コヴィングトン&バーリング法律事務所

USA パトリオット法とクラウド・サービスの利用
質疑応答

IT 機能及びデータをクラウド･ベースのコンピューティング・サービスにマイグレーションすることを検討するにあたり、クラウド・サービスが保持データのセキュリティ及びプライバシーに対しどの様な影響を与えるか等、企業は様々な利点やコストを考慮しなければなりません。米国のクラウド･ベースのサービスに関しプライバシー面で生じる主な懸念は、この様なサービスを利用した場合、米国政府が特にパトリオット法（愛国者法、又は「2001 年度テロ行為を傍受・妨害する為に必要となる適切な手段を提供することによってアメリカを団結し強化する法」“**U**niting and **S**trengthening **A**merica by **P**roviding **A**ppropriate **T**ools **R**equired to **I**ntercept and **O**bstruct **T**errorism Act of 2001” 以下略してパトリオット法という）に基づき企業顧客のデータにより広い範囲でアクセスすることが出来るのではないか、という疑問です。特に欧州企業によるクラウド・サービスの利用に関し度々報道されてきたこの懸念は、多くの場合、パトリオット法や政府によるデータ・アクセスを規定する米国及び各国の法律の誤解から生じているものです。

初めに、よく見られる説明とは異なり、パトリオット法自体は米国政府がユーザー・データにアクセスする為の方途ではありません。それは、実際には様々な既存の連邦制定法に対する改正法の集積です。これらの改正法は、制定以降数回変更されていますが、2001 年 9 月に発生したテロ襲撃に直接対応するものとして、当初は米国政府のテロ行為に戦う能力の強化を意図していました。これらの改正法は例として：

＊　かつて組織的犯罪と戦う為に許容されていた捜査手法を米国政府がテロ事件に適用することを認める。

＊　外国による情報諜報活動を調査する米国政府の権限を拡張することによってテロ組織の活動やその他米国に対する秘密諜報活動も包含する。

＊　国際的な資金洗浄活動やテロ行為への資金調達を阻止する権限を拡張する。

＊　米国の国境安全保障を強化し、米国政府の情報機関や警察機関の間で情報交換が行われることを遮った、そして９・１１襲撃を阻止できなかった要素となった障壁を取り除く。

＊　有効な裁判官令状に基づき執行される限り既に許容されている、政府による捜索を更に効率的にする。例えば、改正法は連邦制定法を改正し、多数の州において通信業者が保持するデータの開示が必要な場合、州それぞれの捜査令状を（何人もの裁判官に）申請する必要なく単一の捜査令状で執行することを可能にする。

よって、パトリオット法は米国政府がオンライン・データにアクセスする為の権限を創設したものではありません。逆に、これらの権限は、様々な既存の刑法及び刑事訴訟法において既に制定されていたものです。

加えて、パトリオット法の改正法は、米国政府に対し、オンライン・データに対して無制限のアクセスを認めるものではありません。逆に、これらの改正法は、オンライン･データに適用される限り、この改正法の国家安全保障というごく狭い目的に関連する捜査においてのみ政府がデータにアクセスすることに限定されています。

又、よく見られるパトリオット法の説明とは異なり、パトリオット法によって改正された制定法は、米国司法制度に基づく手続保障に継続して従うことになります。実際、米国の法律は、クラウドに保存されているデータに対し多層のプライバシー保護を提供しており、米国政府がクラウド事業者に対して顧客のデータの開示を請求する権限を制限しています。これらの保護措置は、米国国民のみに限定されておらず、米国外に所在する非米国企業が所有するデータにも適用されます。

更に、EU（欧州連合）諸国を含む、ほとんどすべてと言ってもよいほどの多くの国々と比較してみても、米国が外国企業やそのデータに対し、より広い管轄を主張している訳ではありません。これは米国外で保管されているデータに対する管轄に関しても言えることです。

最後に、欧州企業は、EU のデータ保護指令を遵守する能力を妨げられることなく米国事業者のクラウド・サービスを利用することができます。米国の事業者が EU と米国間のセーフ・ハーバー条約につき認証及び準拠しており、その指令によって要求されている適切な約定を欧州企業との間で契約上締結していれば、その欧州企業は、法令遵守の観点からすると、社内でデータを保管するのと実質的には同じ立場にあることになります。

