NISHIMURA & ASAHI

西村あさひ法律事務所

# 個人情報保護法上求められる安全管理措置等の実務上のポイント

個人情報保護・データ保護規制ニューズレター　2022 年 12 月 27 日


執筆者：

E-mail 岩瀬 ひとみ
E-mail 菊地 浩之
E-mail 河合 優子
E-mail 村田 知信
E-mail 五十嵐 チカ
E-mail 松本 絢子
E-mail 菅 悠人
E-mail 山﨑 泰和


目次



## Ⅰ 個人情報保護法上求められる安全管理措置等の実務上のポイント

### 1. はじめに

個人情報保護法は、個人情報取扱事業者に対して、個人情報を取り扱う際には、個人情報の安全管理のために必要かつ適切な措置を講じ、また個人情報を取り扱わせる従業員及び委託先の必要かつ適切な監督を行わなければならないと定めているが、実務上講じるべき具体的な措置は法律の規定からは必ずしも明らかではない。他方で、個人情報保護委員会によれば、委員会へ直接報告された個人データの漏えい等の事案は、2022 年度上半期において 1,587 件にのぼり、前年度上半期と比べても件数は増加傾向にあるとのことであり、個人情報保護委員会は、個人情報取扱事業者に対して、個人情報を適正に取り扱うよう、注意喚起を行っている[1]。また、近年、必要かつ適切な措置や監督が行われていなかったことを理由として、個人情報保護委員会が事業者に対して指導等の行政処分を行う事案が発生している。

本稿では、実務上講じるべき安全管理措置等について、個人情報保護委員会が公表しているガイドラインにおける安全管理措置等に関する解説を概観するとともに、実際に個人情報保護委員会が事業者に対して指導を行った事案を概観し、講じなければならない措置の内容や程度について検討する。

### 2. 安全管理措置等に関する個人情報保護法上の規定

個人情報保護法は、個人情報取扱事業者に対して、その取り扱う個人データ(個人情報データベース等を構成する個人情報をいう(同法 16 条 1 項、3 項)。個人情報取扱事業者が保有する個人情報は多くの場合、「個人データ」に該当すると考えられる。)について、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(いわゆる「安全管理措置」)を講じなければならないと定めている(同法 23 条)。また、同法は、個人データの安全管理が図られるよう個人データを取り扱わせる従業員や、個人データの取扱いを委託する委託先に対して、必要かつ適切な監督を行わなければならないとしている(同法 24 条、25 条。以下従業員及び委託先の監督とあわせて「安全管理措置等」という。)。

もっとも、個人情報保護法は、「必要かつ適切な」措置や監督を行う義務を定めるにとどまり、具体的に講じなければならない措置を明らかにはしていない。そこで、以下では、ガイドラインの記載や、公表されている実際の事案を概観する。

---

1　https://www.ppc.go.jp/files/pdf/221109_chuui_jigyousha.pdf

## 3. ガイドラインにおける安全管理措置等

### (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(通則編)

(i) 安全管理措置

「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)」[2](個人情報保護委員会、2022 年 9 月一部改正)(以下「ガイドライン(通則編)」という。)では、安全管理措置について、「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」と定め(51～52頁)、その具体的内容については、「10(別添) 講ずべき安全管理措置の内容」に記載して説明している。

「10(別添) 講ずべき安全管理措置の内容」が定める安全管理措置の具体的内容は、(a)基本方針の策定、(b)個人データの取扱いに係る規律の整備、(c)組織的安全管理措置、(d)人的安全管理措置、(e)物的安全管理措置、(f)技術的安全管理措置、(g)外的環境の把握、の 7 項目に分けて整理されており、それぞれの項目に対して講ずべき具体的な措置が例示されている。ただし、安全管理措置を講ずるための具体的な手法の例示については、「リスクに応じて、必要かつ適切な内容とすべきものであるため、必ずしも次に掲げる例示の内容の全てを講じなければならないわけではなく、また、適切な手法はこれらの例示の内容に限られない。」としており(162 頁)、具体的にいかなる内容の安全管理措置を講ずれば「必要かつ適切な」安全管理措置を実現したことになるのかは、例示されている手法からは、直ちに読み取ることは難しい。

なお、安全管理措置の具体的な手法として、概ね以下のような措置が例示として挙げられている。

(a) 基本方針の策定

個人データの適正な取扱いの確保について組織として取り組むために、例えば「事業者の名称」、「関係法令・ガイドライン等の遵守」、「安全管理措置に関する事項」、「質問及び苦情処理の窓口」等の項目を含む基本方針を定めることとされている。

(b) 個人データの取扱いに係る規律の整備

個人データの漏えい等の防止その他の個人データの安全管理のために、個人データの取得、利用、保存、提供、削除・廃棄等の段階ごとに、取扱方法、責任者・担当者及びその任務等について定める個人データの取扱規程を策定することが考えられるとしている。

