

個人情報保護委員会 監視監督権限の行使状況の概要等を公表

2024年9月4日

弁護士 中井 杏

個人情報保護委員会は、2024年8月28日、2024年度第1四半期における[監視・監督権限の行使状況の概要と漏えい等報告の処理状況](#)について公表しました。各文書は、今後四半期ごとに取りまとめられ、公表されるということです。

本ニューズレターでは、各文書から読み取れる個人情報保護委員会の行政指導の傾向と、企業における今後の対応について解説します。

<目次>

1. 監視・監督権限の行使状況と漏えい等報告の処理状況の概要
2. 安全管理措置義務の不備として指導されている事項の傾向
3. 指導・助言等の事案の公表について
4. 企業における今後の対応

1. 監視・監督権限の行使状況と漏えい等報告の処理状況の概要

漏えい等報告の処理状況によれば、2024年度第1四半期の個人情報取扱事業者による漏えい等報告は4120件であり、2023年度より増加しています。

監視・監督権限の行使状況の概要によれば、2024年度第1四半期の民間事業者に対する指導・助言は110件で、そのうち62件は安全管理措置（個情法23条）や委託先の監督義務（個情法25条）に関するもの、47件が漏えい等報告の提出の遅延に関するものとなっています。

また、注目すべき点は、110件の指導・助言のうち、安全管理措置か委託先の監督に関するものでないものは、開示請求の対応に関するものが1件あるのみであることです。安全管理措置や委託先の監督に関する指導は、漏えい等報告により個人情報保護委員会が指導すべき事案を把握する端緒があるため件数が増えると考えられるものの、漏えい等に関するもの以外の個人情報保護法違反による行政指導がなされることは非常に少ないことが読み取れます。

2. 安全管理措置義務の不備として指導されている事項の傾向

個人情報保護委員会は、安全管理措置に不備があったケースとして①VPN（Virtual Private Network）機器の脆弱性やECサイトを構築するためのアプリケーション等の脆弱性が公開され対応方法がリリースされていたにもかかわらず、事業者が放置していたこと、②ID・パスワードが容易に推測されやすいものとされていたこと、③設定ミスによりデータベースへのアクセス制御が不適切な状態になっていたことや、ファイアウォールが解除されていたこと、④サポート詐欺によるもの、を特に取り上げて言及しています。

この他にも、事業者の規程に反し、私物である外部電磁的記録媒体の利用や持ち帰り等が行われ、個人データが入った HDD を紛失した事案が組織的安全管理措置及び物理的安全管理措置に関し指導されているものなどがあります。

この点、[ガイドライン通則編 10-6](#)の技術的安全管理措置の外部からの不正アクセス等の防止として①「機器やソフトウェア等に標準装備されている自動更新機能等の活用により、ソフトウェア等を最新状態とすること」が明示的に例示されています。

また、IPA（独立行政法人情報処理推進機構）「[中小企業の情報セキュリティ対策ガイドライン第 3.1 版](#)」では、必ず実行すべき重要な対策として、①「OS やソフトウェアは常に最新の状態にしよう」、②「パスワードを強化しよう」、③「共有設定を見直そう」などが指摘されており、これらは基本的な対策として位置付けられています。

さらに、IPA「[情報セキュリティ 10 大脅威 2024](#)」でも、①脆弱性対策を適切に行うこととして、サポート切れの OS やソフトウェア、ハードウェアを使用しないことや、迅速に更新プログラムの適用をすること、②パスワードを適切に運用することが共通対策として指摘されています。また、③設定ミスによる情報漏えいも、情報セキュリティ 10 大脅威の一つとして指摘されています。

このような状況を踏まえると、個人情報保護委員会からみて、容易に対策が可能であるにもかかわらず、対策していなかったと認定されるような原因による漏えい等が発生した場合には、指導・助言の対象となる可能性が高まると思われます。したがって、企業においては、公表されている資料を参考に、重要な対策として指摘されている事項については、対応しておくことが重要だと考えられます。

また、指導・助言の 4 割近くが漏えい等報告の提出の遅延であることも特徴的です。個人情報保護委員会に対する個人データの漏えい等の報告は、個人情報保護法規則 7 条に定められた漏えい等又は漏えい等のおそれを知った時点から概ね 3～5 日以内（初日算入）に行わなければならないとされており（[ガイドライン通則編 3-5-3-3](#)）。しかし、実務上は、個人情報の漏えい等の事態を最初に知った部署から漏えい等報告を行う部署に報告がなされるまでに一定の時間を要してしまいがちであることに加え、当該事態が個人情報保護委員会に報告しなければならない事態なのかの判断や、報告書面に関する社内調整にも時間を要することを踏まえると、概ね 3～5 日以内に速報を行うことは容易ではありません。そこで、情報漏えい等が発生した場合の対応マニュアルを作成し、従業員に周知しておくことが非常に重要になります。

なお、安全管理措置は、「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」とされています（[ガイドライン通則編 3-4-2](#)）。今回公開された事案の概要では、これらの事項が網羅的に公表されているものではないため、具体的にどのような考慮がなされているかまでは明らかではありません。もっとも、従業員情報の漏えい等事案は、事業者名を明らかにした事案の公表はされない傾向にあるとみられていましたが、指導・助言はなされております。

3. 指導・助言等の事案の公表について

今回、漏えい等報告の提出の遅延に関する事案を除き全ての事案の概要と指導事項が公表されたとみられません。もっとも、具体的な事案は特定されないような形で事案の概要は記載されているため、個人情報の漏えい等によるレピュテーションリスクが今まで以上に高まったものではないと思われます。

4. 企業における今後の対応

今回の監視・監督権限の行使状況の概要の公表により、個人情報保護委員会からみて、容易に対策が可能であるにもかかわらず、対策していなかったと認定されるような原因による漏えい等には行政指導がされる傾向があることがわかりました。したがって、各機関が公表する資料を参考に、重要な対策と位置づけられている事項については、対応を行っていくことが重要となります。

他方で、事案の概要と指導事項は公表されても、具体的な事案が特定できるような情報が公開されているものではないため、個人情報の漏えい等によるレピュテーションリスクが今まで以上に高まったものではないと思われます。

もっとも、個人情報の漏えい等は、個人情報保護委員会による行政指導よりも、報道や本人通知によるレピュテーションリスクの方が重大であるため、企業においては引き続き事業や個人データの性質を考慮した対策を行っていくことが重要となります。

関連記事

- ・ 特集記事「[個人情報の漏えい等報告についての FAQ](#)」
- ・ ニュースレター「[個人情報保護委員会による行政指導の近時の傾向](#)」(2023.08.30)
- ・ ニュースレター「[個人情報保護委員会による行政指導の近時の傾向 \(2023年9月～2024年1月\)](#)」(2024.01.30)

以上

ニュースレターの配信登録は[こちら](#)です。
バックナンバーは[こちら](#)でご覧いただけます。

牛島総合法律事務所
<https://www.ushijima-law.gr.jp/>