経由して、外国にあるサーバーに記録されている契約者の情報を強制的に取得することを実現する法律である。米国クラウド法によるデータ開示命令は、刑事捜査手続である。よって、仮に日本政府が、または日本政府の委託を受けた米国系パブリッククラウド事業者が、米国政府に対して、外国主権免除法に基づく主権免除の適用を米国に求めても、全く無意味であると考えられる。

なお、米国クラウド法は、米国当局が米国系パブリッククラウド事業者に対してデータ開示命令を発布する手続きを規定するものであり、当該データ開示命令にお

---

① Schooner Exchange v. McFaddon, 11 U.S. 116 (1812)
② ジュリスト No. 727 (1980.11.1), 米国主権免除法, 西立野 園子, 有斐閣, P.117
③ アメリカ合衆国の主権免除法について, 鳥居 勝一, 法政論叢 16, 1980

ける当事者は、米国当局と米国系パブリッククラウド事業者との間の 2 者である。すなわち、捜査令状の名宛人は、あくまでも民間企業である米国系パブリッククラウド事業者であり、契約者である日本政府ではない。そのため、仮に主権免除の概念が民事訴訟のみを対象とするのか、または刑事訴訟も含むのかの点を捨象して考えたとしても、そもそも民間企業が命令の名宛人となる捜査令状または行政召喚状の効力 (裁判権) を、その民間企業から免除することできない。外国主権免除法の免除の法的な限界がある以上、いかに米国系パブリッククラウド事業者が、米国政府には主権免除が適用できるから安全である旨をマーケティング資料において述べているとしても、それは全く効果がなく、無意味である。

よって、政府答弁の「外国主権免除法に基づく主権免除の適用を米国に求める」という手法は、文字通りの意味であれば、米国クラウド法に対する対処策としての効果がないと思われる。

(d) 政府答弁の趣旨は第 18 編 121 章 2703 条 (h) の手法で実現できる可能性は一応存在する

米国における外国主権免除法に基づき主権免除の概念が民事訴訟のみを対象としており、米国クラウド法に対抗するために効果がないにもかかわらず、なぜ、政府答弁では、「⑤ 万一米国クラウド法に基づく要請 (命令) があった場合は、米国系パブリッククラウド事業者から日本政府に (事前の) 通知が行なわれ、外国主権免除法に基づく主権免除の適用を米国に求めることで、開示が行われないものと考えている。」(第 210 回国会 衆議院 内閣委員会 第 7 号 2022/11/11) という説明がなされたのだろうか。

おそらく、上記の政府答弁の趣旨は、米国クラウド法に基づく開示命令に対して、日本国政府は米国政府に対して契約者である日本国の現地法 (日本法。すなわち、日本国憲法や行政機関の保有する個人情報の保護に関する法律) を尊重し、米国政府の命令行為が、日本法に決して抵触することのないよう、開示命令を変更または破棄するよう法的に要求できる余地があるという意味であろう。確かに、第 18 編 121 章 2703 条 (h) には、外国の判断の尊重を実現する余地がある規定が存在する。これは、米国クラウド法上における外国主権免除法のようなものであるといってもよ

い。同条 (h) の標題の原文は、「Comity Analysis and Disclosure of Information Regarding Legal Process Seeking Contents of Wire or Electronic Communication」である。"Comity Analysis" とは、直訳すると、国際礼節に基づく法的解釈というような意味であるが、分かりやすいように日本語要約では「外国の判断の尊重」としている。同条 (h) の規定を活用すれば、確かに、日本政府は米国系パブリッククラウド事業者に対して、米国クラウド法に基づく開示命令に対応して、日本法を遵守して開示命令を控えるよう、米国当局に要請することができる可能性がある。しかしながら、これを日本政府が利用するには、重要な条件として、「適格外国政府」として米国に認定される必要がある。「適格外国政府」の要件は、第 2523 条に明記されている。すなわち、米国政府との間で「行政協定」を締結した外国政府のみが、「適格外国政府」とみなされる。仮に日本政府が行政協定を締結し、米国における適格外国政府として承認された場合は、日本政府は米国政府に対して第 18 編 121 章 2703 条 (h) (2) の「破棄または変更を求める異議申立て」を行なうことができる (より厳密には、この申立ては、やはり米国系パブリッククラウド事業者から行なう必要があり、日本政府から直接米国政府に対して行なうことはできない)。この場合、第 18 編 121 章 2703 条 (h) (3) に記載されているとおり、米国裁判所は、いくつかの事項を判断し、データ開示命令の「破棄または変更」を認めるか否かを審査することになる。政府は、この手法を採ることができる旨を表現しようとして、「外国主権免除法に基づく主権免除の適用を米国に求めることで、開示が行われないものと考えている。」と答弁したものであると考えたならば、誰でも、この答弁の内容を納得することができるであろう。