(c) 組織的安全管理措置

組織的安全管理措置には、例えば、組織体制の整備、あらかじめ整備された個人データの取扱いに係る規律に従った運用及び利用状況の記録、個人データの取扱状況を確認するための手段の整備、漏えい等事案の発生又は兆候を把握した場合に適切かつ迅速に対応するための体制の整備、並びに安全管理措置の評価、見直し及び改善等が挙げられている。

(d) 人的安全管理措置

人的安全管理措置については、従業者に、個人データの適正な取扱いを周知徹底するとともに適切な教育を行わなければならない、と説明されており、具体的には、従業者への定期的な研修を行うことや、就業規則等に個人データについての秘密保持に関する事項を盛り込むことが例示されている。

2 https://www.ppc.go.jp/personalinfo/legal/guidelines_tsusoku/

(e)　物的安全管理措置

物的安全管理措置として、個人情報データベース等を取り扱うサーバやメインコンピュータ等の重要な情報システムを管理する区域、及びその他の個人データを取り扱う事務を実施する区域について適切な管理を行うこと、個人データを取り扱う機器、電子媒体及び書類等の盗難又は紛失等を防止するために、適切な管理を行うこと、個人データが記録された電子媒体又は書類等を持ち運ぶ場合、容易に個人データが判明しないよう、安全な方策を講じること、及び個人データを削除し又は個人データが記録された機器、電子媒体等を廃棄する場合は、復元不可能な手段で行うこと、が挙げられている。

(f)　技術的安全管理措置

技術的安全管理措置については、個人データを取り扱う情報システムの適切なアクセス制御を行うとともに、当該情報システムを外部からの不正アクセス又は不正ソフトウェアから保護する仕組みを導入し、また情報システムの使用に伴う個人データの漏えい等を防止するための措置を講じ、これらを適切に運用しなければならない、としている。

(g)　外的環境の把握

個人情報取扱事業者が、外国において個人データを取り扱う場合、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、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、としている。

(ii)　従業者の監督

ガイドライン(通則編)は、個人情報取扱事業者は、その従業者に個人データを取り扱わせるに当たって、安全管理措置を遵守させるように、当該従業員に対し必要かつ適切な監督をしなければならない、としている。個人情報取扱事業者は、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等に起因するリスクに応じて、必要かつ適切な措置を講ずるべきこととされている点は、安全管理措置と同様である。

(iii)　委託先の監督

ガイドライン(通則編)は、個人情報取扱事業者は、個人情報の全部又は一部を委託することにより他の者に取り扱わせる場合には、委託先に対して、必要かつ適切な監督を行うものとしている。具体的には、委託先において自らが講じるべき安全管理措置と同等の措置が講じられるよう監督するとともに、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等に起因するリスクに応じて、(a)適切な委託先の選定、(b)委託契約の締結、特に当該契約に委託先において講ずるべき安全管理措置や個人情報の取扱い状況を合理的に把握できるための規定を盛り込むこと、(c)委託先に定期的に監査を行う等により、委託契約に盛り込んだ安全管理措置等が実施されている状況を把握するべきものとしている。

(iv)　小括

以上のように、ガイドライン(通則編)においては、講ずべき安全管理措置等について、取り扱う個人データの内容、個人データが漏えいした場合に本人が被る影響の大きさ等を考慮し、必要かつ適切な措置を講じるべきものであることが強調されている。また、具体的に講じるべき措置についても例示等することにより説明されており、実務上安全管理措置等として講じる対策を検討する際には参考になる。一方で、「必要かつ適切な」安全管理措置等を講じるべき個人情報保護法上の義務を果たしたといえるために、どの程度の範囲で安全管理措置等を講じればよいのかという点は、個別具体的な事情を考慮しての各自の判断に委ねられており、必ずしも明確にその基準を読み取ることはできない。

### (2) 特定分野ガイドライン

個人情報保護委員会は、ガイドライン(通則編)を含む個人情報取扱事業者一般を対象とするガイドラインの他に、特定の事業分野を対象とするガイドラインとして、(1)金融関連分野、(2)医療関連分野、及び(3)情報通信分野向けにガイドライン等を公表している [3]。これらの特定の事業分野向けのガイドラインにも、個人情報取扱事業者が講じるべき安全管理措置等に関する記載がある。各事業分野向けのガイドラインにおける安全管理措置等に関する記載は、他の事業分野にも一般的に通用するような記載も多いため、以下ではそのうち特徴的な記載を中心に紹介する。

#### (i) 金融関連分野ガイドライン

金融関連分野向けのガイドラインとしては、「金融分野における個人情報保護に関するガイドライン」、「金融分野における個人情報保護に関するガイドラインの安全管理措置等についての実務指針」、「信用分野における個人情報保護に関するガイドライン」、「債権管理回収業分野における個人情報保護に関するガイドライン」(いずれも、2022 年 4 月一部改正)が公表されている。

