個人情報保護委員会による行政指導の近時の傾向

2023 年 8 月 29 日

弁護士　中井　杏

＜目次＞

改正個人情報保護法が施行された 2022 年 4 月 1 日以降、個人情報保護委員会により公表される行政指導事案が増加しており、2022 年度は 6 件、2023 年度は 8 月時点までに既に 4 件が公表されています（※）。
個人情報保護法が官民一元化され、個人情報保護委員会の監督権限が拡大する中、今後も行政指導が活発化することが見込まれるところ、本ニューズレターでは委員会の違反に対する権限や、近時の行政指導の内容や傾向について解説します。
※…行政機関等に対する行政指導、次世代医療基盤法に関する行政指導を含みます。

1.個人情報保護委員会の権限

個人情報保護委員会は、個人情報取扱事業者に対し、①報告の求め及び立入検査（法 146 条 1 項）、②指導及び助言（法 147 条）、③勧告（法 148 条 1 項）及び命令（法 148 条 2 項、3 項）を行うことができます。そして、命令に違反した場合に初めて、一年以下の懲役又は百万円以下の罰金が科されます（法 178 条）。

また、個人情報等の取扱いに関する苦情についてのあっせん（法 132 条 2 号）も行われており、本人からの個人情報保護法相談ダイヤルへの相談などがきっかけとなっています。

2.行政指導等の動向

個人情報保護委員会「令和 4 年度年次報告」によると、2022 年度の個人情報取扱事業者の漏えい等報告の処理件数は 7685 件、また、個人情報取扱事業者に対する報告徴収は 176 件（うち個情委によるものは 81 件）、立入検査は 26 件（うち個情委によるものは 1 件）、指導及び助言は 115 件となっています。
報告徴収、立入検査、指導及び助言が漏えい等事案以外についても行われるものであることも踏まえると、単に漏えい等報告を行っただけで、直ちに行政指導に至るものではないと考えられます。

3.行政指導が公表された事案

(1)漏えい等に関する事案

ア　決済情報の漏えいに関する事案（2022 年 7 月 13 日）

本件は、決済事業者が不正アクセスをうけ、決済情報等が格納されているデータベースから個人データが外部に流出した事案です。

漏えいしたことが確認された情報は、氏名、郵便番号、住所、電話番号、メールアドレス、クレジットカード番号、有効期限の計 593 件、漏えいした可能性がある情報は、クレジットカード番号、有効期限、セキュリティコードの計 460,395 件でした。

個人情報保護委員会からは、指導の原因となる事実として、決済事業者が多数の個人データを恒常的に取り扱うという性質を踏まえると、個人データ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み必要があるにも関わらず、①情報セキュリティ基本規程上、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おらず、どのシステムにおいて情報資産を取り扱っているか把握していなかったこと、②個人データの取扱い状況についての監査・点検を一部実施していなかったこと、③内部監査規定等において規定の外形のみ整備していたものの、それを実行するための人員配置等の実質を伴っていなかったこと、④不正侵入を検知した際のセキュリティアラートの十分な検証を行っていなかったことを指摘されています。

また、経済産業省からも 2022 年 6 月 30 日に割賦販売法に基づく改善命令を受けています。

イ　自治体から委託を受けた事業者による漏えいに関する事案（2022 年 9 月 21 日、2023 年 2 月 22 日）

本件は、自治体から臨時特別給付金支給事務を受託していた IT サービス事業者の再委託先の従業者が、暗号化された個人データを記録した USB メモリを紛失した事案です（その後、USB メモリは発見され、個人情報が流出した事実も確認されていないとのことです。）。

漏えい等のおそれがあった個人データは、全住民の住民基本台帳の情報（46 万 517 人分）、全住民の税情報（36 万 573 件）、非課税世帯等臨時特別給付金の対象世帯情報（R3 年度分 7 万 4,767 世帯分、R4 年度分 7,949 世帯分）、生活保護受給世帯と児童手当受給世帯の口座情報（生活保護 1 万 6,765 件、児童手当 6 万 9,261 件）で給付該当審査のための障害有無等の要配慮個人情報も含まれていました。

