人事労務管理のためのサービスをクラウド環境を利用して開発・提供する場合及び当該サービスを利用する場合における、個人情報保護法上の安全管理措置及び委託先の監督等に関する留意点について（注意喚起）

令和６年 12 月 17 日
個人情報保護委員会

当委員会は、クラウド上で提供され、多数の企業において利用されている人事労務管理サービスが不正アクセスを受け、個人番号（マイナンバー）を含む個人データ（以下「個人データ」という。）が漏えいした事案（以下「本事案」という。）について、個人情報の保護に関する法律（平成 15 年法律第 57 号。以下「個人情報保護法」という。）及び行政手続における特定の個人を識別するための番号の利用等に関する法律（平成 25 年法律第 27 号。以下「番号法」という。）上の問題点を、調査・検討しました。

当該調査・検討の結果を踏まえ、以下のとおり、安全管理措置及び委託先の監督に関する留意点を整理しました。

人事労務管理サービス等を開発し提供する個人情報取扱事業者（委託先）及びサービスを利用して従業者の個人データを取り扱う個人情報取扱事業者（委託元）[1]におかれましては、以下の点に留意の上、当該個人データの取扱いを行っていただきますようお願いします。

１　事案

(1)　概要

A社は、クラウド上で提供される、人事労務管理を行うためのシステム（以下「本件システム」という。）を開発・運用し、顧客である企業や店舗（以下「顧客企業等」という。）にサービスを提供していました。あるとき、本件システムに保管されていた顧客企業等が取り扱う個人データ（以下、「本件個人データ」という。）について、外部の者がダウンロードしたことにより「漏えい」が生じました。

(2)　本件システムで管理されていた個人データ

本件システムは、顧客企業等が、クラウド環境で従業者の人事労務管理を行うためのシステムであり、本件システムで保管されていた個人データには、多数の顧客企業等の従業者の氏名、生年月日、住所等に加え、雇用契約書、運転免許証、住民票、健康診断書、銀行口座の情報を示すキャッシュカードの券面[2]、マイナンバーカード等の画像が含まれていました。

---

[1] 番号法における個人番号利用事務等実施者を含む。
[2] キャッシュカードの種類によっては、券面にクレジットカード番号や有効期限が記載されているものがありました。

(3)　Ａ社における個人データの取扱い（委託）

顧客企業等は、本件個人データを、本件システムの利用を通じて本件システム内に保管し、管理していました。そして、Ａ社は、本件システムのサービス提供に伴い、顧客企業等から本件個人データの取扱いの委託を受けていました。

つまり、顧客企業等が本件個人データの取扱いについての委託元であり、Ａ社が委託先という関係にありました。

(4)　漏えい発覚の経緯

Ａ社がサービス提供を開始してから数年後、その頃にＡ社の親会社となった会社が、本件システムに関するセキュリティ調査を行いました。

その結果、Ａ社における本件システムの開発時に、本件システム上で取り扱われる本件個人データを保存するためのクラウドストレージサーバ（以下「本件サーバ」という。）内のバケットの設定（公開・非公開）に関する問題点及びファイルリストの設定（公開・非公開）に関するミスが存在し、サービス提供開始時から、特定の操作を行うことで、本件サーバに外部からアクセスが可能な状態となっていたことが判明しました。

また、その後の調査の結果、外部の者が本件サーバにアクセスし、その時点で本件サーバに保管されていた個人データ全てについて、ダウンロードされた痕跡があることが発覚し、漏えいが生じたことが判明しました[3]。

２　Ａ社（委託先）に関する留意点

(1)　本件システムに保管される個人データの項目

本件システムは、人事労務管理業務を電子化し簡便化することを目的とするものです。前記１(2)のとおり、本件システムで保管されていた個人データには、顧客企業等の多数の従業者の氏名、生年月日、住所等の個人データに加え、雇用契約書、運転免許証、住民票、健康診断書、給与を振り込むための銀行口座の情報を示すキャッシュカードの券面、マイナンバーカード等の画像が含まれていました。

本件個人データには、病歴、クレジットカード情報、マイナンバー等の、漏えい等した場合に本人の重大な権利利益の侵害が発生するおそれの大きいものが含まれています。また、住民票、運転免許証、マイナンバーカード等のむやみに他人に見せるべきでない書類を撮影した画像が含まれていました。