「金融分野における個人情報保護に関するガイドライン」(以下「金融分野ガイドライン」という。)では、個人情報取扱事業者が講じるべき安全管理措置を、個人データの安全管理に係る基本方針・取扱規程等の整備(8 条 7 項)と個人データの安全管理に係る実施体制の整備(8 条 8 項)に分けて整理している。さらに、個人データの安全管理に係る基本方針・取扱規程等の整備として講じるべき措置として「組織的安全管理措置」、また個人データの安全管理に係る実施体制の整備として、「組織的安全管理措置」、「人的安全管理措置」、「物理的安全管理措置」及び「技術的安全管理措置」を講じるべきものと整理している。

加えて、金融分野ガイドラインでは、従業員の監督について講じるべき対策を以下のとおり具体的に説明している(9 条 3 項)。以下の説明は、金融分野に限らず参考になる。

- 従業者が、在職中及びその職を退いた後において、その業務に関して知り得た個人データを第三者に知らせ、又は利用目的外に使用しないことを内容とする契約等を採用時等に締結すること。
- 個人データの適正な取扱いのための取扱規程の策定を通じた従業者の役割・責任の明確化及び従業者への安全管理義務の周知徹底、教育及び訓練を行うこと。
- 従業者による個人データの持出し等を防ぐため、社内での安全管理措置に定めた事項の遵守状況等の確認及び従業者における個人データの保護に対する点検及び監査制度を整備すること。

さらに、金融分野における安全管理措置等については、「金融分野における個人情報保護に関するガイドラインの安全管理措置等についての実務指針」が定められており、講じるべき安全管理措置の内容が具体的に説明されている。

「債権管理回収業分野における個人情報保護に関するガイドライン」では、以下のとおり、特に委託先の監督について詳細に説明しており、委託契約に盛り込む事項として、以下の様な事項を明記するべきものとしている(第 6、3(3))。こちらも、金融分野に限らず参考になる。

(委託契約に盛り込む事項)
- 委託先の秘密の保持に関する事項
- 委託者及び受託者の責任の明確化に関する事項
- 再委託に関する事項(再委託の禁止又は再委託する場合の個人データ保護の水準の条件等)
- 個人データの取扱いの制限に関する事項(委託契約範囲外の取扱いの禁止等)
- 個人データの取扱いに係る安全管理措置に関する事項
- 個人データの管理状況の報告及び監査に関する事項
- 個人データの漏えい等発生時の対処に関する事項

---

3 https://www.ppc.go.jp/personalinfo/legal/guidelines/

・　委託終了時における個人データの返還・消去に関する事項
・　契約に違反した場合における契約解除の措置その他必要事項(「その他必要事項」としては、善良なる管理者の注意義務及び漏えい等事案発生時における被害に対する損害賠償責任などがある。)

(ii)　医療関連分野ガイドライン等

医療関連分野向けのガイドラインとしては、「医療・介護関係事業者における個人情報の適切な取扱いのためのガイダンス」、「健康保険組合等における個人情報の適切な取扱いのためのガイダンス」、「国民健康保険組合における個人情報の適切な取扱いのためのガイダンス」、「国民健康保健団体連合会等における個人情報の適切な取扱いのためのガイダンス」及び「経済産業分野のうち個人遺伝情報を用いた事業分野における個人情報保護ガイドライン」(いずれも、2022 年 3 月一部改正)が公表されている。

「医療・介護関係事業者における個人情報の適切な取扱いのためのガイダンス」においては、講じるべき安全管理措置として、ガイドライン(通則編)に記載されているような事項に加えて、個人データの保管及び不要となった個人データの廃棄、消去について記載されている(Ⅳ、7、(2)⑧及び⑨)。これらは、患者のカルテ等、機微性の高い個人情報を長期間保管する医療・介護関係事業者の特性を加味した記載であるものと考えられる。

(個人データの保存)
・　個人データを長期にわたって保存する場合には、保存媒体の劣化防止など個人データが消失しないよう適切に保存する。
・　個人データの保存に当たっては、本人からの照会等に対応する場合など必要なときに迅速に対応できるよう、インデックスの整備など検索可能な状態で保存しておく。

(不要となった個人データの廃棄、消去)
・　不要となった個人データを廃棄する場合には、焼却や溶解など、個人データを復元不可能な形にして廃棄する。
・　個人データを取り扱った情報機器を廃棄する場合は、記憶装置内の個人データを復元不可能な形に消去して廃棄する。
・　これらの廃棄業務を委託する場合には、個人データの取扱いについても委託契約において明確に定める。

(iii)　情報通信分野ガイドライン

情報通信関連分野向けのガイドラインとして、「電気通信事業における個人情報保護に関するガイドライン」(2022 年 3 月一部改正)、「放送受信者等の個人情報保護に関するガイドライン」(2022 年 4 月一部改正)、「郵便事業分野における個人情報保護に関するガイドライン」(2022 年一部改正)、「信書便事業分野における個人情報保護に関するガイドライン」(2022 年一部改正)が公表されている。

