日　時：令和７年３月 19 日（水）13：00～
場　所：個人情報保護委員会　委員会室
出席者：大島委員長代理、浅井委員、清水委員、藤本委員、梶田委員、髙村委員、
　　小笠原委員、宍戸委員
　　佐脇事務局長、西中事務局次長、小川審議官、大槻審議官、佐々木総務課長、
　　吉屋参事官、香月参事官、山口参事官、片岡参事官、澤田参事官

○佐々木総務課長　それでは、定刻になりましたので、会議を始めさせていただきます。
　本日は、藤原委員長が御欠席でございます。委員長代理に係る委員会決定の規定に基づき、大島委員長代理に以後の委員会会議の進行をお願いいたします。
○大島委員長代理　それでは、ただいまから、第318回個人情報保護委員会を開会いたします。
　本日の議題は三つです。
　議題１「地方公共団体等における個人情報保護法の運用に関する令和６年度の取組状況等について」、事務局から説明をお願いします。
○事務局　議題１「地方公共団体等における個人情報保護法の運用に関する令和６年度の取組状況等について」、御説明させていただきます。
　資料１の１ページ目を御覧ください。本議題は、地方公共団体等において令和３年改正法が令和５年４月１日に施行されたことに伴い、改正法の着実かつ円滑な運用・取扱いを確保するため、当委員会が実施した本年度の取組の状況等について御報告・御説明させていただくものでございます。
　資料、中ほどの「令和６年度における目標と取組の方向性」につきましては、昨年３月22日の第277回委員会で御説明させていただいており、目標として「委員会と地方公共団体等との信頼関係の維持・強化及び地方公共団体等の職員の更なる理解促進を通じた、地方公共団体等における適正かつ円滑な行政運営の確保」を掲げ、「令和６年度における取組の方向性」として、①地方公共団体等における改正法の着実かつ円滑な施行への支援、②地方公共団体の機関の実務に即した研修等の実施、③地方公共団体等に対する制度運用に資する情報の提供、④地方公共団体等における制度運用実態等の把握を挙げております。これらに基づいて、当委員会は地方公共団体等に対して多岐にわたる取組を実施してきたところです。
　２ページ目を御覧ください。本年度の取組状況について御報告いたします。
　「①地方公共団体等における改正法の着実かつ円滑な施行への支援」については、まず「法施行条例等の内容に関する分析調査結果等」として、前年度から引き続き地方公共団体から届出のあった法施行条例等の内容について分析調査を実施し、開示請求手数料等、条例で定める必要のある事項や条例要配慮個人情報等、必要に応じて条例で定めることが考えられる事項についてその実態や傾向を把握いたしました。調査結果を踏まえ、誤りや

不備等のある条例の規定を有する団体に対して、当該部分について指摘し、条例の内容にかかわらず、法令に基づく個人情報の適正な取扱いを確保するよう文書で通知いたしました。

次に、「地方ブロック担当窓口を通じた相談・照会への対応」として、改正法施行への対応・準備を契機に、令和４年度から地方ブロックごとの担当窓口を設置し、地方公共団体等からの相談・照会に対応してきたことを踏まえ、本年度も引き続き当該窓口を設置し、地方公共団体等の深化・多様化する課題や相談に寄り添うことで適切にサポートを実施しており、本年度２月末までの地方公共団体等からの相談・照会への回答件数は、延べ895件となっております。

なお、地方公共団体等からの相談内容は、令和４年度に比べ法施行条例等の制定・届出といった改正法施行への対応・準備に関するものが少なくなり、現行法の解釈や制度の運用、各団体が実施する事業における保有個人情報の取扱い等、一般的な課題に関する相談・照会が大部分となっております。

３ページ目を御覧ください。「②地方公共団体の機関の実務に即した研修等の実施」については、各地方公共団体の個人情報保護制度担当者の個人情報保護制度の理解促進に加えて、「団体間の横のつながり」及び「委員会と地方公共団体との顔の見える関係」の構築を目的として、本年度から当該担当者を対象に、グループ討議を中心とした実務に即した研修会を都道府県単位で実施することとし、８府県で開催いたしました。