＊　　＊　　＊

１．　パトリオット法を含め、米国の法律は、如何なる目的であれ、米国政府がその入手したいあらゆる情報に対しアクセスすることを許容しているのですか？

米国の法律は、クラウドに保管されているデータを含め、個人及び企業のデータに対し多層のプライバシー保護を設けています。これらの法律は、米国政府がクラウド事業者に対し顧客データの開示を請求する権限に対する重要な制限です。米国・海外いずれに所在するデータであっても、警察機関は、データを入手する前に、政府による無制限なアクセスに対する保護措置として設定された手続に従わなければなりません。これらの保護措置は米国国民に限らず、米国外に所在する外国の（企業を含む）当事者にも適用されます。

２．　パトリオット法により、外国企業のデータには米国政府によるアクセスという新しいリスクが生じていますか。

クラウド・サービスが発明されるより遥かに昔の約 10 年前に、米国議会はパトリオット法を制定しています。それ以前に存在していた連邦制定法においても、法の執行という目的であれば、データが米国外に保管されている場合であっても、データ開示を強制する権限が米国政府には付与されていました。パトリオット法は、米国に対するテロ行為及び秘密諜報活動を阻止する米国政府の権限を強化する改正法を導入しました。パトリオット法

の対象が限定されていることから、そのデータ･アクセスに関する条項は、ほとんどのクラウド顧客にとっては関係がないことになります。

３．　パトリオット法は、米国政府がオンラインのデータにアクセスする権限の根拠となるのですか。

パトリオット法は、米国政府によるオンライン・データに対する合法的なアクセスを定める法律を含む、既存の制定法に為された多数の改正法です。オンラインの文脈で言えば、警察機関がデータにアクセスする権限及びデータのプライバシー保護を提供する主要な連邦制定法は、電子コミュニケーション・プライバシー法 (Electronic Communications Privacy Act, 略して“ECPA”) です。米国では、データをホストしているオンライン・サービス提供者は、一般的に他の事業には適用されない ECPA に基づく命令に従わなければならない可能性があります。政府は、企業の事業拠点にあるデータへのアクセスについては、企業に対し有効な令状を送達しこれを執行することが可能である為、ECPA に基づく命令は、企業顧客の情報に米国政府がアクセスする権限に基本的な変更を加えるものではありませんが、ありえることとしては、企業自体を通じてではなく、オンラインのサービス提供者を通じてのアクセスが可能になるということです。

４．パトリオット法は、米国の法律が適用される範囲を広め、あるいは米国のクラウド・サービス事業者が、米国政府からの外国のユーザーのものを含むデータ請求に対応するべき根拠を提供したのでしょうか。

パトリオット法が制定されるより遥かに昔から、米国の裁判所は、米国に存在がある企業は、（その情報の所在地が何所であろうと）その企業がそのデータの「占有、管理、又は支配」をしている限り、米国政府による有効な情報請求に応じる義務があるとの判断を示していました[1]。この法的原理は、EUの幾つかのメンバー国が取っている考え方（これら各国の規定では、警察機関が国内でアクセス可能なデータについては管轄を取得することを許容している）とあまり違いがなく、米国との接触、又は米国に存在がある会社に対し米国政府が合法的な情報請求をした場合にはそれに応じることを従前から求めており、それは欧州でデータを保存している欧州企業に対しても同様です。

５．　米国のクラウド・サービス事業者は、米国の警察職員から請求を受けた場合や、合法的な米国の送達請求に応じた場合に、ユーザーに対しそれを通知することを禁じられていますか。

一般論としては、米国の提供者は、政府から請求があったことを顧客に通知することを禁じられていません。更に殆どの場合、政府からの請求を顧客に送り顧客にどう対応するか判断させる機会を与えています。但し、テロに関する調査、又は秘密諜報活動の様に本質的に守秘されるべき内容の場合等、限られた状況においてはサービス提供者が米国の警察職員からの請求に関しユーザーに通知をすることが法律上禁じられている場合もあります。

[1] この管轄に関する判断基準が示された最も有名な判例として *United States v. Bank of Nova Scotia*, 691 F.2d 1384 (11th Cir. 1982) があり、米国刑事手続の下で事業者が海外に所在する情報の開示を求められる可能性がどのような場合にあるのかを述べた、影響力のある先例として広く知られている。

６．　欧州のクラウド・サービス事業者の方が、米国のクラウド・サービス事業者より、米国政府の情報へのアクセスに対し、より高いレベルの保護を顧客に提供することができるのでしょうか。