それぞれのガイドラインでは、安全管理措置の例示が示されているが、内容は概ねガイドライン(通則編)の「10(別添) 講ずべき安全管理措置の内容」と同様である。

## 4.　個人情報保護委員会による公表案件等

個人情報保護委員会は、個人情報保護法 144 条に基づき指導等の行政処分を行った場合には、当該案件の概要を公表している。そして、近時、個人情報保護法上要請される安全管理措置が実施されていなかったこと等を指摘する案件が公表されているため、以下では公表案件の概要を概観する。

### (1)　株式会社メタップスペイメントに対する指導 [4](公表日:2022 年 7 月 13 日)

株式会社メタップスペイメント(以下「メタップス」という。)は決済代行業者であり、加盟店を通じて一般消費者である顧客の決済

4　https://www.ppc.go.jp/news/press/2022/20220713/

情報を取得し、また加盟店から任意で提供を受け、顧客の個人情報等の個人情報を恒常的に多量に取り扱っていた。2021 年 8 月 2 日から 2022 年 1 月 25 日にわたって、メタップスが設置したデータセンターサーバーに複数回の不正アクセスがあり、その結果、約 46 万件の個人情報が流出した [5]。

本件の個人情報保護委員会の公表資料では以下の点が指摘されている。

- メタップスでは、情報セキュリティ基本規程上、個人データを含む自社が保有する情報資産について棚卸しを実施することになっていたものの、情報資産管理台帳の整備がされていなかったため、棚卸しが適切に実施されず、どのシステムにおいて情報資産を取り扱っているかすら把握していなかった。
- また、個人データの取扱状況についての監査・点検も一部実施しておらず、その重要性に見合った取扱いを行っていなかった。内部監査規程等において規程の外形のみ整備していたものの、それを実行するための適切な人員配置等の実質を伴わず、内部監査が機能していなかった。
- メタップスでは、多数の個人情報を恒常的に取り扱うという性質を踏まえると、個人情報の適正な取扱いの確保について、組織としてより重点的に取り組む必要があった。

**(2) BIPROGY 株式会社に対する指導 [6](公表日:2022 年 9 月 21 日)**

BIPROGY 株式会社(以下「BIPROGY」という。)は、多くの行政機関等からシステム開発・保守業務の委託を受けていた IT サービス事業者であり、尼崎市からは臨時特別給付金支給事務を受託していた。本件は、尼崎市における臨時特別給付金支給事務に従事していた BIPROGY の再々委託先の従業員が、個人データが保存された USB メモリをかばんに入れて管理区域外に持ち出し、持参した状態で飲酒を伴う飲食を行い、その結果 USB メモリを紛失したものである [7]。

本件の個人情報保護委員会の公表資料では以下の点が指摘されている。

- BIPROGY では、個人情報の取扱いに係る規律自体は存在していたものの、同規律に従った運用を確保するための組織的安全管理措置が適切に講じられていなかった。
- そもそも BIPROGY では、個人情報の取扱い上のリスクに応じて必要かつ適切な措置を検討するための組織体制がなく、個人情報に関連する事務を現場担当者のみで判断することが実態となっており、適切な安全管理措置を講ずるための組織体制が整備されていなかった。
- 個人情報を取り扱う区域に対する入退室管理、個人情報を保存する電子媒体に対して盗難等を防止するため施錠できるキャビネット等に保管する等の措置、個人情報への不要なアクセスを防ぐためのアクセス制御等の措置といった物理的・技術的安全管理措置が適切に講じられていなかった。
- 実務を担う再委託先等の従業者に対して、具体的な手順や講ずべき安全管理措置に関して何ら指示することなく、再委託先等の従業者らに一任し、再委託先における個人情報の取扱状況を把握していない等、再委託先等の監督を適切に行っていなかった。
- 特に、尼崎市からの委託業務には、住民基本台帳上の情報が含まれる多量の個人や、障害有無等の要配慮個人情報など、多量かつ機微性の高い個人情報を恒常的に取り扱う性質があり、BIPROGY においては、個人情報の取扱いに関して個人情報保護法を厳に遵守し、とりわけ、高い水準の安全管理措置等を講じることが求められていた。

**(3) キャッシュレス決済機能を提供する事業者の皆様への注意喚起 [8](公表日:2019 年 8 月 6 日)**

具体的な事案ではないが、個人情報保護委員会は、キャッシュレス決済機能を提供する事業者向けの注意喚起を行っている。その内容は、既存サービスのアカウントに対するリスト型アカウント攻撃をはじめとする不正アクセスにより、決済機能が悪用さ

5 https://www.metaps-payment.com/company/20220228.html

6 https://www.ppc.go.jp/news/press/2021/220921kouhou/

7 事実関係は、BIPROGY の調査委員会による報告書に詳しい(https://www.city.amagasaki.hyogo.jp/_res/projects/default_project/_page_/001/030/947/1128houkokusyo.pdf)。