個人情報保護委員会からは、指導の原因となる事実として、生活困窮者に速やかに金銭的支援を行うという重要な事務に関連して多量かつ機微性の高い個人データ（障害の有無、口座番号等）を恒常的に取り扱う事業の性質を踏まえると、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るにもかかわらず、①個人データの取扱いに係る規律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、②委託された個人データの取扱い上のリスクの影響、対処可否、許容可否等を組織的に分析し承認するといったリスクに応じた必要かつ適切な措置を検討するための体制がなく、現場担当者のみで判断していたこと、③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こと、④委託先に対し個人データの取扱いについて、具体的な手順や講ずべき安全管理措置について何ら指示することなく、再委託先の従業員らに一任し、その検討結果の確認を行わず、実際の個人データの取扱いについて報告を求めることもなく、個人データの取扱い状況を把握していなかったことが指摘されています。

また、本件は自治体が保有する個人情報が漏えいしたおそれのあった事案として、報道でも大きく取り上げられました。さらに委託元自治体から IT サービス事業者に対しては、2950 万 1005 円の損害賠償請求がなされました。

ウ　車両の位置情報等の漏えいに関する事案（2023 年 7 月 12 日）

本件は、クラウド環境の誤設定により車両利用者に対するサービスのためのサーバが公開状態に置かれ、車両から収集した約 230 万人分の車載器 ID、車台番号、車両の位置情報等が、外部から閲覧できる状態にあり、個人データの漏えいが発生したおそれが生じた事案です。

個人情報保護法上の問題点としては、従業員に対する個人情報に関する研修内容が不十分だったため、車載器 ID、車台番号、車両の位置情報等が個人情報として認識されておらず適切な取扱いが行われていなかったことや、クラウド環境における設定に不備がありアクセス制御が適切に実施されていなかったこと及び委託先の監査・点検を実施しておらず、個人データの取扱い状況を適切に把握していなかったことが指摘されています。

エ　医療情報の管理をしていた委託先におけるプログラムの設定ミスによる漏えい事案（2022 年 11 月 2 日）
（次世代医療基盤法に関する事案）

本件は、A 社（委託先）及び B 社（再委託先）が、医療機関（委託元）から医療情報の管理及びその医療情

報の中から次世代医療基盤法に基づき A 社が提供を受けることができる情報（※1）を抽出し A 社のデータベースに転送する業務の委託を受けていたところ、プログラムの設定ミスにより、次世代医療基盤法に基づく患者への通知を行っておらず、A 社が提供を受けることができない情報（以下「未通知患者情報」といいます。）を A 社データベースに転送していた事案です。これは、プログラムの設定ミスによるものであり、医療機関が A 社に意図せず提供したものであるため、「漏えい」（個情法 26 条 1 項）として取り扱われています。

漏えいした個人データは、9 万 4,579 人分（※2）であり、医療情報であるため要配慮個人情報に当たります。

個人情報保護委員会からは、指導の原因となる事実として、医療情報は、患者が治療という目的を達成するために選択の余地が極めて乏しい中で提供した情報であるという側面を持っているのであり、当該個人データの性質及びその量からすると、漏えい等が発生した場合のリスクは特に高いこと、及び、次世代医療基盤法におけるオプトアウトの権利を奪わないようにしなければならないこと、本件は外観上同一の事業者であるが、法律上異なる性質の事業者の領域にデータが移転するという特質上なれ合いを防止する観点からとりわけ高い水準の安全管理等を講ずることが求められると指摘されております。

そして、そうであるにもかかわらず、①未通知患者情報の漏えいを覚知する端緒が存在しなかったために、被害の拡大及び長期化が生じたこと、②医療機関が委託先における医療情報の取扱い情報の報告を適切に求めていなかったこと、③委託先 A 社が再委託先 B 社の漏えい等防止措置の妥当性に関する検討を自ら行わず、B 社が提示した方策の確認や事後の検証も行っていないこと、④B 社におけるプログラム設定の妥当性の確認不足があり、未通知患者情報が A 社データベースに転送されていないことを確認する仕組みを構築していなかったこと、⑤漏えい等のおそれ等を検知した場合の報告連絡体制や報告の目標時間に係る規定の運用が十分に機能していなかったことが指摘されています。

また、行政指導の内容において、組織的安全管理措置及び技術的安全管理措置として、自社の責任者による確認だけではなく、委託先や外部の有識者による妥当性の確認を経ることとの指導がなされています。

