牛島総合法律事務所
危機管理/不祥事対応/個人情報/プライバシーニューズレター

個人情報保護委員会による行政指導の近時の傾向（2023 年 9 月～2024 年 1 月）

2024 年 1 月 30 日

弁護士　中井　杏

個人情報の取扱いに関するリスクコントロールを検討するためには、監督官庁である個人情報保護委員会の動向を把握しておくことも重要です。本ニューズレターでは、個人情報保護委員会による近時の行政指導の分析と、留意するべき点について述べます。
2022 年から 2023 年 8 月までに公表された行政指導の分析や行政指導の傾向については個人情報保護委員会による行政指導の近時の傾向（2023.08.30）をご参照ください。

1. 近時の行政指導の概況

2023 年 9 月から 2024 年 1 月までの間に、新たに公表された個人情報保護委員会による行政指導事案は 5 件（※）であり、2023 年度はこれまでに計 9 件の行政指導事案が公表されています。2021 年度が 1 件、2022 年度が 6 件だったことを踏まえると、行政機関等が個人情報保護委員会の監督対象になったことを踏まえても、重要な行政指導を公表することに積極的な姿勢であることが見受けられます。
また、2023 度上半期の個人情報取扱事業者に対する報告徴収は 60 件（2022 年度上半期は 62 件）、指導・助言は 165 件（2022 年度上半期は 30 件）でした（令和５年度上半期における個人情報保護委員会の活動実績について（概要））。指導・助言は、2021 年度が 217 件、2022 年度が 115 件と一時的に減少していましたが、2023 年度は 2021 年度を上回ることが予想され、増加傾向にあるといえます。

※マイナンバーに関する行政指導及び行政機関等に対する行政指導を含みます。

2. 行政指導が公表された事案

以下では、実務対応を検討するうえで、把握しておくべき行政指導について解説します。

(1)自治体による個人情報の漏えい事案（2023 年 11 月 29 日）

青森県上北郡野辺地町において使用していた USB メモリが紛失し、当該 USB に記録されていた町民に関する保有個人情報の漏えいのおそれが発生した事案です。

本件は地方公共団体に対する行政指導ですが、企業においても注目すべきは、漏えい等報告の速報が、事案の発覚から 28 日後に提出されていることが、組織的安全管理措置の不備の理由として考慮されている点です。
漏えい等報告は、報告対象事態を知ったときから、概ね 3～5 日以内（初日参入）に速報を提出しなければならず（個人情報保護法規則 8 条 1 項、通則ガイドライン 3-5-3-3）、これは地方公共団体の場合も同様です（個人情報の保護に関する法律についての事務対応ガイド（行政機関等向け）93 頁）。
企業においては、従前どおり、報告対象事態をいずれかの部署が知ってから、5 日以内に提出するようにしつつ、遅くとも 28 日を超えた場合には行政指導において考慮された例があることを留意する必要があります。

(2)オプトアウト届出事業者への行政指導（2024 年 1 月 17 日）

個人情報保護法 27 条 2 項は、一定の事項を届け出た場合、本人の同意なく個人データの第三者提供ができることを定めており、かかる届出を行った事業者は、オプトアウト届出事業者と呼ばれています。
2023 年 2 月から 3 月に実施したオプトアウト届出事業者に対する実態調査の結果、調査に未回答又は回答内容が不十分だったオプトアウト届出事業者に対し、報告等の求めがなされていました。これを受けて、個人情報保護法上の問題点があったオプトアウト届出事業者に対し行われた行政指導です。
企業において注目すべき点は、不適正利用（個人情報保護法 19 条）に当たる個人情報の利用が問題点として指摘されている点で、（当該オプトアウト届出事業者）が、「販売先が、法に違反するような行為を行う者にも名簿を転売する転売屋（ブローカー）だと認識していたにもかかわらず、意図的に販売先での名簿の用途を詳しく確認せず、転売屋に名簿を販売した」ことが、不当な行為を助長又は誘発するおそれがある方法による個人情報の利用であると指摘された点です。
不適正利用禁止規定（同法 19 条）は、2020 年の改正により新設された規定ですが、その文言自体は、広く適用され得る規定となっています。同規定が新設されるきっかけとなった破産者マップ事案について、同条違反が指摘されたことはありましたが、本件は、破産者マップ事案以外の具体的な事案において 19 条違反が問題点として指摘された事例となります。
企業においては、今後も具体的な適用事例に注目し、自社の個人情報の取扱いが不適正利用に当たらないよう注意していく必要があります。