8 https://www.ppc.go.jp/news/press/2019/20190806/

れ、利用者に被害が発生する事例が報告されており、決済機能を提供するアプリケーション等を導入済、又は導入の検討を行っている事業者に対して、不正アクセスに備えた十分な対策を講じることを求めるものである。

本注意喚起も、キャッシュレス決済のために必要な機微性の高い個人情報を大量に取り扱うキャッシュレス決済事業者向けに、必要な対策を実施するよう特に注意喚起したものとみることができる。

### 5. 総括

以上、個人情報に関する安全管理措置についてのガイドラインにおける記載と、個人情報保護委員会が公表している具体的な事案等について概観した。

ガイドラインにおいては、講じるべき安全管理措置の内容が例示に基づき説明されており、実務上講じる安全管理措置を検討するうえでは参考になる。もっとも、ガイドラインにおいても、個人情報を取り扱うことによって生じるリスクに応じた安全管理措置を講じるべきことが強調されており、具体的にいかなる安全管理措置を講じるべきかは、各事業者の個別の事情によることになる。

公表案件では、いずれも大量の個人情報を取り扱っているなど、高い水準の安全管理措置を講じるべき事業者であったことが指摘されており、やはり安全管理措置を講じる上では、適切なリスク分析を行うことが第一歩であると言える。また、いずれの公表案件も、規程や内部監査体制などが形式的には定められていたものの、実態としては形骸化していたことが指摘されており、基本的なことではあるが、安全管理措置は一度講じるだけではなく、継続的に実施した上で、運用等を見直し維持していくことが重要である。

## Ⅱ 個人情報保護・データ保護規制 各国法アップデート

### 1. 中国

- 2022 年 11 月 8 日、「ネットワーク安全標準実践ガイドライン-個人情報越境取扱活動安全認証規範 V2.0」の意見募集稿について意見を募集する通知が公布され、2022 年 11 月 15 日まで意見募集が行われた。本意見募集稿は、同規範の V1.0(当事務所個人情報保護・データ保護規制ニューズレター2022 年 9 月 1 日号「電気通信事業法改正のポイント」参照。)を基としているが、本意見募集稿では、個人情報処理者が国外の受領者と法的合意を締結する場合、双方に個人情報の越境移転の目的、センシティブレベル、量、方法、保存期間、保管場所などをさらに明確化することを求めており、また、合意(書)には、個人情報の主体の権利、個人情報の主体の権利を保護する方法及び手段を列挙することを求めている。
  また、本意見募集稿では、①認証を受ける者は必ず法人資格を有すること、②基本原則を適用する主体は国外の受領者に拡張すること、③越境移転の合意の内容を追加し、個人情報処理者と国外受領者の責任及び義務を明確にすること、④個人情報に関する権利利益が侵害された場合、個人情報処理者、国外の受領者のいずれにも賠償請求を行う権利を有することとする変更がなされた。V1.0 と比較して、個人情報を受領する中国国外の者に対する義務及び責任が強化されている。
- 2022 年 11 月 18 日、「個人情報保護認証の実施規則」が公布された。本規則は、個人情報処理活動を規制し、個人情報の合理的な使用を促進し、個人情報処理者が認証を通じて個人情報保護能力を高めるために、「中華人民共和国認証認定条例」に基づき、個人情報処理者の個人情報の収集、保存、使用、処理、伝送、提供、開示、削除及び越境移転などの処理活動に対する認証の基本原則及び要件を定めている。

### 2. 香港

2022 年 11 月 14 日、PCPD(香港の個人情報保護委員会)は、EC ヘルスケアという企業が、統合システムを通じて様々なブランド間で顧客の個人データを共有していたことの調査報告書(「EC ヘルスケアに関する報告書」)及び、Fotomax Limited のデータベースがランサムウェアの攻撃を受けたことに関する報告書(「ランサムウェア攻撃に関する報告書」)を公表した。双方の報告書では、調査結果を踏まえて、同様の個人データを取り扱う事業者に対する推奨措置を公表している。

- EC ヘルスケアに関する報告書では、複数のブランドを運営する組織に対して以下の 6 つの事項を推奨している。
  - データ収集の目的とデータの移転を受ける可能性のある受領者の分類について顧客の理解を促進するために、明瞭かつ簡潔な個人情報収集文書を提供すること

- 新たな目的のために顧客の個人データの使用(開示及び移転を含む)を行う前に、顧客から同意を取得すること
- 業務の範囲及びスタッフの権限を考慮して、顧客の個人データに対するスタッフのアクセス権及び検索権を適切に割り当てること
- 相当量の個人データの取扱いを伴う計画を実施する前に、プライバシー影響評価を実施し、個人データプライバシーの保護のために、当該評価によって特定された影響及びリスクに対応するための適切な措置を採用すること
- ガバナンス責任の一部として個人データプライバシーの保護を含む、個人データプライバシー管理プログラムを実施すること
- 個人データプライバシーを尊重する組織文化を発展させることを目的として、組織が、PDPO(Personal Data (Privacy) Ordinance)に基づく要求を遵守し、プライバシー管理プログラムを実施することを確保するために、データ保護責任者を任命すること