さて、確かに日本政府が第 18 編 121 章 2703 条 (h) を活用すれば、米国政府に対して米国クラウド法に基づく開示命令を阻止するために、(米国系パブリッククラウド事業者を通じて間接的にであっても) 異議申立てをする余地が生まれるが、これには、次の 3 つの大きなハードルがある。

(ア) まず、日本政府は、米国政府との間で、第 2523 条に規定されている「行政協定」を締結しなければならない。行政協定が締結されていない限り、

第 18 編 121 章 2703 条 (h) (2) の「破棄または変更を求める異議申立て」は不可能である。行政協定の締結自体は、すでにいくつかの国 (英国、オーストラリア等) が米国と締結済みであるため、そのこと自体のハードルはそれほど高くないと考えられる。

(イ) 仮に行政協定を締結し、第 18 編 121 章 2703 条 (h) (2) の「破棄または変更を求める異議申立て」を行なったとしても、その異議申立てが認められるかどうかは、第 18 編 121 章 2703 条 (h) (3) に基づき、日本の裁判所ではなく、米国の裁判所が判断することとなってしまう。米国の裁判所は、日本の主権者にとって正統性がある裁判所ではなく、他人 (外国) の裁判所に過ぎない。もともと、行政機関に対する個人情報をみだりに第三者に開示されない自由権は、日本国憲法 13 条で保障される権利であり、また、日本国の法律に基づいて保障される権利である。住基ネット事件最高裁判例基準 (3) の「個人情報の漏えい」を阻止し、また、行政機関の保有する個人情報の保護に関する法律 6 条 (安全確保の措置) 1 項、8 条 (利用及び提供の制限) 1 項で規定されている保護の状態を維持するためには、そのような異議申立ては、必ず、日本法に基づいて、日本の裁判所で審理されなければならないはずである。しかし、第 18 編 121 章 2703 条 (h) (2) を活用しても、日本の裁判所で審理がなされない以上、日本国憲法 13 条および行政機関の保有する個人情報の保護に関する法律 6 条 (安全確保の措置) 1 項、8 条 (利用及び提供の制限) 1 項で規定されている個人情報の保護の保障が実現されていない状態は、変わらない。したがって、行政協定においては、当該司法判断は米国の裁判所ではなく日本の裁判所で行なう旨の協定を締結しなければならない。しかし、米国がその条件を実際に受諾する可能性は低い。

(ウ) 仮に (ア)、(イ) の問題が解決されたとしても、第 18 編 121 章 2703 条 (h) (4) に規定されている「(米国の) 裁判所が第 2705 号 (a) (2) で示

されている不利益な結果を予防するために直ちに開示する必要があると判断した場合」には、異議申立て中であっても、データが米国政府に開示されてしまう。一度データが米国政府に開示されてしまったならば、これを取戻すことは不可能で、異議申立ては全く無意味になってしまう。したがって、米国との行政協定においては、第 18 編 121 章 2703 条 (h) (4) の司法判断についても、(イ) と同様に、日本の裁判所で行なう旨の協定を締結することが必要になってしまう。しかし、この条件についても、米国が実際に受諾する可能性は低い。

しかし、繰り返しであるが、未だ日本は米国と行政協定を締結していないので、政府答弁の趣旨は第 18 編 121 章 2703 条 (h) の手法で実現することはできないと考えられる。