(2)　安全管理措置

個人情報保護法第 23 条において、「個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又は毀損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じなければならない」とされています[4]。

---

[3] ただし、Ａ社の報告によれば、現在のところ二次被害については確認されていないとのことです。

[4] なお、番号法第 12 条において、個人番号利用事務実施者及び個人番号関係事務実施者は、「個人番号の漏えい、滅失又は毀損の防止その他の個人番号の適切な管理のために必要な措置を講じなければならない」とされています。

そして、個人情報の保護に関する法律についてのガイドライン（通則編）（以下「個人情報保護法ガイドライン」という。）の「3-4-2 安全管理措置（法第 23 条関係）」においては、以下のとおり規定しています。

> 個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又は毀損（以下「漏えい等」という。）の防止その他の個人データの安全管理のため、必要かつ適切な措置を講じなければならないが、当該措置は、個人データが漏えい等をした場合に本人が被る権利利益の侵害の大きさを考慮し、事業の規模及び性質、個人データの取扱状況（取り扱う個人データの性質及び量を含む。）、個人データを記録した媒体の性質等に起因するリスクに応じて、必要かつ適切な内容としなければならない。

本事案のように、漏えい等をした場合に本人の重大な権利利益の侵害が発生するおそれのある個人データを、クラウド環境を利用したシステム上で顧客のために大量に取り扱うサービスを開発・提供する場合には、特にアクセス制御の点や不正アクセス等を防止するための措置について、開発段階から注意して設計し、ユーザーの利便性に偏らない安全なシステムを構築し、サービス提供をすることが重要です[5]。

また、システムに係る網羅的な脆弱性診断等を実施するなど、継続的な見直しも大切です[6]。

３　顧客企業等（委託元）に関する留意点

当委員会は、委託元である個人情報取扱事業者のうち、本件個人データに係る本人数の多い事業者に対し、委託先に対する監督状況についての報告徴収を行い、報告された内容及び追加の調査内容に基づき、検討を行いました。

個人情報保護法第 25 条において、「個人情報取扱事業者は、個人データの取扱いの全部又は一部を委託する場合は、その取扱いを委託された個人データの安全管理が図られるよう、委託を受けた者に対する必要かつ適切な監督を行わなければならない」とされています[7]。そして、個人情報保護法ガイドライン 3-4-4 は、以下のとおり規定しています。

> 取扱いを委託する個人データの内容を踏まえ、個人データが漏えい等をした場合に本人が被る権利利益の侵害の大きさを考慮し、委託する事業の規模及び性質、個人データの取扱状況（取り扱う個人データの性質及び量を含む。）等に起因する

[5] 組織的安全管理措置及び技術的安全管理措置（個人情報保護法ガイドライン 10-3 及び 10-6、特定個人情報の適正な取扱いに関するガイドライン（事業者編）（別添１）2-C 及び 2-F 参照）等が問題となります。

[6] なお、A社からは、脆弱性診断の強化等の再発防止策を策定・実施していくとの報告を受けています。

[7] また、番号法第 11 条において、「個人番号利用事務等の全部又は一部の委託をする者は、当該委託に係る個人番号利用事務等において取り扱う特定個人情報の安全管理が図られるよう、当該委託を受けた者に対する必要かつ適切な監督を行わなければならない」とされています。

リスクに応じて、次の（1）から（3）までに掲げる必要かつ適切な措置を講じなければならない。

(1)　委託先の選定について

顧客企業等の多くは、事前に、A社に対し、セキュリティ対策の取組状況を確認していることが認められました。また、A社も、顧客企業等へのサービス提案時に自社のセキュリティ対策について説明等を行っていました。

(2)　委託契約の締結について

ア　多くの顧客企業等は、A社が提示する利用規約（以下「本件利用規約」という。）についてのみ合意しており、覚書等は締結していませんでした。本件利用規約の合意のみであったこと自体が、個人情報保護法上や番号法上、直ちに問題というわけではありません。問題は、本件利用規約において、本件個人データの取扱いについてどのような内容が規定されていたかという点です。

この点、本件システムは、漏えい等した場合に本人の重大な権利利益の侵害が発生するおそれのある個人データを大量に保管するシステムであるにもかかわらず、本件利用規約には、個人情報保護法ガイドライン 3-4-4(2)に掲げる「個人データの取扱いに関する、必要かつ適切な安全管理措置として、委託元、委託先の双方が同意した内容」や、「委託先における委託された個人データの取扱状況を委託元が合理的に把握すること」に関する規定はありませんでした（本件利用規約においては、一般的な秘密保持に関する事項や、A社における本件個人データの取扱いについて同社のプライバシーポリシー[8]に従うという点が記載されるにとどまっていました。）。