- ランサムウェア攻撃に関する報告書では、顧客の個人データを取り扱う事業者について、以下の事項について特に注意を払うよう要求している。
  - システムがハッキングされた際の潜在的な影響を評価するために定期的なリスク評価を実施することによって、ハッカーの攻撃を防止するための警戒を怠らないようにすること
  - PDPO を遵守して個人データを取り扱い、個人データの全ライフサイクルにおいて個人データを効率的に取り扱うための個人データプライバシーマネジメントプログラムを確立すること
  - PDPO の遵守を監視するために特定の役員をデータ保護責任者に任命すること
  - できるだけ早期にセキュリティの脆弱性を修正するために効果的なパッチ管理手続を構築することを含む、情報システム管理を高めること
  - 将来の評価における参照のために社内のコミュニケーションを適切に文書化し、維持すること

## 3. 台湾

台湾政府のデジタル発展部は、台湾個人情報保護法 27 条 3 項に基づき、2022 年 11 月 15 日に「デジタル経済関連産業非公務機関による個人情報ファイル安全保護計画実施弁法」の草案を公表した。当該草案によれば、①無店舗小売業、②ソフトウェア出版業、③コンピュータシステムのデザインサービス業、④ポータルサイトの運営、データ処理、ウェブホスティング及び関連サービス業、並びに⑤その他情報提供サービス業者は、本弁法に従い個人情報ファイルに係る安全保護計画、及び業務終了後の個人情報の取扱方法を制定しなければならない。また、これらの業者は個人情報ファイル安全保護措置を取るため、下記各項目に対応する体制を整えなければならない。

- 管理担当者等の配置
- 個人情報処理、利用状況の定期点検
- 個人情報に係るリスク分析及び管理
- 個人情報の窃取、改ざん、毀損、滅失又は漏えい事故の予防、通報及び対応
- 個人情報の収集、処理及び利用に係る内部管理手続
- 越境移転の制限の確認、当事者への告知、及び監督
- 個人情報ファイル安全保護に関する安全管理及び人員管理
- 周知・啓発活動及び教育訓練
- 個人情報を保存する設備の安全管理
- 個人情報の安全性に関する監査
- 使用記録及び処理証拠等の保存
- 個人情報の安全保護に係る全般的な継続的改善

## 4. オーストラリア

2022 年 11 月 28 日、情報漏えい事故への罰則の強化を含む個人情報保護に係る改正法案(Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022 (Privacy Bill))が連邦議会で可決され、2022 年 12 月 12 日に公布、施行された。本改正により、重大な又は繰り返されるプライバシー侵害に対する罰則の強化(自然人:444,000 豪ドルから最高 250 万豪ドル、

法人：222 万豪ドルから、最高で(i)5,000 万豪ドル、(ii)当該行為から当該法人グループが直接又は間接に得た利益の 3 倍、(iii)裁判所が(ii)を算定できない場合は 12 か月間(侵害継続期間の方が長い場合は当該期間)に係る当該法人グループの調整売上高の 30%、のいずれか高い額)等がなされた。その他の法案の概要については、当事務所個人情報保護データ保護規制ニューズレター2022 年 11 月 22 日号もご参照。

## 5. タイ

タイでは、2022 年 12 月 15 日、個人情報保護法の下位規則である"Notification of the PDPC re: Criteria and Method for Reporting the Personal Data Breach B.E. 2565 (2022)"が公表され、同日に施行された。当該 Notification では、データブリーチの定義や、当局への通知の対象となるデータブリーチの特徴、当局及びデータ主体へ通知すべき事項等が定められている。

## 6. フィリピン

フィリピンでは、2022 年 11 月 14 日より、フィリピン国家プライバシー委員会(NPC)への処理者登録義務に関する通達の改正案が公表されパブリックコメントが募集されている。現行の通達では、個人データの処理者のうち、少なくとも 1,000 人のセンシティブ個人データを処理している、250 名以上の従業員を雇用している等の一定の要件を満たす個人又は団体のみが NPC への登録を義務付けられている。しかし、改正案は、個人データ又はセンシティブ個人データを取り扱うすべての管理者及び処理者について、NPC への登録義務を課す内容となっている。

## 7. インド

インドでは、2019 年 12 月 11 日に個人情報保護法案(the Personal Data Protection Bill)が国会に提出されたが、2022 年 8 月 3 日に当該法案は撤回された。政府は、当該法案の代わりとして、2022 年 11 月 18 日、2022 年デジタル個人情報保護法案(The Digital Personal Data Protection Bill, 2022)の草案を公表し、2023 年 1 月 2 日までパブリックコメントが募集されている。当該草案では、データの国外移転について、政府が指定した一定の地域や国について別途定められる一定の条件の下データ移転を認める等、一律に厳しい条件を定めていた元の個人情報保護法案よりも緩やかな規制が定められている。その他、同意を含むデータ処理の法的根拠、データブリーチの場合に必要とされる対応、データ主体の権利(アクセス権、訂正権、削除権等)等が規定されている。