4　統治行為論により違憲審査を回避できるか

仮に米国クラウド法に関係してガバメント用クラウドに関する違憲審査が行なわれようとするとき、国の視点において、統治行為論を利用してこれを回避することができるかが問題となる。

日米関係における基地問題について統治行為論が展開され憲法審査が回避された事件として、砂川事件最高裁判例 (最大判昭和 34 年 12 月 16 日) がある。砂川事件では、日米安保条約が違憲無効であるか否かが争われたが、「本件安全保障条約は、(略) 主権国としてのわが国の存立の基礎に極めて重大な関係をもつ高度の政治性を有するものというべきであって、(略) 裁判所の司法審査権の範囲外のもの」とされ、日米安保条約の違憲性は司法審査の対象とならないとされた。このように、外国関係における統治行為論の展開においては、違憲審査の対象が国家全体の運命に関する重要事項である場合を必要とするとされる。

さて、ガバメント用クラウドを米国系パブリッククラウド事業者が提供し、日本の行政権がガバメント用クラウドに国民・住民のプライバシー情報を保存しているときに米国クラウド法により住民情報が米国連邦政府または米国州政府に対して無断でデータ取得されてしまうことに関する違憲性は、国家全体の運命に関する重

要事項にはあたらないと考えられる。なぜならば、日本国は、国家の運命を保つための引換え条件として、米国からそのようなデータ取得ができる状態をできるだけ維持するよう強制されたことはなく、また、米国から米国系パブリッククラウド事業者を特に利用するよう圧力をかけられたこともないのであり、米国系パブリッククラウド事業者をガバメント用クラウドの基盤の提供事業者として選択している理由は、米国政府の意向ではなく、単に日本国の自由意思でこれを選択しているに過ぎないので、米国系パブリッククラウド事業者の積極的利用は、国家全体の運命を保つという目的とは何も関係がないためである。

そして、ガバメント用クラウドへシステムを移行する前であっても、機微なプライバシーが問題となるような各種 IT システムは動作させることができてきたし、また、システムを移行した後であっても、任意の時点で任意の非米国系パブリッククラウド、プライベートクラウドまたはオンプレミスシステムに回帰することは可能であり、それを行なわずにあえて米国クラウド法の対象となるリスクのある米国系パブリッククラウド事業者を選択し続けることは、単に、国または地方公共団体の完全な自由意思によるものであるためである。

このことから、われわれは、米国クラウド法に関係してガバメント用クラウドに関する違憲審査が行なわれようとするとき、統治行為論を利用して、その違憲判断の接近を回避することは、不可能であると思われる。

第 6 節　まとめ —— 米国クラウド法対策手法

ガバメント用クラウドに係る米国クラウド法対抗手法を述べた国会答弁 (2021 年、2022 年) におけるこれまでの政府の提案手法 ① ～ ⑤ を再掲する。

【提案手法 ①】 日本政府または日本の地方公共団体の有するクラウド上のデータに関し、米国政府から米国系パブリッククラウド事業者へのデータ提供命令があった場合、日本政府または日本の地方公共団体の有する国民の個人情報が米国政府に提供されることを避けるため、米国系パブリッククラウド事業者の異議申立てや日本政府への事前の通知を求め、そのような通知があったならば、日本政府が米国系パブリッククラウド事業者と協議し、"適切に対応" する。(第 204 回国会 参議院 内閣委員会 第 17 号 2021/5/11、第 208 回国会 衆議院 内閣委員会 第 12 号 2022/03/25)

【提案手法 ②】 仮に米国政府がデータを取得できてしまったとしても、米国政府がその内容にアクセスできないように、"暗号化措置" を事前に講じているので、米国政府へのデータ漏えいの危険は防止できる。(第 204 回国会 参議院 内閣委員会 第 17 号 2021/5/11、第 208 回国会 衆議院 内閣委員会 第 12 号 2022/03/25)