米国における管轄の判断基準は、事業者が何処で会社を設立しているかではなく、その事業者が米国に存在があるか、及びそれ以外に米国と充分な接触があるか、にあります。よって、欧州のクラウド・サービス事業者であっても米国に存在する事業者であるならば、米国の警察機関からの要請に応じなければならない可能性があることは、米国のクラウド･サービス事業者と同様です。クラウド・コンピューティングにおける「規模の経済」に鑑みると、重要なクラウド･サービス事業者になることを目指す会社が、米国との相当な接触を避けることによって米国の管轄を免れるなどということができるのか、との疑問が当然生じます。更に、欧州のクラウド事業者は全て、他の多くの国と同様に米国が外国に所在する情報に対してもアクセスすることを可能とする、共助条約、及び裁判所から裁判所への協力依頼等、伝統的な法律手段による請求方法に従わなければなりません。

７．　米国のクラウド・サービス事業者が提供しているクラウド・サービスを利用することによって、欧州企業が EU のデータ保護指令に遵守することを妨げられてしまう可能性はありますか。

多くの米国のクラウド・サービス事業者は、EU と米国間のセーフ・ハーバー条約の規定を遵守しています。この条約は、米国企業のデータ保護の実務が、EU のデータ保護指令及び EU メンバー国の施行法におけるデータ保護適合性基準を満たしていることを示すことを可能とする正式な枠組みです。セーフ･ハーバー規定に準拠するクラウド事業者は、EU の指令において定義されている適切なプライバシー保護を提供するように義務付けられています。個別のクラウド事業者は、欧州の顧客に対し適切な契約上の約定をすることによって、そのセーフ・ハーバー遵守を強化することができます。

８．　欧州のユーザーのデータを米国政府に開示することは、米国と EU の間のセーフ･ハーバー条約の違反となりますか。

セーフ･ハーバー条約は、米国に存在が認められる如何なる事業者に対しても、その支配下にある情報を米国政府が開示させることを許容する、長年定着してきた米国法の運用を覆すものではありません。実際、それは、米国法を遵守することを許容しており、情報が米国国外に保管されている場合にも適用されます。又、セーフ・ハーバー条約は、セーフ･ハーバー原則への準拠を、国家安全保障、公共の利益、あるいは法の執行の要求を充足するに必要な範囲に限ることを明確に許容しています。

９．　パトリオット法の様な米国の法律は、他国の法律より域外適用の範囲が広く、従って、米国のクラウド・サービス事業者を利用した方が政府に情報アクセスされるリスクが大きいのではありませんか。

各国の警察機関がユーザー･データに対する管轄を主張するにあたって従うルールや手続は様々かもしれませんが、殆どすべてと言ってよいほどの多くの国は極めて範囲の広い管

轄を主張しています。例えば、ベルギーは、ベルギー所在の犯罪者に関連しているとベルギーの警察機関が主張しているということで、管轄を主張しました。イタリアの検察当局も同様に、イタリアにおける犯罪活動の調査に関る米国所在のデータに対し管轄を主張しています。又、英国及びフランスには、適用範囲が広いルールがあり、一定の場合に第三国に保管されているデータの押収が許容される程です。

１０．　欧州やその他外国に本社がある企業が、米国のクラウド・サービス事業者を利用した場合、そのデータはパトリオット法を含め適用される米国諸法に基づきアクセスの対象になりやすくなりますか。

クラウド・サービスを利用する企業が米国との接触又は米国に存在がある場合、その企業の情報が米国の警察機関によるアクセスの対象になる可能性は従前からあり、このことは、その企業の世界中の何処の施設に情報が保管されているか、サービス提供者によってホストされているかにかかわりません。米国に存在がない、又は米国と接触がない企業の場合でも、共助条約や裁判所から裁判所への協力依頼等、米国の警察機関が外国にある情報にアクセスすることを可能とする法的手段を有していることは、他の国と同様です。

１１．　米国政府のデータ請求の対象となる可能性がある企業はクラウド･サービス事業者だけですか。

長年確立している米国の法律においては、どの様な企業でも米国に存在があれば、（米国の企業であろうとなかろうと）その会社が占有、管理、又は支配するデータを政府に提供するよう請求されることがあります。これには米国外に保管されているデータ、及び子会社や関連会社の下にあるデータも含まれます。