イ　他方、一部の顧客企業等は、本件利用規約以外に別途覚書等を締結していました。これらの覚書等には、A社における本件個人データの取扱いに係る安全管理措置、その実施状況の報告、監査等について規定されていました。

また、A社における安全管理措置に関する条項が明記された「契約書」や「覚書」という形ではないものの、当事者双方合意の下、A社における本件個人データの安全管理措置に関するチェックシートを用いて、契約締結前及び契約締結後も定期的に、A社における本件個人データの取扱状況を確認していた顧客企業等も認められました。

(3)　委託先における本件個人データの取扱状況の把握について

ア　多くの顧客企業等においては、定期的な監査の実施や、A社からの定期的な安全管理措置に関する報告の受領等の、A社における本件個人データの取扱状況の把握に関する措置は実施されていませんでした。

[8] なお、A社のプライバシーポリシーにおいて、安全管理措置に関する記載はありませんでした。

イ　他方、一部の顧客企業等においては、自ら作成した安全管理措置に関するチェックシートを用いて、A社に対し報告を求める等、本件個人データの取扱状況を把握するための一定の措置を実施していることが認められました。

(4)　小括

ア　本事案では、以上のとおり委託元である顧客企業等を調査した結果、一部の顧客企業等においては、個人情報保護法ガイドライン等に照らし、必要かつ適切な監督が一定程度行われていることが認められました。他方、多くの顧客企業等においては、漏えい等をした場合に本人の重大な権利利益の侵害が発生するおそれのある個人データを含む、大量の個人データの取扱いの委託を行っている本件の状況に照らし、監督が不十分であることが認められました。

イ　委託先に対する監督を一定程度実施していたとしても、委託先における個人データの漏えい等事態を回避することができなかったと思われるケースもありますが、平時において契約に安全管理措置に関する規定を設けたり、委託先における安全管理に関するチェックシート等を利用したりすることにより、開発・提供事業者（委託先）と利用事業者（委託元）の双方において、個人データの安全管理について意識を高めていただくことにより、漏えい等事態が生ずる可能性を低減できるものと考えます。

4　留意点のまとめ

(1)　委託先における留意点

本事案のように、漏えい等をした場合に本人の重大な権利利益の侵害が発生するおそれのある個人データを、クラウド環境を利用したシステム上で顧客のために大量に取り扱うサービスを開発・提供する場合には、特にアクセス制御の点や不正アクセス等を防止するための措置について、開発段階から注意して設計し、ユーザーの利便性に偏らない安全なシステムを構築し、サービス提供をすることが重要です。

人事労務管理のためのクラウドサービスを提供する事業者におかれては、取り扱う個人データの性質及び量に応じて、近年における不正アクセスの動向にも注意しつつ、必要な安全管理措置を講じていただき、安全なサービスの開発・提供に努めていただくようお願いします。

なお、クラウドサービスの提供に際しては、当該クラウドサービスを提供する事業者において、あらかじめ作成した定型的な利用規約等について合意することで、当該クラウドサービスの利用に係る契約を締結する場合も多いと思います。クラウドサービスを提供する事業者におかれては、あらかじめ、必要かつ適切な安全管理措置等に係る記載を盛り込んだ利用規約等の整備に努めていただくようお願いいたします。

(2) 委託元における留意点

本件システムのようなクラウドサービスを利用して、漏えい等をした場合に本人の重大な権利利益の侵害が発生するおそれのある個人データを含む大量の従業者等の個人データを継続的に管理していく場合には、そのようなリスクに応じた措置を講ずる必要があります。

本事案では、前記３のとおり、利用規約以外に個人情報保護法のガイドライン等の記述に従って別途覚書等を作成し、委託先に対して個人データに係る安全管理措置を義務付けるチェックシートなどを用いたりするなどして委託先における個人データの取扱い状況を把握する等の措置を講じている個人情報取扱事業者も認められました。

委託元となる個人情報取扱事業者におかれましては、委託する個人データの性質及び量に応じて、委託元として、必要かつ適切な委託先の監督を行っていただくようお願いします。

以　上