【提案手法 ③】 日本政府と米国系パブリッククラウド事業者との契約上、一切の紛争は "日本の裁判所が管轄" し、"日本法を準拠法" とする。(第 204 回国会 参議院 内閣委員会 第 17 号 2021/5/11)

【提案手法 ④】 米国クラウド法は、米国政府に無制限なアクセスを認めるものではなく、米国のための犯罪捜査という極めて限定された場合において、米国の裁判所が発する米国の令状 "等" に基づき、米国系パブリッククラウド事業者に対して開示命令が行なわれるに過ぎないから、脅威は限定的であると考える。(第 208 回国会 衆議院 内閣委員会 第 12 号 2022/03/25、第 210 回国会 衆議院 内閣委員会 第 7 号 2022/11/11)

【提案手法 ⑤】 万一、米国クラウド法に基づく命令があった場合は、米国系パブリッククラウド事業者から日本政府に事前の通知が行なわれるであろう。この場合、"外国主権免除法に基づく主権免除の適用" を米国に求めることで、開示を阻止

できる。(第 210 回国会 衆議院 内閣委員会 第 7 号 2022/11/11)

これらについて、それぞれ、前記のとおり分析をしたところ、提案手法 ①、③、④、⑤ には、米国クラウド法による国民の個人情報への侵害に対しては効果がないと考えられる。

むしろ、提案手法 ①、③、④、⑤ は、米国クラウド法や米国の主権免除の概念、ならびに外国主権免除法に関する規定と比較して齟齬があり、日本の主権者を説得する手法として逆効果であると思われる。日本の主権者 (総体としての国民) や、その代表者である議員の方々は、いったんは、政府答弁における提案手法 ①、③、④、⑤ を一応正しそうなものであると認識して、それ以上の詳しい議論をしなかった可能性がある。しかし、これは政府答弁の理論が十分堅牢に成り立っていたからではなく、むしろ、政府の側も主権者の側も、とても新しい事柄であったことから、十分な理解に達する前に、他の事柄に関する議論のための余裕も十分に必要であるという時間的制約によって、いったんは議論の沈着があったというのに過ぎないように見えるのである。すなわち、問題は十分に解決されておらず、おそらく、今後主権者 (の代表としての議員の方々) は提案手法 ①、③、④、⑤ には実際には効果がないのではないかということを考え始め、政府に対して再度確認をするように頼んでくる可能性が、おおいに存在するのである。そこで、われわれは、今、できるだけ早く勉強を重ね、何らかの方法で、過去にすでに行なった提案手法 ①、③、④、⑤ について、それぞれ、より良い補強理論を考案し、その新たな理論を添加することにより、十分な堅牢性を確保して、説明責任が果たせる状態を維持しておく必要がある。これに成功した場合、われわれの政府は、ガバメント用クラウドに関して、主権者の信頼を勝ち取ることができ、ガバメント用クラウドの推進が可能な程度の強力な支持力を維持するであろう。他方で、より力強い指摘がなされるまでに提案手法 ①、③、④、⑤ について補強をすることができなかった場合は、提案手法 ①、③、④、⑤ の不備について論難が生じ、批判の声が高まり、われわれの政府がガバメント用クラウドの推進が可能な程度の強力な支持力を維持できることについての懸念が生じるかも知れない。そこで、これを避けるために、われわ

れは、改めて提案手法 ①、③、④、⑤ に係る理論を再検討し、米国クラウド法や、それの基礎となっている米国の憲法学や法律学や文化などの知見を高め、不明な点はさまざまな識者に尋ねるなど、十分な努力を行なう必要がある。

そして、もちろん、提案手法 ②、すなわち、「仮に米国政府がデータを取得できてしまったとしても、米国政府がその内容にアクセスできないように、"暗号化措置" を事前に講じているので、米国政府へのデータ漏えいの危険は防止できる。」(第 204 回国会 参議院 内閣委員会 第 17 号 2021/5/11、第 208 回国会 衆議院 内閣委員会 第 12 号 2022/03/25) には、これが確実に具備された場合は、十分な効果があると考えられる。② が確実に実現されている限り、実は、提案手法 ①、③、④、⑤ の理論が不完全であっても、主権者に対しては、個人情報の十分な保護が実現できていると説明することが可能である。暗号化による完全なデータの機密性の支配が保障されている限り、米国クラウド法に基づいて米国がデータの中身を無断で取得することは不可能であると技術的に説明可能である。これが常に説明できれば、主権者の不安は減り、提案手法 ①、③、④、⑤ の理論に関する完備が多少遅れていても、致命的な問題は生じないと思われる。