次に、「③地方公共団体等に対する制度運用に資する情報の提供」として、行政機関等に係るガイドライン及び事務対応ガイドの一部改正を行ったほか、地方公共団体等が庁内研修等で活用できる教育コンテンツ（動画）を作成し、今月中に公表する予定です。

また、「個人情報保護法　いわゆる３年ごと見直しに係る検討」に関する状況等について、適時適切に情報提供を行い、併せて意見照会を実施したところです。

４ページ目を御覧ください。「④地方公共団体等における制度運用実態等の把握」については、さきに御説明の研修会の実施に際して、対象団体から制度運用の状況等についてアンケート調査を実施いたしました。アンケートでは、利用目的以外の目的のための利用及び提供における適法性の判断、開示請求に際しての開示・不開示の判断、職員個々の制度に関する理解促進などが懸念として寄せられたところです。

また、今月５日の第316回委員会で報告がありましたが、令和５年度における保有個人情報の取扱いに関する施行状況調査を実施したところです。

以上の取組状況から、改正法の施行に当たり必要であった法施行条例等の制定・届出については適切な対応がなされた一方、地方公共団体等においては現行法の運用に当たり、法令に基づく個人情報の適正な取扱いの確保が目下の課題となっており、制度運用に関する相談対応や理解促進についての支援は引き続き必要であると認識しております。

５ページ目を御覧ください。これらを踏まえ、次年度以降、「今後の地方公共団体等に対する支援の方向性について（案）」を御説明いたします。

まず、委員会においては、地方公共団体等における個人情報の適正な取扱いを確保するため、引き続き各種の取組を実施し、必要な支援を実施していくこととといたします。

具体的な支援の方向性として、「地方公共団体等からの照会・相談に対する対応」として、令和３年改正法の施行対応のための窓口は設けませんが、地方公共団体等から寄せられる法解釈を始めとした各種の照会や相談に対しては、引き続き寄り添った丁寧な対応を行い、適切にサポートを実施していきます。

「地方公共団体職員向けの研修の実施」として、地方公共団体職員向けに実務に即したグループ討議を中心とした研修を引き続き実施し、「団体間の横のつながり」及び「委員会と地方公共団体との顔の見える関係」の構築に努めていきます。

「地方公共団体等に対する制度運用に資する情報の提供」として、地方公共団体等のニーズを踏まえ、事務対応ガイドやQ&Aを適時適切に更新するほか、研修資料や広報資料等、制度運用に有用な情報を提供するとともに、制度改正を始めとする個人情報保護制度の動向等について、適時適切に情報を提供していきます。

「地方公共団体等における制度運用実態等の把握」として、地方公共団体等における制度運用に関する課題等を把握し、今後の制度の在り方に関する議論等につなげていきます。

以上で事務局からの説明は終わりますが、資料は委員会終了後、当委員会のホームページにて公表を予定しております。

以上でございます。

○大島委員長代理　ありがとうございました。

ただいまの説明につきまして、御質問、御意見をお願いいたします。

清水委員、お願いします。

○清水委員　ありがとうございます。

ただいま、事務局から地方公共団体等における個人情報保護法の運用に関する令和６年度の取組状況等について報告していただき、今後の支援の方向性について説明を頂きました。令和３年改正法の施行に当たり必要であった法施行条例等の制定・届出に関しては、三千を超える地方公共団体において適切な対応がなされ、また、新たな個人情報保護制度に基づく運用が日々行われているものと認識しております。

改正法の施行から２年が経過しようとしており、地方公共団体等においては法令に基づく個人情報の適正な取扱いの確保が重要な課題とされています。

また、「いわゆる３年ごと見直し」に係る検討も進められている現状に鑑みれば、これまでの改正法の施行・一元化に関する支援から、個人情報の適正な取扱いの確保に関する支援へと軸足を移す時期に来ていると考えます。

事務局におかれましては、地方公共団体等が直面している個人情報の取扱いに関する多様な課題に対して真摯に向き合い、引き続き団体に寄り添った支援をお願いしたいと思います。