## 8. アルゼンチン

2022 年 11 月 29 日、アルゼンチンの公共情報アクセス庁(the Agency for Access to Public Information: DPA)は、アルゼンチン国民の個人データを処理する外国の個人及び法人を、アルゼンチン個人情報保護法上の「データベース責任者」として登録することができるオンライン登録フォームを導入した。これにより、アルゼンチン国民の個人データを処理する外国人データベース責任者は、アルゼンチンに拠点を置いていない場合でも、国が管理するデータベース登録簿に登録することが必要になった。

## 9. ペルー

2022 年 10 月 24 日、ペルーの個人データ保護当局(ANPD)は、「個人データの国際移転に関するガイド」を承認した。同ガイドにより、イベロアメリカデータ保護ネットワーク(RIPD)が作成した個人データの国際移転のためのモデル契約条項(MCC)を使用することで、個人データ保護法において、個人データを国際移転する際に求められる「受領国において十分な個人データの保護水準が保証されている場合」という条件を満たすことが認められた。

## 10. 欧州

### (1) ICO による個人データの越境移転に関するガイダンス更新版の公表

2022 年 11 月 17 日、英国個人情報保護監督機関(ICO)は、移転リスク評価(TRA)及びそのツールに関する章を含む、個人データの越境移転に関するガイダンスの更新版を公表した。本ガイダンスでは、TRA に関する、ICO と欧州データ保護評議会(EDPB)によるアプローチの違いや、ICO は英国からの越境データ移転について、ICO 及び EDPB のいずれのアプローチに依拠しても差し支えないことが明確化されている。なお、TRA ツール案並びに IDTA 案及び SCC アデンダム案の概要については、当事務所ヨーロッパニューズレター2021 年 11 月 26 日号「英国個人情報保護監督機関(ICO)による国際データ移転契約案等の公表」を参照されたい。

### (2) EU・米国間の十分性認定ドラフトの公表

2022 年 12 月 13 日、欧州委員会は、Privacy Shield に代わる新たな十分性認定の枠組みとなる EU-U.S. Data Privacy Framework (DPF)に基づく十分性認定決定のドラフトを公表した。当該ドラフトは、同年 10 月 7 日に発効した大統領令 14086 (EO14086)及びその関連規則を受けたものであり、今後は、欧州データ保護評議会(EDPB)等の欧州連合の関係機関による意見の公表を待つことになる。米国の十分性認定が正式に決定されれば、DPF に参加する企業に対しては、他に特段の保護措置等を実施せずに EEA 域内から個人データを自由に移転できるようになる。

### (3) Meta に関する GDPR65 条に基づく EDPB 決定

欧州データ保護評議会(EDPB)は、2022 年 12 月 6 日、大手ソーシャルメディアサービスである Meta に関する GDPR65 条に基づく決定を採択した。複数の監督当局が、アイルランドの監督当局が作成した決定草案に対して、処理の適法性根拠(GDPR6 条)、データ保護の基本原則(GDPR5 条)、罰金を含む是正措置に係る判断に関して異議を申立て、かかる異議申立てについて合意が成立しなかったため、GDPR65 条 1 項(a)に基づき、EDPB への付託が行われた。当該決定においては、行動ターゲティング広告及びサービス向上を目的とする個人データ処理に際しての同意取得方法の適法性が争いになったとされており、サービス利用規約の中に個人データの利用に関する同意条項があったとしても、かかる同意条項によって GDPR 上有効な同意を取得することはできないとの判断が示されたと報じられている。現時点では当該決定は公表されていないが、アイルランドの監督当局が管理者に対して決定を通知した後、EDPB がウェブサイト上に当該決定の内容を公表することとなる。

### (4) 日英間のデジタルパートナーシップ

総務省、経産省、デジタル庁とイギリスのデジタル・文化・メディア・スポーツ省は、2022 年 12 月 7 日、以下の取り組みを含むデジタルパートナーシップを構築していく方針を決定した。同パートナーシップは、2019 年の日英共同声明、2020 年の日英包括的経済連携協定(CEPA)、及び 2022 年 5 月 4 日の共同公約で示されたパートナーシップに基づいている。

①デジタルインフラと技術：電気通信市場に関する協働、サイバー攻撃への対応能力の向上、半導体の安定的な供給の保証、インターオペラビリティの確保、及び信頼性のある AI 開発の促進
②データ：信頼性のある自由なデータ流通(Data Free Flow with Trust、DFFT)の実践、データ保護の規制における協力、データイノベーションに関する協働
③デジタル規制と基準：子どもを含むユーザーのオンライン上の安全性確保、デジタル市場における連携、デジタル技術基準に関する連携、インターネットガバナンスに係る問題への対応についての協力
④デジタルトランスフォメーション：2022 年 10 月 31 日に日英間で締結された協力覚書に基づくデジタルガバメントトランスフォーメーション、デジタル技術の社会への浸透、デジタルアイデンティティに関する問題解決

