【講演レポート】JIPDEC セミナー「個人情報のクラウド保管 実務における対応ポイント」

クラウドサービスと個人情報保護の実務

アマゾンウェブサービスジャパン合同会社　公共部法務統括　笹沼　穣氏

クラウドサービスとは

ここでは主に基盤系インフラのクラウドサービスを対象に説明します。

クラウドサービスは、インターネット（ブラウザ）を経由して、いつでもどこからでもアクセスでき、従量課金制で提供されるオンデマンドの、ストレージ、仮想サーバ、暗号化ツールなどのさまざまな IT リソースを誰でもがセルフサービスで利用できるサービスです。

クラウドサービス利用のメリットは DX 加速につながる点です。自社で物理的設備を持たず、その時必要なリソースだけを従量課金制で利用できるためコスト最適化が図られます。さらに最新技術を利用することや自分たちでシステムを管理しなくてもよく、業務に集中できます。また、クラウドのセキュリティには大規模な投資が行われているため、クラウドサービスを利用した方がセキュリティの面でも安全と考えられる面があります。

クラウドのセキュリティ概念と責任範囲

AWS を例に、クラウド事業者と利用者の責任分担について示します。（図 1）

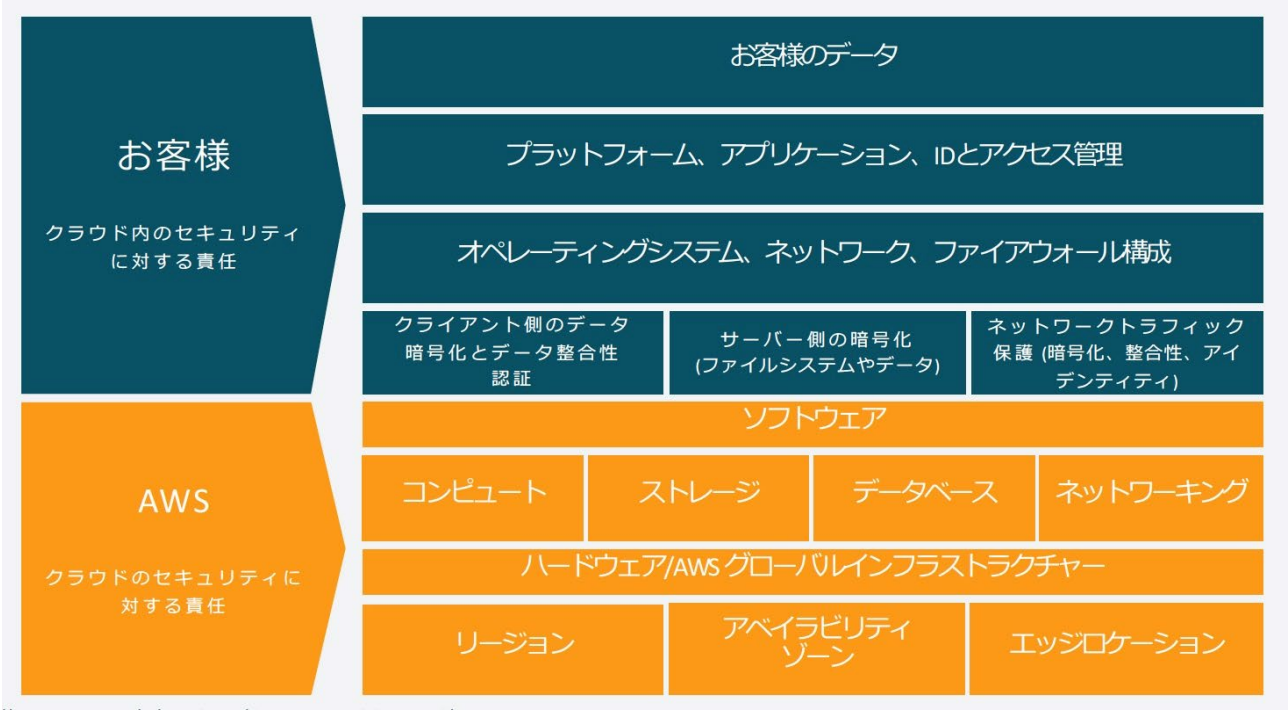

図１．クラウドサービスの責任共有モデル

クラウド事業者は、クラウド自体のセキュリティに対して責任を負います。一方、利用者側はクラウド環境内のセキュリティ、たとえばアクセス権限、アプリケーション開発、パスワード設定などが適切に行われているかに対して責任を持つことになります。各クラウドサービスにより責任範囲・境界点は異なりますが、利用者はクラウドサービスを適切に使うことで、パスワード管理やデータ保護、稼働率などの可視化が可能となり、利用者としての責任を果たしやすくなる、という点がクラウドサービスの特徴と言えるでしょう。なお、利用者側の分担範囲についてクラウド事業者側が何もしない、ということではなく、利用者に対しトレーニングや資料公開、コンサルティングなど支援も行うことで、多くのクラウド事業者は利用者が責任を果たせるような体制を整備しています。

クラウド事業者側責任の確認方法として、独立した第三者が発行した監査報告書（SOC 報告書）を参照するのがよいでしょう。また、国際認証標準の ISO27001 や ISO27017 の要件を満たしていたり、日本政府の ISMAP 登録事業者であれば、セキュリティの基準を満たしていることが確認できます。