以上です。

○大島委員長代理　ほかにはいかがでしょうか。よろしいでしょうか。

特に修正の御意見はないようですので、原案のとおり決定したいと思いますが、よろしいでしょうか。

御異議がないようですので、そのように取り扱うこととします。事務局においては所要の手続を進めてください。

また、本議題の資料、議事録及び議事概要の取扱いについてお諮りします。本議題の資料、議事録及び議事概要については、公表することとしてよろしいでしょうか。

御異議がないようですので、そのように取り扱うこととします。

それでは、次の議題に移ります。次の議題は、監督関係者以外の方は退席願います。

（監督関係者以外退室）

○大島委員長代理　議題２「株式会社イセトーに対する個人情報の保護に関する法律に基づく行政上の対応について」、事務局から説明をお願いします。

（内容について一部非公表）

○事務局　では、議題２に関しまして、御説明いたします。

まず、第１の「事案の概要」となりますが、株式会社イセトーは、金融機関や地方公共団体等の取引先から委託を受けて、様々な通知書の印刷・発送業務を実施しています。イセトーは、本件委託業務に伴い、本件委託元から個人データ及び保有個人情報の取扱いの委託を受けているところ、令和６年５月26日、イセトーのサーバが第三者から不正アクセスを受け、通知書の内容及び発送先に関する個人データの漏えい及び毀損が発生しました。

続いて、第２の「事実関係」となります。１の「本件漏えい等事態の概要」ですが、本件は、イセトーのサーバが第三者から不正アクセスを受け、個人データを含む電子ファイルがランサムウェアにより暗号化され、さらに窃取されたファイルがダークウェブ上に公開されたことにより、本件個人データについて漏えい及び毀損が生じた事案になります。

続いて、本件個人データの項目は、主に通知書に記載された氏名及び住所ですが、送付物の種類によりその他固有の情報が含まれます。例えば金融機関の通知書には確定拠出年金やローン残高等の金額、地方公共団体の納税通知書には税額情報等が含まれます。また、健康保険組合のジェネリック差額通知書には、要配慮個人情報が含まれます。

（３）は人数についてですが、本件個人データに係る本人数は合計3,076,477人で、うち民間事業者委託分は2,509,886人、行政機関等委託分は566,561人の内訳となります。このうち、要配慮個人情報が含まれる個人データに係る本人数は13,150人となります。

また、本件漏えい等事態で影響を受けた本件委託元は41団体であり、本件委託元に委託をしていた再委託元も含めた場合、影響を受けた団体数は約100団体となります。

続いて、２の「イセトーにおける個人データの保管状況」についてです。イセトーは通知書の印刷・発送業務を受託するに当たり、委託元から専用線、ファイル転送サービス等を通じて個人データを受領しています。イセトーは社内ネットワークを業務系ネットワー

クと基幹系ネットワークに分けて業務を行っているところ、イセトーによれば同個人データは業務系ネットワークでのみ保管し取り扱うルールとしていました。ただし、この保管ルールはあくまでもイセトー内でのルールであり、委託元とイセトーとの間で締結された契約書等には同ルールに関する記載はありませんでした。また、イセトーによれば、ルールは社内で公知のルールであったとのことですが、規程等に明文化されたものではなく、従業者は日々の業務の中でルールを理解していたとのことです。

続いて、３番の「不正アクセスの侵入経路及び本件漏えい等事態の発生原因」について説明します。

まず、（１）の「侵入経路」ですが、フォレンジック調査により、攻撃者はVPN機器を経由し、基幹系ネットワークへ不正に侵入したことが判明しました。しかしながら、イセトーによれば、イセトーにおけるログ取得が十分ではなかったことから、同VPN機器の認証回避方法及び基幹系ネットワークへの侵入方法の詳細の確認には至っていないとのことです。同調査によれば、攻撃者は基幹系ネットワークへの侵入後、同ネットワークのファイルサーバ及びPCから本件個人データを暗号化し、窃取しました。なお、業務系ネットワークへの侵入には成功していないことが確認されています。

続いて、（２）の発生原因になります。前記（１）のとおり、イセトーは、VPN機器のログを適切に取得していなかったため、フォレンジック調査によっても真因は分かっていません。しかしながら、VPN機器のアップデートに問題があり、侵入当時、最新パッチが適用されていませんでした。具体的には、イセトーは令和３年４月以降、アップデートを行っておらず、侵入当時、脆弱性について対応が未了でありました。