### (5) ガバメントアクセスに関する OECD 加盟国による共同宣言

OECD 加盟国は、2022 年 12 月 14 日、国家安全保障や法執行の目的で個人データへのガバメントアクセス(GA)が行われる際に、プライバシーやその他の人権及び自由を保護するための共通のアプローチに関する個人データに対する GA についての宣言を採択した。本宣言は、OECD のプライバシーガイドラインを補完するものであり、自由と人権を重視する民主主義国家の集まりである OECD 加盟国において行われる GA は以下の 7 つの原則を守るべきことを明示している。

| | |
|---|---|
| 法的根拠 | 法の支配の下で運営される民主的に設立された機関により採択及び実施される法的な枠組みにより、GA が規制されること。 |
| 正当な目的 | 政府は、法の支配の下で定められた、特定された合法的な目的での GA のみを行い、批判や反対意見を弾圧するための GA は行わないこと。 |
| 承認 | GA にあたって適切な事前承認を得なければならない仕組みを確立すること。 |
| データの取扱い | GA により取得された個人データは、権限ある政府職員のみが処理できるようにすること。 |
| 透明性 | 個人がプライバシーその他の人権及び自由に対する GA の影響について理解できるようにするため、GA の法的な枠組みは、明確で容易にアクセス可能なものとすること。 |
| 監督 | コンプライアンス部門、裁判所、議会、立法委員会又は独立した行政機関を通じた適切な監督が行われ、監督により GA の法的な枠組みの遵守が保証されること。 |
| 救済 | 個人に対し、司法上及び非司法上の救済のための措置を提供すること。救済のための措置には、アクセスの停止やデータの削除等が含まれ、場合により、個人が被った損害の賠償も含まれ得る。 |

### (6) BCR-C に関するレコメンデーション案

欧州データ保護評議会(EDPB)は、2022 年 11 月の総会において、管理者用の Binding Corporate Rules(BCR-C)の承認申請とその要素及び原則に関するレコメンデーション案を採択した。同レコメンデーション案では、BCR-C の承認申請のフォームが示されており、承認申請のフォームに記載しなければならない内容と、BCR-C を保持する上で遵守する必要のある GDPR47 条に定める要件について解説がなされている。また、同レコメンデーションの発効前に承認された BCR-C についても、同レコメンデーションの要求を満たすことが求められる(パラグラフ 13)。同レコメンデーション案については、2022 年 11 月 17 日から 2023 年 1 月 10 日までの期間、パブリックコメントが募集される。

## 11. サウジアラビア

2021 年 9 月 24 日に個人データ保護法(Personal Data Protection Law)が公布され、施行時期が延期されていたことは、当事務所個人情報保護・データ保護規制ニューズレター2021 年 11 月 26 日号及び当事務所個人情報保護・データ保護規制ニューズレター2022 年 5 月 11 日号で紹介した。個人データ保護法には、例えば GDPR との対比上の課題点とみられる事項が含まれており、それらの一部に対処した内容の同法の改正案が 2022 年 11 月 20 日から 12 月 20 日まで意見公募手続に付された。改正法の内容は確定を待つ必要があるが、主な改正点は以下のとおりである。

- 越境移転:十分性の概念が導入され、十分性が認定される法域へデータの越境移転を認める。
- データ処理の根拠:要配慮ではない個人データにつき、正当な利益がある場合には当該個人データの処理を可能とする。
- データ侵害時の本人通知:データ主体(本人)に損害を与える可能性がある場合又はデータ主体の権利と利益を害する場合に、本人への通知を必要とする。

- データポータビリティの権利[9]：技術的に可能であればという限定付で導入されている。
- 位置データ：要配慮個人データから除外され、位置データも上記の正当な利益を根拠として取扱い可能となる。

## 12. 米国

2022 年 11 月 3 日、ペンシルバニア州のデータ侵害通知法を改正する法律が成立した。改正点の一つは個人情報の範囲の拡大であり、新たに、①医療情報(医療従事者が作成した処置、診断等の記録に含まれる個人を特定し得る情報)、②健康保険情報(保険証券番号等とアクセスコードその他保険金不正使用に使われ得る情報の組合せ)、③ユーザ名又はメールアドレスとパスワード又は秘密の質問の組合せについて、これらが州の住民の名前とともに侵害された場合、侵害通知の対象となる。また、改正法では、通知の方法や通知のタイムライン等も改正されている。改正法は 2023 年 5 月 2 日に施行される。



西村あさひ法律事務所　広報室　E-mail

[9] データ主体が個人データを受け取り、またある管理者から別の管理者に移行する権利