(3)コールセンターシステムの保守運用の委託先従業員による顧客又は住民等情報の不正持出事案（2024 年 1 月 24 日）

本件は、複数の民間事業者及び地方公共団体等からコールセンター業務に関し個人データの取扱いの委託を受けていた A 社が、コールセンター業務用システムの保守運用のため個人データの取扱いを B 社に再委託していたところ、B 社に派遣されていた派遣社員が個人データを不正に持ち出し、名簿業者に売却した事案です。
発覚の経緯は、委託元の 1 社（X 社）が、顧客から不審な投資勧誘電話があったとの連絡をうけ、X 社において社内調査及び警察への捜査依頼が行われました。しかし、X 社からの漏えいの事実が確認できなかったため、X 社が A 社に調査を依頼し、A 社及び B 社において調査が行われた結果、いったんは A 社から漏えいは確認されなかった旨の報告がなされました。その後、警察が B 社に対して捜査が行ったことを発端として、A 社が個人データの漏えいがあったことを認めたというものです。
持ち出された個人データは、民間事業者 30 社、独立行政法人 1 機関及び地方公共団体 38 団体から委託された約 928 万人分のものであり、氏名、住所、電話番号、生年月日、メールアドレス、サービス種別・回線 ID 等が含まれていました。また、持出行為が行われたのは 2013 年 7 月頃から 2023 年 2 月頃までと約 10 年にわたっています。個人データを持ち出した方法は、①サーバにアクセスしサーバ内の個人データをダウンロードした方法、②保守業務用端末から私物 USB メモリに書き出す方法、③システム管理者権限を悪用し保守拠点以外からリモートアクセスにより個人データにアクセス、ダウンロードし、私物 USB メモリに書き出した方法があり得るとされています。

事案の重大性については、大量の個人データ等が長期にわたり漏えいしたこと、個人データ等が名簿業者に売却された可能性が高いこと、個人データ等の性質として企業の商品購入履歴や地方公共団体の住民であるこ

と等から推測することで、年齢、性別、利用企業及び行動範囲等で分類し、嗜好性又は経済状況といった情報を分析され、悪用されることが懸念されることが考慮されています。
報道によれば、本件で持ち出された個人データは名簿業者に売却され、さらに名簿業者が別の会社に売却し、営業のために用いられたことが明らかになっています。
例えば、名簿業者から名簿を購入した者が、名簿を特殊詐欺のために用いたり、不当に商品を販売するために用いたりした場合は、明らかに嗜好性又は経済状況といった情報を分析され、悪用されるような場合といえると思われます。しかし、名簿業者から名簿を購入した事業者における個人データの利用方法にかかわらず、(2)のとおりオプトアウト事業者に対し行政指導が行われていることを鑑みれば、個人情報保護委員会は名簿業者への売却そのものに対して問題意識を有しているものと思われます。
法律上の問題点としては、A 社及び B 社に安全管理措置（法 23 条）の不備があったこと、A 社に対し再委託先の監督（法 25 条）に不備があったことが指摘されています。
合わせて、コールセンター業務を運営又は受託している個人情報取扱事業者に対し、安全管理措置に関する注意喚起が出されています。

本件事案には、個人データの取扱いにおいて一般的に注意すべき点への示唆が含まれています。
第一に、安全管理措置の不備の指摘においては、結果として不正持出が発生したことが、各安全管理措置の不備を裏付ける事情として考慮されています。
例えば、B 社の人的安全管理措置（従業者の教育）について、「本件事案における X（※派遣社員のこと）の不適切な取扱いを質せず、漏えいを防止するに至らなかったことからすると、その取組は、B 社の従業者が適切な情報セキュリティの確保や個人データ等の適正な取扱いの重要性に関する認識を醸成するには不十分な内容であったと言わざるを得ない」などと指摘されています。