また、イセトーのパスワード管理においては、業務系ネットワークについては英文字、記号、数字の３種混合、８桁以上、30日で更新するパスワードポリシーを規定していました。他方、今回不正アクセスを受けた基幹系ネットワークについては、３種混合や８桁以上という制限はなく、45日でパスワード更新を行うということのみが規定されていました。

くわえて、本件で不正利用された管理者アカウントについては、基幹系ネットワークのものであるところ、パスワードポリシーにおいて45日で更新することを規定していたにもかかわらず、実際には更新を実施しておらず、平成29年２月から同じパスワードを使用していました。また、利用していたパスワードは推測がある程度容易な英小文字のみの11桁であり、十分な強度ではありませんでした。

以上から、本件における攻撃者の侵入については、不十分な脆弱性管理及びパスワード管理が原因となった可能性が高いものとなります。

続いて、「個人データの保管場所に関する問題点」です。前記２のとおり、イセトーでは保管ルールが存在していました。そのため、本件個人データについては業務系ネットワークでのみ保管し、基幹系ネットワークでは本件個人データを取り扱わないこととなっておりました。

しかしながら、イセトーの全56部署のうち開発部門等の３部署においては、部署内において本来アクセス権限がない従業者と業務データを共有する目的や、通知書発送の有無等の業務管理を行う目的で保管ルールを遵守せず、本件個人データを基幹系ネットワーク上のサーバへコピーの上、業務を行っていました。

かかる状況の下、攻撃者が基幹系ネットワークへ不正アクセスを成功させたため、本来は基幹系ネットワークに存在しないはずの本件個人データがランサムウェアにより暗号化され、かつ窃取され、ダークウェブ上に公開されて漏えいする事態に至りました。

続いて、４番の「二次被害の発生状況」ですが、イセトーによれば、令和６年６月18日の11時から22時30分の間、本件個人データがダークウェブ上へ公開されていました。イセトーでは本件委託元へ本件漏えい等事態に関する説明を行うとともに、本件個人データの悪用等による二次被害に関する情報提供を呼びかけているところ、現時点においてはそのような情報提供は受けておりません。

次に、第３の「個人情報保護法上の問題点」について説明いたします。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」とされているところ、イセトーにおける個人データの取扱いに関し、以下の問題点が認められました。

まず、（１）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」になります。個人情報の保護に関する法律についてのガイドライン10－６（３）において、「個人データを取り扱う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、適切に運用しなければならない」と規定しています。

しかしながら、前記第２の３（２）アのとおり、イセトーは、令和３年４月以降、VPN機器のアップデートを実施しておらず、VPN機器の認証に関連する脆弱性等について対応が未了でした。その上、イセトーにおいては基幹系ネットワークに関するパスワードポリシーにおいて、パスワードを45日で更新することを規定していたところ、管理者アカウントについては更新を実施しておらず、平成29年２月から同じパスワードを使用しておりました。そして、実際のパスワードは推測がある程度容易な英小文字のみの11桁でありました。なお、イセトーは多要素認証を導入しておりませんでした。

以上から、イセトーにおいてはVPN機器を最新の状態にしなかったことによってブルートフォース攻撃に関する脆弱性等が残存し、かつ、管理者アカウントのパスワードの強度が十分でない状態であったといえ、個人データを取り扱う情報システムを外部からの不正アクセスから保護する仕組みを導入し、適切に運用する点について不備が認められると考えられます。

次に、（２）組織的安全管理措置の「組織体制の整備」です。ガイドライン10－３（１）において、個人情報取扱事業者は、「安全管理措置を講ずるための組織体制を整備しなければならない」と規定しています。この点、イセトーにおいては保管ルールという

重要な業務ルールについて明文化がされておらず、実際に一部の部署において保管ルールが守られていませんでした。また、VPN機器については約３年もの間、アップデートがなされておらず、パスワードポリシーについても基幹系ネットワークについては桁数や文字についての制限がなく、更新日数についての規定は存在したものの遵守されておらず、約７年もの間、管理者アカウントのパスワード更新が行われていない状態でした。

このような不備については、イセトーにおいて経営層を含む管理者が適切に状況を把握できていなかったこと、また、個人データの取扱いに関する責任分担や役割の明確化が不十分であったことに起因するものと考えられ、安全管理措置を講ずるための組織体制の整備に問題があったものと認められると考えられます。