重要なのは、クラウド事業者はすべてのサービス利用者に対し同一の多種多様なサービスを提供しており、利用者側でクラウドサービスを利用目的に応じて適切に利用するという考えです。

同じクラウドサービスを使っていても、大企業は個人情報をクラウドに保存する、個人事業主は自社サイトを作ることができますが、利用者側がどのように利用しているか、クラウド事業者は関与していないので、利用者側で自己のニーズに合わせた構築を行うこととなります。たとえば、情報を暗号化するか否かの判断について、個人情報なら暗号化をする必要があると思われますが、自社サイトに載せる写真は暗号化しないことになると思われるため、利用者側のニーズにより異なります。

クラウドサービス導入にあたる個人情報保護関連の論点

論点 1）クラウドサービスの利用は第三者提供および越境移転にあたるか？

・第三者提供

個人情報保護委員会の FAQ で明確にされていますが、クラウド事業者が個人データを取り扱わないこととなっている場合は、第三者提供、委託ともに該当しません。（「個人情報の保護に関する法律についてのガイドライン」に関する Q&A7-53 参照）※1　これがいわゆる「クラウド例外」です。

「取り扱わないこととなっている場合」とは、以下 2 つの条件を満たしている必要があります。

① 契約条項によってクラウド事業者がサーバに保存されている個人データを取り扱わない旨定められている、かつ

② 適切にアクセス制御が行われていること。

・個人データの越境移転規制

越境移転についても上記と同様の考え方となります。（同 Q＆A12-3 参照）

・クラウドにおける個人情報チェックポイント

クラウド利用が上記のクラウド例外に該当するか（第三者提供に該当しないか）は、以下の点を確認します。

① 契約条項にクラウド事業者が個人データを取り扱わない旨が定められているか
例）AWS カスタマーアグリーメント 1.4 条では「アマゾンは、利用者コンテンツ（データ）にアクセスしない」と記載されており、契約条件を満たしていると考えます。

② 適切にアクセス制御が行われているか
この点については、責任共有モデルに基づき、利用者側の責任でデータの暗号化やアクセス制御設定を行う、などの対応が考えられます。各クラウド事業者は暗号化ツールやアクセス管理ツール等も提供しているので、利用者は必要に応じてこれらのサービスを利用し、「適切なアクセス制御の実施」を担保することになります。クラウド例外が適用される場合、自社でシステムを管理していることと同じことになるので、利用者は適切な安全管理措置を講じる必要があることに留意してください。

※1「個人情報の保護に関する法律についてのガイドライン」に関するＱ＆Ａ

論点 2）米国 CLOUD 法によるデータアクセスのリスク

米国 CLOUD 法（Clarifying Lawful Overseas Use of Data 法）は、1980 年代に成立した法律に修正を加え 2018 年に施行された、クラウドができる前からある法律ですが、「米国籍のクラウド事業者が提供するクラウドサービスを利用してデータを保存すると、米 CLOUD 法によってデータが米国政府に筒抜けになる」と多くの誤解を生んでいる法律です。

本法は、裁判所の令状に基づき、捜査当局が犯罪の証拠となるデータに強制的にアクセスするための手続きを定めた法律です。捜査当局はあいまいな根拠で「探り出し」のために令状をとることはできず、具体的にどの犯罪が犯されて、どこに証拠があるかを裁判所に示す必要があることから、「データが米国政府に筒抜けになっている」というのは誤りです。

また、「CLOUD 法は米国籍のクラウド事業者にのみ適用される」と誤解されていますが、この点は米司法省が明確に否定しており※2、アメリカの裁判所の管轄権が及ぶ場合は、日本を含め世界中の事業者に本法が適用されます。

※2 米司法省の見解（The Purpose and Impact of the CLOUD Act – FAQs）

米 CLOUD 法に関しては、正しく理解するだけでなく、クラウド事業者がどう対応するかを確認しておくことが重要です。

- 政府からのデータの開示要請が不適切と考えられる場合、法的異議申し立てを行うか
- 開示要請を受けた場合、利用者に対し、当局からの要請があったことを通知するか
- 開示要請対応方針について情報公開を行っているか

さらに、クラウド事業者によっては、法令遵守のために開示請求についてどれぐらい対応しているのか、公開されている実績等を確認することも可能です。

米 CLOUD 法に限らず、全世界の政府からのデータ開示要請に対し、クラウド事業者がどのように対応しているかを確認するのがよいでしょう。

なお、上記の CLOUD 法に関する考えは、日本政府の見解※3 と齟齬ありません。

※3. 2022 年衆議院国会答弁での政府発言
2022 年 3 月）https://kokkai.ndl.go.jp/#/detail?minId=120804889X01220220325&spkNum=114&current=1
同年 11 月） https://kokkai.ndl.go.jp/#/detail?minId=121004889X00720221111&spkNum=101&single

講師プロフィール

アマゾンウェブサービスジャパン合同会社 公共部　法務統括
笹沼　穣氏

外国法事務弁護士。米国ニュージャージー州・ニューヨーク州弁護士。
ニュージャージー州裁判所、米系法律事務所での勤務を経て、2016 年にアマゾンに入社しアマゾンウェブサービスを担当。現在はアマゾンウェブサービスジャパン公共部門の法務統括。

本内容は、2023 年 9 月 5 日に開催された JIPDEC セミナー「個人情報のクラウド保管 実務における対応ポイント」講演内容を取りまとめたものです。