※1…次世代医療基盤法においては、医療分野の研究開発のために医療情報を匿名加工して利用するために認定事業者に医療情報を提供することについて、医療機関が患者本人にあらかじめ通知し、本人がオプトアウトをしなかった医療情報について、認定事業者に提供することができます（次世代医療基盤法 30 条 1 項）。
※2…漏えい元となる医療機関のうち、6 医療機関は地方独立行政法人であり、本件発生時点では個人情報保護法が適用されなかったため、個人情報保護法の適用対象となる医療機関から漏えいした個人データにかかる本人の数は 4 万 4,395 人。

また、次世代医療基盤法に基づく通知を行っていない患者の情報を認定事業者に意図せず提供し漏えいした事案として、2023 年 7 月 12 日付行政指導も公表されています。

(2)不適切な個人データの取扱いに関する事案

オ　個人データである手術動画を本人の同意なく提供した事案（2022 年 11 月 2 日）

本件は、複数の医療機関が、眼科手術の術野を記録した手術動画を、患者本人の同意なく、医療機器メーカーに提供していたという事案で、各医療機関の従業者である医師が医療機関に無断で手術動画の提供を行っていることもあったという事案です。

医療機器メーカーに対しては、他社とデータのやり取りを行う場合は、データ内の個人情報の有無等を検討し、法令やガイドラインを遵守した適切な制度設計を行い運用すること等が指導されました。

また、手術動画を個人データとして管理していた医療機関については、適切に本人の同意を取得するよう指導がされました。さらに、従業者が無断で第三者提供を行わないよう適切な安全管理措置と従業者の監督を行う体制の整備及び従業者教育を行うことが指導されました。

合わせて公表された「医療機関における個人情報の取扱い」に関する注意喚起において、手術動画をその撮影順に記録し続けるのみで特定の個人情報を検索することができない状況の場合、手術動画は個人データに該当しないものの、手術動画の機微性等を踏まえれば、医療機関においては、これを適切に管理することが重要であるとの指摘がなされました。

なお、本件では本人の同意なく提供された手術動画の件数については公表されておりません。

カ　新電力顧客情報の不適切な取扱いに関する事案（2023 年 6 月 29 日）

本件は、グループ会社である一般送配電事業者と、関係小売電気事業者間において、一般送配電事業者が保有する顧客情報のうち、関係小売電気事業者以外の小売電気事業者（以下「新電力事業者」といいます。）と契約している者の顧客情報を、関係小売電気事業者がその立場を利用し、自社業務に利用していた事案であり、適正取得義務違反（個情法 20 条 1 項）並びに安全管理措置義務違反（個情法 23 条）及び委託先の監督義務違反（個情法 25 条）が指摘されています。

電気事業法においては、一般送配電事業者は託送供給等の業務に関して知り得た電気使用者に関する情報をその業務等の目的以外のために利用・提供することができず（電気事業法 23 条 1 項）、また一般送配電事業者とグループ会社である関係小売電気事業者は一般送配電事業者に対して、上記情報の提供等を求めてはならない（電気事業法 23 条の 3 第 1 項第 1 号）とされております。

しかし、一般送配電事業者と関係小売電気事業者は、送配電事業において管理していた顧客データベース（以下「送配電データベース」といいます。）を共同利用し、新電力事業者の顧客情報を関係小売電気事業者が閲覧できないよう情報遮断措置をとっていたものの、当該情報遮断措置に問題があったことを奇貨として関係小売電気事業者が新電力事業者に関する顧客情報を閲覧したり、送配電データベースへアクセスするための ID 又は操作端末の管理に問題があったことにより、関係小売電気事業者が送配電データベースを閲覧したりしていたことが指摘されております。また、一般送配電事業者は、非常時における顧客対応業務を委託するために、関係小売電気事業者に送配電データベースの閲覧権限を与えていたところ、関係小売電気事業者は非常時以外にも閲覧していたとのことです。さらに、関係小売電気事業者は、システム業務委託会社を通じて送配電データベースから新電力事業者の顧客情報を入手していたと指摘されています（その他にもいくつかの不適切な取扱いを指摘されています。）。