だが、提案手法 ② のみを、米国クラウド法対策としての実質的な唯一の頼りにするという場合は、提案手法 ② の実装にすべての重圧がのしかかるのであり、決して失敗が許されない状況に陥ることとなるので、この場合は、最大限の技術上および運用上の注意を払わなければならない。提案手法 ② において具備が必要なクライアント側での暗号化に関しては、繰り返しになるが、最も注意しなければならない点として、暗号化の手法が機能するためには、米国パブリッククラウドに保管されるすべてのデータは、確実に、「クライアント側」で暗号化を施されている必要がある。そして、その暗号鍵は、決して米国パブリッククラウドのいずれかの領域に保管されてはならないことになる。なぜならば、仮に暗号鍵がいずれかの米国パブリッククラウド上に、平文で、または復号化可能な形式で、保管されていたとしたら、米国連邦政府または米国州政府の職員は、米国クラウド法を用いて、データと、暗号鍵の両方を容易に取得することができてしまうためである。このことについては、「資料③」のクライアント側暗号化で詳しく説明をしている。また、ク

ライアント側での暗号化を確実にするためには、現段階の技術水準では、国民の個人情報を含むデータそのものの保管 (たとえばデータベース機能やメールサーバー機能等) に PaaS や SaaS を利用することができないことを意味する。だが、そのうちに、たとえば SaaS のデータベースにおいて行レベルのクライアント側暗号化の手法が現実的・一般的になるときが到来するかも知れない。そうしたならば、SaaS を利用することも可能となるから、あまり心配しなくても良さそうである。それまでは、SaaS のデータベースの行に平文データを書き込む必要が生じてしまい、そのデータは、米国クラウド法に基づき漏えいのおそれが生じてしまうので、提案手法 ② にほとんど依存する場合では、利用することができないということになる。

国は、ガバメント用クラウドが米国系パブリッククラウド事業者によって提供される場合においては、米国クラウド法への対処として、提案手法 ② に関するクライアント側データ暗号化を、自らのガバメント用クラウド利用に関しては自ら確実に施すとともに、他人 (地方公共団体その他の法人) に対してガバメント用クラウドの利用を指示する場合は、必ず、提案手法 ② に関するクライアント側データ暗号化を施すことを指示するべきである。

これまでにみたように、ガバメント用クラウドを米国系パブリッククラウド事業者のクラウド基盤上で実現する場合には、すでに国会答弁を行なった手法 ① ～ ⑤ について、いずれを実効性のある手法として採るかというその戦略によって、取り得るソフトウェア的な選択肢や、実装の複雑さなどが、大きく変動するので、細心の注意が必要である。国民の個人情報をデータとして取り扱うシステムを、パブリッククラウド上に構築運用するということは、そう簡単なことでなく、ソフトウェア実装技術と、セキュリティ技術と、法的技術の 3 つが密接に関係する、とても高度な問題でもある。これは、一種の苦行のようなものである。このような苦行がガバメント用クラウドを進める上においてその行進する洞窟通路の随分中頃を過ぎた隘路に両手を大引く広げて立ちはだかっているということも知らされることなく、とても太平な快適洋行であると聞かされて次々に入ってきた方々の場合、これには、面食らうのである。だが、このクラウド・コンプライアンスの苦行