第二に、システム管理者アカウントは、個別に割り振ることで識別と認証を可能にし、また相互監視を行えるようにすることが重要です。
本件では、B 社の保守運用担当者がシステム管理者アカウントを用いて作業を行うためには、通常 B 社内の保守拠点に設置された保守端末で作業を行う必要がありましたが、システム管理者アカウントの権限を用いることで、保守拠点以外からも個人データにアクセスできるようシステム設定を行うことができたため、当該権限を悪用し保守拠点以外から個人データにアクセスし、個人データの不正な持ち出しを行った可能性があります。
この点、B 社では、システム管理者アカウントが個人単位で付与されておらず、4 人で共用する状態でした。また、これによりアクセス者の識別と認証が適切に行われていなかったとされています。
システム管理者の権限管理については、独立行政法人情報処理推進機構「組織における内部不正防止ガイドライン第 5 版」（2022 年 4 月）（内部不正防止ガイドライン）42 頁においてシステム管理者が複数人いる場合は、システム管理者 ID ごとに適切な権限範囲を割り当てシステム管理者が相互に監視できるようにしなければならないと指摘されています。
また、アクセス者の識別と認証は通則ガイドライン 10-6 において安全管理措置として義務付けられているのみならず、内部不正防止ガイドライン 44 頁においても共有 ID 及び共有のパスワード・IC カード等を使用せず、システム管理者 ID を個別のパスワード・IC カード等で認証しなければならないと指摘されています。また、個別のアカウントを付与していなければ、不正があった場合に、誰が不正をしたかの事実調査が困難となり、原因の究明や被害の拡大防止に支障をきたします。
システム管理者は大きな権限を持つため、相互に監視でき、権限分散をしておかなければ、管理者が 1 人で内部不正を実行する機会を与えてしまうことになるため、システム管理者の設計に留意する必要があります。

第三に、委託元や関係者から不正調査の依頼があった場合は、真摯に対応し、また不正調査に対応できる体制を構築しておくことが重要です。
本件では、委託元において個人情報の漏えいの疑いが生じたため、2022 年 4 月に A 社に対し調査が依頼されています。A 社と B 社はともに調査を行ったものの、個人データの漏えいは確認されなかったことを報告し

ています。しかし、その後、警察がB社に対し捜査を実施したところ、2023年8月にA社が個人データの漏えいがあった事実を委託元に報告しています。
報道によれば、2022年の時点で、委託元は警察に不正競争防止法違反により相談を行っていたとのことです。
自社の従業員が他社から示された営業秘密を持ち出した場合、不正競争防止法違反の両罰規定（同法22条）により罰される可能性があります。また、自社の個人情報を従業員が持ち出した場合も、個人情報保護法違反の両罰規定（同法184条）により罰される可能性があります。
委託元や関係者から、不正調査の依頼があった場合、すでに警察への相談が行われており、場合によっては自社が処罰される可能性があることを念頭に置き、調査依頼には適切に対応する必要があります。また、事実関係を検証することができるような体制を整備しておくことが重要です。

これらの行政指導も含めた2024年の個人情報保護法の対応ポイントに関する無料セミナーを、以下のとおり2024年2月16日（金）に実施します。お気軽にお申し込みください。

U&Pリーガルセミナー「20分でわかる2024年の個人情報保護法の対応ポイント～行政指導の傾向、2025年改正に向けてなど～」（中井杏）（2024/2/16 15:00～（後日の配信も予定））

関連記事

・ニューズレター「顧客情報の持ち出しに関する個人情報保護法上の刑事責任と実務対応」
・ニューズレター「個人情報保護委員会による行政指導の近時の傾向」

関連セミナー

・U&Pリーガルセミナー「法務が把握すべき個人情報保護委員会による行政指導の近時の傾向」（中井杏）（無料：2024/3/31まで配信中（2023/9/8収録））

以 上