【講演レポート】JIPDECセミナー

クラウドを利用する際に遵守すべき個人情報保護法のルール

個人情報保護委員会事務局
参事官補佐　木村　一輝氏

クラウドを利用する場合の留意点

1）個人データ※1の第三者への「提供」（個人データの第三者提供）に該当するか

氏名などを含む特定の個人を識別することができる情報である「個人情報」を、容易に検索することができるように体系的にまとめた「個人データ」をクラウド事業者に対して提供していることになるか否か、という論点です。提供があるか否かは、クラウド事業者において個人データを“取り扱うこととなっているかどうか”が判断基準となり、提供に該当する場合は個人情報保護法第27条、第28条のルールを遵守しなければなりません。

契約条項において、当該クラウド事業者がサーバに保存された個人データを取り扱わない旨が定められており、適切にアクセス制御を行っている場合は取り扱わないと整理できます。ただし、提供に該当しない場合でも安全管理措置を講ずる必要があります。提供にあたるかは、実際に採用したサービスの条項や仕組みをしっかり確認して判断してください。

なお、同法人内において日本支店から海外支店のサーバに個人データを移転するなど、自社の範囲内での個人データの移転は第三者提供にはあたりません。

※1　個人情報保護委員会Q&A「「個人情報」と「個人データ」の違いは何か。」

2）「個人データの第三者提供」に該当した場合の個人情報保護法上のルール（外国のクラウド提供事業者を利用する場合を中心として）

法28条のルール

外国にあるクラウド事業者に個人データを第三者提供する場合は、法28条のルールを遵守しなければなりません。法28条1項・2項では、以下３つの例外を除き、原則として本人に対して情報提供をした上で、あらかじめ外国にある第三者への個人データの提供を認める旨の本人の同意を得なければならないと定められています。

・例外１　外国にある第三者が日本と同等の水準にあると認められる個人情報の保護に関する制度を有している国に所在する場合。具体的にはEUと英国に所在する場合で、この場合は法28条ではなく法27条のルールを遵守しなければならない。
・例外２　外国にある第三者が継続的に基準適合体制を整備している場合。この場合は法27条及び法28条3項のルールを遵守しなければならない。

・例外３　法27条１項各号に該当する場合（法令に基づく場合等）

本人同意の要否について

➢　日本にあるクラウド事業者の場合

原則として利用するクラウド事業者の所在が日本にある場合は法27条が適用されます。委託、事業継承、共同利用の場合など同意が不要な場合もありますが、原則として本人同意が必要となります。また、委託と整理できる場合は本人同意が不要となりますが、法25条における適切な委託先の選定や委託契約の締結、委託先での個人データの取り扱い状況の把握など「委託先の監督」は必要です。

➢　外国にあるクラウド事業者の場合

前述した通り、提供先がEUまたは英国、または基準適合体制が整備されている場合は、日本の事業者と同じく法27条が適用され、それ以外の場合は28条1項・2項が適用されます。

情報提供と同意

法28条1項・2項に従って、事業者はまず、あらかじめ本人に対して確実に認識できると考えられる適切な方法で情報（所在する外国の名称、当該外国の個人情報保護制度※2と提供先が講ずる個人情報保護のための措置）提供を行い、本人から外国にある第三者への提供を認める旨の同意を得られた場合に限って、個人データを提供することができます（図1）。当該外国の法制度等を確認することは本人同意を取得するために必要なものですが、事業者側が移転先の制度を調査することで理解を深める効果も期待できます。