問題は、決して、日本政府のみが困っている訳ではない。他の先進国政府も、発展途上国政府も、すべての国で、今、皆困っていることなのである。ヨーロッパの各国の様子 (資料 ④-2)の外国資料から、このことは、明らかである。この問題の本質を考えると、それはまさに、どのようにして、米国クラウド法の問題を解決しつつ、便利で高性能な米国系パブリッククラウド事業者のサービスを利用するかという、技術的享楽性が感じられるような、相反する物事の両立の実現という、曲芸的デジタル領域である。ここに、創造の余地があるのであるといえる。われわれは、この難解な苦行問題に、馳駆をいとわずに、正面から向き合う必要がある。他国の低水準 IT 人材が陥るような、分からないことを分からないままとし、知らない領域を責任分解点の彼岸側であるから無関係として、生じた問題を虚偽の説明で取り繕い、不十分な点を認識・容認しているにもかかわらず不十分なままこれを放置し先送りするというような不完全な対処を決して行なわずに、日本人らしく、問題を、次々と、正しく解決しなければならない。末節は少々不十分でもよいとしても、主要な部分について、決して、妥協をしてはならない。システムに関する技術的側面、セキュリティ的側面、法的側面のいずれもが、つぎはぎだらけの怪物的構造とならないためには、常に、一人一人の頭脳でさまざまな事項を一応は全部理解する必要があり、その結果として、強靭な思考能力が、組織的に形成され、これに、大きな価値が生じる。そうして、先ほどの洞窟隘路に両手を大引く広げて立ちはだかっていた苦行を正しく解消すれば、その先には、誠に快適なペーブメントで過ごせる日々が、必ずや待受けているのである。ヨーロッパ人など他国の人には問題物を越えることはもしかすると困難かも知れないが、われわれ日本人は、優秀であり、この目的地に漕ぎ着くことは、十分に可能なことである。そして、その成果として、さまざまな新しい運用手法、構築ノウハウ、ミドルウェア的なソフトウェア、法的技術、外国政府との交渉術など、豊富な価値があるものが、次々とわれわれの政府人材から生まれるのである。その能力こそが、いわゆる、デジタルガバメント能力というものである。われわれの政府が切望しているのはまさにそのような組織的能力の自然的発生という鴻業物なのである。そして、このような物事を解決していく過程で得られる実力が、日本国の行政部門として、組織的に有する価値となり、単

にコンピュータ部門だけでなく、経営や企画、戦略立案といった、凡そ重要な局面で常に有用であるなるような一般的問題解決能力に転化され、日本人のその人材水準が異様に高いことが、他国との有意な差となり、ひいては、高い国際競争力を帯びた価値のある人材群集団として、その人材と生み出す価値物は、日本から、世界中に、いよいよ、展開をしてゆくことになるのである。

参考文献

【書籍、論文】
米国行政法研究―行政行為に対する司法審査，橋本 公亘著，有信堂，1958/03

Black's Law Dictionary（英米法辞典）第 5 版，MA Henry Campbell Black，1979/05/01

アメリカ合衆国の主権免除法について，鳥居 勝一，法政論叢 16，1980

米国主権免除法，西立野 園子，ジュリスト No.727，有斐閣，1980/11/01

米国主権免除法における外国の非商業的不法行為， 臼杵 知史， 北大法学論集 36 (3)，1985/10/15

9.11 テロ損害賠償請求事件における主権免除について， 水島 朋則， 名古屋大学 法政論集 230 号，2009/06

主権免除について，村上 正子，法律時報 第 889 号，2000/03

国家の主権免除 横田基地訴訟鑑定書を中心として，原 強，法律時報 第 889 号，2000/03

主権免除と基地問題 憲法学の立場から，高作 正博，法律時報 第 889 号，2000/03

アメリカの憲法判例に見る主権免除の理論，高野 幹久，関東学院「法学」 14 (1)，2004/09

Administrative Subpoenas in Criminal Investigations, Charles Doyle, CRS Report for Congress, 2006/03/17

域外リモートアクセスによる証拠収集にかかる米国 CLOUD 法に基づく行政協定に関する一考察，有本 真由，情報ネットワーク・ローレビュー 第 18 巻，2018

憲法 第七版，芦部 信喜，岩波書店，2019/03/19

Mitigating the risk of US surveillance for public sector services in the cloud, Jockum Hildén, Communication Rights in the Age of Digital Disruption, ヘルシンキ大学，フィンランド，2021/09/30
https://policyreview.info/articles/analysis/mitigating-risk-us-surveillance-public-sector-services-cloud