その結果、以下の指摘をされています。

(ア) 適正取得義務違反（個情法 20 条 1 項）

まず、個情法 20 条 1 項の「偽りその他不正の手段」とは、「不適法な」又は「適正性を欠く」方法（偽りによる方法を含む。）をいい、関係小売電気事業者の取得行為が、電気事業法に違反する方法による場合には、「不適法な」取得に該当し、同法に直ちに違反しないとしても、同法の制度趣旨や公序良俗に反している等、社会通念上、適正とは認められない取得行為である場合には、「適正性を欠く」との考え方が示されました。

そして、経済産業省の業務改善命令や、電気・ガス取引等監視委員会の「一般送配電事業者による非公開情報の漏えい事案に係る報告書」において、電気事業法違反や趣旨に違背する行為であると認定されていることを踏まえ、いくつかの関係小売電気事業者の取得行為が適正取得義務違反に当たるとされました。

(イ) 安全管理措置義務、委託先の監督義務違反（個情法 23 条、25 条）

まず、一般送配電事業者及び関係小売事業者が担っている電力関係事業は、いずれも国民の生活の基盤として不可欠な社会インフラであり、その公共的性質に鑑みると、各事業者においては、その取り扱う個人データに関し、高い水準での従業者の監督を含めた安全管理措置の整備が必須であると指摘されております。

そして、一般送配電事業者については、アクセス制御を適切に実施していなかったこと、個人データを取り扱う区域の管理を適切に行っていなかったこと、アクセスログの定期的な分析や、個人データの取扱いに関して定期的に監査を行っていなかったこと、従業員教育に関し、一般的な内容の研修を行うに留まり、送配電事業の中立性を実現するための適切な情報セキュリティの確保や個人データ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だったこと及び委託先としての関係小売事業者に対し定期的な監査等を行っていなかったことが問題点として指摘されています。

また、関係小売電気事業者については、個人データの取扱いについて定期的な監査を行っていなかったこと、従業員教育が一般送配電事業者と同様不十分であったこと、委託先の定期的な監査等を行っていなかったことが問題点として指摘されています。

本件では、漏えいした個人データにかかる本人の数は公表されておりませんが、新電力事業者に関する顧客

情報であったことから相当数が漏えいしたと考えられます。

なお、一般送配電事業者及び関係小売電気事業者は、同日付で、資源エネルギー庁が保有する「再エネ業務管理システム」に関する個人情報の取扱いについても、行政指導を受けています。

また、経済産業省から、2023 年 4 月 17 日に業務改善命令及び業務改善勧告がなされております。

4.行政指導が行われる事案の分析と実務対応のポイント

公表された事案は、違反事案について影響のある本人の数が多数（数万人以上）であったり、取り扱う個人情報の性質が医療情報や税に関する情報といった要配慮個人情報を含む機微な情報であったり、医療情報やインフラ、行政機関の保有する情報など当該情報を提供しない選択肢が本人にないといった事案、また複数の同種事業者で同様の違反が行われている事案であり、社会的影響が大きいという特徴があります。

さらに、いずれの事案も消費者、患者、住民といった属性の本人の個人情報に関する事案であり、この点からも社会的影響が大きい事案であるといえます。

公表事案において指摘されている違反法令は、漏えい等事案に関する安全管理措置義務違反（個情法 23 条~25 条）、適正取得義務違反（個情法 20 条 1 項）、本人同意のない第三者提供（個情法 27 条 1 項）等となっています。

行政指導の違反法令の内訳などは公表されていませんが、漏えい等報告が義務付けられていることにより、個人情報保護委員会における漏えい等事案の認知件数が多いことが原因だと考えられます。また、上記の法令違反は、社会的影響が大きくなる傾向にあることも一因だと考えられます。

企業においては、取り扱う件数が大量になる場合や、個人情報の性質が機微である場合、当該個人情報を本人が提供しないという選択肢が乏しい場合には、特に法令・ガイドラインに沿った対応と、高い安全管理措置を行っていくことが重要だと考えられます。

また、実務上、同業他社の対応を踏まえ自社の対応を決めるといったことは一般的ですが、個人データである手術動画を本人の同意なく提供した事案や、新電力顧客情報の不適切な取扱いに関する事案のように、複数の事業者がまとめて行政指導を受けることもあることから、業界慣行にかかわらず、必要に応じて自社としてのコンプライアンス対応を適切に検討していくことが重要です。

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」（無料：9/8（金）16:00～17:00 ＆ 後日配信予定）

以 上