なお、「適切な方法」の具体策は決められておらず、メール送付、WEBサイトでの掲示など、各事業者の工夫に委ねられる形になっています。

※2　個人情報保護委員会「外国における個人情報の保護に関する制度等の調査」（公表内容は調査時点の情報）

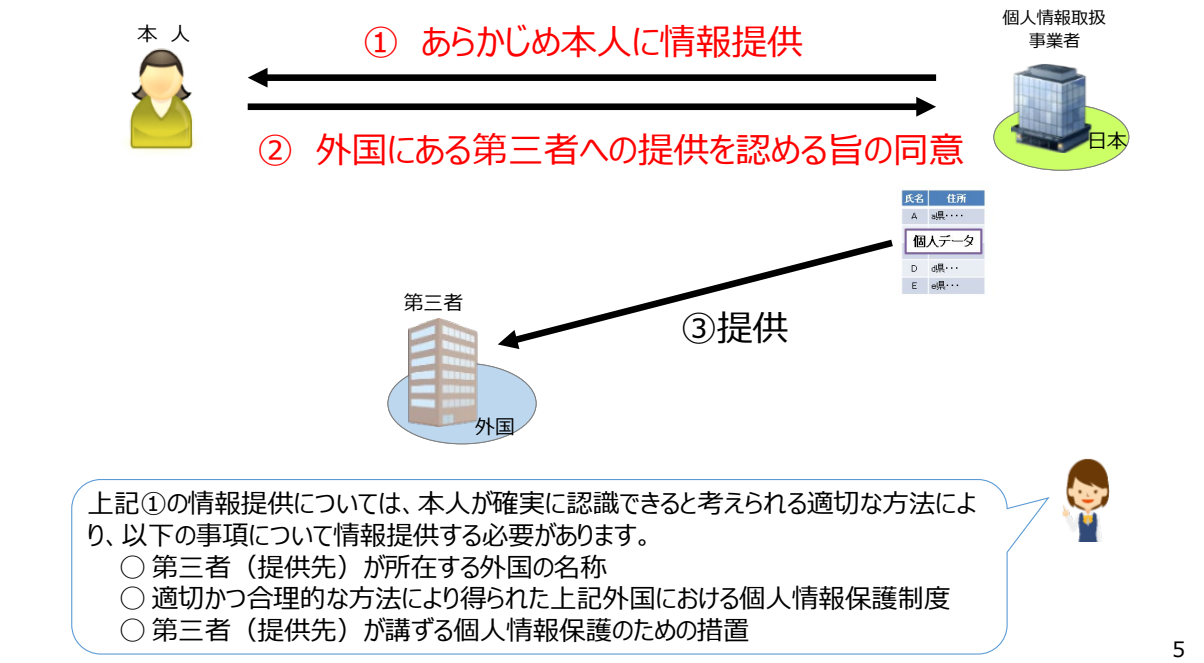

図1　クラウド事業者への第三者提供に該当する場合の留意点（法第28条1項・2項）

基準適合体制について

規則第16条（適切かつ合理的な方法）に定められた基準に適合する「基準適合体制」を整えた第三者に個人データを提供する場合も法27条に従い、また、法28条3項に基づく情報提供と必要な措置を講ずる必要があります。

まず、外国の第三者（提供先）に日本の個人情報取扱事業者と同じような措置を継続的に行う「基準適合体制」を整えてもらう必要があり、体制が整ってはじめて個人データを提供することができます。ただし、提供後も第三者の相当措置の実施状況などの定期的な確認や、支障が生じた際の措置、継続実施が困難と判断した場合の提供の停止など、継続的に必要な措置を講ずる必要もあります。また、本人から必要な措置に関する情報開示の求めがあった場合はそれに応じる必要もあります。

3）クラウドを利用する場合の安全管理措置（外的環境の把握を含む）

クラウド事業者に対して個人データを提供している場合、委託と整理しているのであれば、自社のデータとして安全管理措置※3を講じるとともに、委託先の監督をしなければなりません。また、クラウド事業者に対して個人データを提供していない場合でも、個人データに対して安全管理措置を講じなければなりません。

各事業者は、最高経営責任者の下、基本方針を策定し、組織的、人的、物理的、技術的安全管理措置を行います。また、外的環境の把握も必須です。外国で個人データを取り扱う場合には、思わぬ権利侵害につながる可能性もあるため当該外国の個人情報の保護に関する制度等を把握した上で、安全管理措置を実施してください。

なお、外国のクラウド事業者が提供するサービスの場合、または個人データを保存するサーバが外国にある場合には、外的環境の把握における「外国においてデータを取り扱う場合」に該当します（図2）。