マイナンバー訴訟における「私生活上の自由」，斉藤邦史，情報法制研究 第 10 号，2021/11

CLOUD Act（クラウド法）研究会 報告書，西村高等法務研究所，2023/04

【資料】
Report to Congress on the Use of Administrative Subpoena Authorities by Executive Branch Agencies and Entities，米国司法省，2001
https://www.justice.gov/archive/olp/rpt_to_congress.htm

犯罪捜査における国外データへのアクセス，小向 太郎，総務省 情報通信法学研究会 新領域分科会（令和元年度第 1 回会合），2019/10/16
https://www.soumu.go.jp/main_content/000652702.pdf

Delayed-Notice Search Warrant Report 2021，米国裁判所事務局，2021/09/30
https://www.uscourts.gov/statistics-reports/delayed-notice-search-warrant-report-2021

Law Enforcement Requests Report，Microsoft Corporation，2022
https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report

How Often Do the FBI and the Department of Justice Seek Search Warrants and Subpoenas?，Syracuse University，2022/08/22
https://trac.syr.edu/immigration/reports/693/

【法律】
米国 CLOUD Act（米国クラウド法）（2018；第 115 回 米国議会 下院提出法案 第 4943 号）
https://www.congress.gov/115/bills/hr4943/BILLS-115hr4943ih.pdf

米国連邦法 第 18 編第 121 節 米国クラウド法（STORED WIRE AND ELECTRONIC COMMUNICATIONS AND TRANSACTIONAL RECORDS ACCESS）
https://www.law.cornell.edu/uscode/text/18/part-I/chapter-121

米国連邦法 第 28 編第 97 節 米国外国主権免除法（JURISDICTIONAL IMMUNITIES OF FOREIGN STATES）
https://www.law.cornell.edu/uscode/text/28/part-IV/chapter-97

【国会議事録】
第 193 回国会 衆議院 参考人陳述 宍戸 常寿
https://www.shugiin.go.jp/internet/itdb_kaigiroku.nsf/html/kaigiroku/025019320170601007.htm

第 198 回国会 衆議院 米クラウド法と個人情報保護法上の対応に関する質問主意書 2019/06/13

https://www.shugiin.go.jp/internet/itdb_shitsumon.nsf/html/shitsumon/a198227.htm

第 198 回国会 衆議院 米クラウド法と個人情報保護法上の対応に関する質問主意書 答弁書 2019/06/25
https://www.shugiin.go.jp/internet/itdb_shitsumon.nsf/html/shitsumon/b198227.htm

第 204 回国会 参議院 内閣委員会 第 17 号 2021/5/11
https://kokkai.ndl.go.jp/#/detail?minId=120414889X01720210511

第 208 回国会 衆議院 内閣委員会 第 12 号 2022/03/25
https://kokkai.ndl.go.jp/#/detail?minId=120804889X01220220325

第 210 回国会 衆議院 内閣委員会 第 7 号 2022/11/11
https://kokkai.ndl.go.jp/#/detail?minId=121004889X00720221111

「ガバメント用クラウドのコンプライアンス対策としての最高裁住基ネット合憲基準に照らした米国クラウド法に関する調査研究 ～ 国・地方自治体システムにおける米国クラウド法を原因とする日本国憲法および行政個人情報保護法違反のリスクを安全解消する現実的方法の考察 ～」

2024 年　登 大遊

dnobori@cs.tsukuba.ac.jp

本資料に記載されているすべての内容は、独立した研究者としての意見であり、所属組織全体の見解を示すものではありません。

この資料は、ほとんど 2023/11/25 (土), 26 (日) の 2 日間に、図書館に篭って様々な書籍を調べながら急いで書いたものであり、また、法律は私の専門分野とまったく異なることから、誤りが存在する可能性が、他の技術系の資料と比較して、かなり高い確率で存在すると思います。その点をご了承いただきお読みいただければ幸いです。