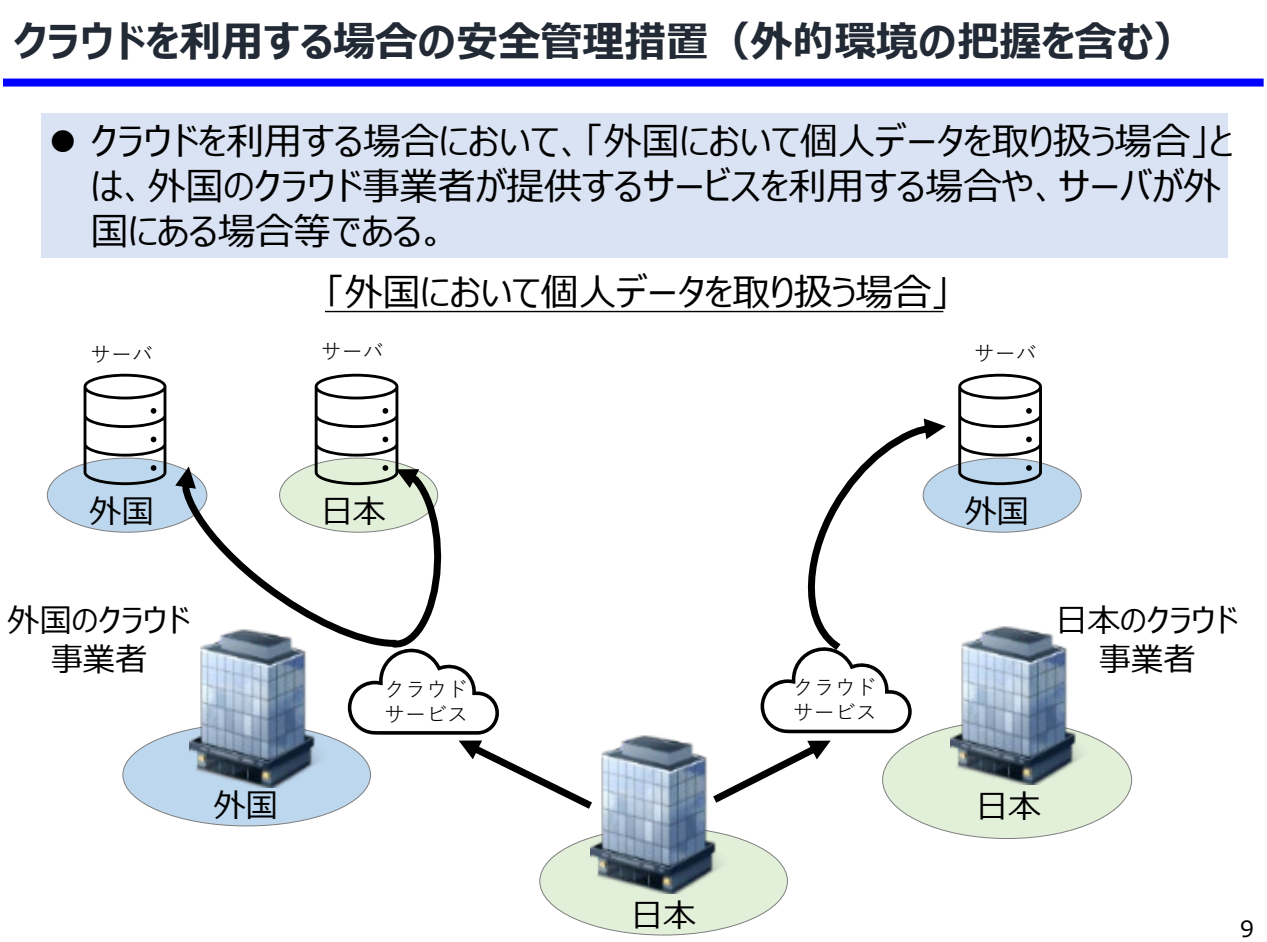

図2　クラウドを利用する場合の安全管理措置（外的環境の把握を含む）

近年、クラウド利用時における公開範囲の設定ミス、IDパスワードの使いまわしや初期設定の変更忘れなどによる情報漏洩等も頻繁に発生しています。クラウドサービスを利用する際の安全管理措置については、各事業者がしっかりと行うようにしてください。

※3　①個人情報保護委員会「講ずべき安全管理措置の内容」
②個人情報保護委員会「WARNING～クラウドサービスやテレワーク環境を利用する際の個人情報の漏えいに関する注意喚起～」

4）クラウドを利用する場合の安全管理措置の公表等

前提として、「保有個人データ」を取り扱う際は下記①～⑤を公表する必要があります。

①個人情報取扱事業者の氏名又は名称等
②全ての保有個人データの利用目的
③保有個人データの開示等の請求に応じる手続等
④保有個人データの安全管理のために講じた措置
⑤保有個人データの取扱いに関する苦情の申出先（認定個人情報保護団体の対象事業者である場合は、その団体の名称等を含む。）

中でも外国において個人データを取り扱う場合には、「④保有個人データの安全管理のために講じた措置」に注意が必要です。安全管理措置のために講じた措置として、個人データを取り扱う外国（サーバ設置国等）の名称とともに、当該外国の法制度を把握した上で講じた措置の内容を明記してください。

なお、保有個人データの公表等の方法としては自社のプライバシーポリシーに掲げている事業者も多くいますし、本人の求めに応じて遅滞なく回答することでも対応可能です。

利用するクラウドサービスの内容、サーバがある国の個人情報保護制度を十分に理解した上でそれぞれに適した安全管理措置を講じることが必要です。

本日ご説明した内容以外の例外や詳細については、個人情報保護委員会が公表しているガイドラインやQ&Aのほか、個人情報保護法相談ダイヤルも設けていますのでご不明な点についてはお問い合わせください。

個人情報保護委員会事務局　参事官補佐
木村　一輝氏

2015年弁護士登録（68期）
丸の内総合法律事務所入所、2022年1月より個人情報保護委員会事務局参事官補佐（任期付公務員）として勤務。

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。