次に、（３）組織的安全管理措置の「個人データの取扱いに係る規律に従った運用」です。ガイドライン10－３（２）において、個人情報取扱事業者は、「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て個人データを取り扱わなければならない」と規定しています。この点、イセトーにおいては印刷・発送業務に係る個人データは業務系ネットワークでのみ取り扱う旨の保管ルールとなっていたものの、実態は３部署において同ルールが遵守されておらず、業務系ネットワークから本件個人データをコピーし、基幹系ネットワーク上のサーバに保存を行っていました。

今回、不正アクセスを受けた領域は基幹系ネットワークにとどまっており、仮に保管ルールが守られていた場合、本件個人データについて漏えい等は発生していなかったであろうという点を考慮すると、本件個人データの保管場所について、規律に沿った運用が実施されていなかった問題は大きいといえます。

また、ログ取得が不十分であった点については、定期的な設定確認、取得状況の把握等を行っておらず、個人データの取扱いの検証が可能な状態ではありませんでした。

次に、（４）組織的安全管理措置の「取扱状況の把握及び安全管理措置の見直し」です。ガイドライン10－３（５）において、個人情報取扱事業者は、「個人データの取扱状況を把握し、安全管理措置の評価、見直し及び改善に取り組まなければならない」と規定しています。イセトーにおいては、個人データの取扱状況について定期的な監査や点検が十分に実施できておりませんでした。そのため、長期間にわたり３部署が保管ルールを遵守せず、基幹系ネットワーク上のサーバに本件個人データを保管するという不適切な取扱いを発見及び是正することができませんでした。これはイセトーにおいて個人データの取扱状況を把握するための体制が整備されていなかったことに起因しており、その結果、本件漏えい等事態の影響が拡大したものといえると考えています。

最後に、（５）人的安全管理措置の「従業者の教育」です。ガイドライン10－４において、個人情報取扱事業者は、「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」とされています。イセトーは、従業者に対して定期的に一般的な情報セキュリティ等に関する研修を行っていましたが、保管ルールを明文化することなく、日常業務における暗黙のルールとして委託元から個人データ等の取

扱いを行っていました。そのため、保管ルールは従業者が常時確認できる状態ではなく、同ルールを周知しているといえる状態ではありませんでした。

このように、従業者に対する個人データの適正な取扱いの教育及び周知徹底が不十分であったことが、保管ルールを認知しながらも基幹系ネットワークへ本件個人データを移していた部署、また、目の前の業務遂行や効率化を重視し、リスク回避策が不明瞭なまま本件個人データを取り扱っていた部署が生じた一因になったものと考えております。

以上のとおり、イセトーにおいては、技術的安全管理措置、組織的安全管理措置及び人的安全管理措置に不備が認められます。

最後に、本件では、前記第３のとおり、イセトーにおいて法第23条が求める安全管理措置について不備が認められました。したがって、法第147条の規定により指導を行うこととしたいと考えております。

最後に、「公表について」です。本件は、攻撃者により実際に情報が窃取され、漏えいが生じた個人データに係る本人数が多く、再委託元等複数にわたる委託元を含めた場合、影響を受けた団体数も多いです。

次に、委託元は地方公共団体も多く、税関係情報等について多くの住民の保有個人情報の取扱いの委託を行っていたケースも複数見受けられ、行政機関等における個人情報の取扱いについての国民に対する透明性や信頼性の確保等の観点を考慮すべきであります。

最後に、漏えいが生じた個人データには、氏名及び住所に加えて、例えば確定拠出年金に関する金額、ローン残高、納税額等、個人の財産に関する情報等、漏えい等した場合に本人の権利利益の侵害が更に拡大するおそれが大きい個人データも含まれています。
したがって、このような事情等を考慮し、本件は公表することとしたいと考えております。

説明は以上です。

○大島委員長代理　ありがとうございました。

ただいまの説明につきまして御質問、御意見をお願いします。

浅井委員、お願いします。

○浅井委員　ありがとうございます。

事務局の御説明ありがとうございました。

一言コメントいたします。今回の事態は、不正アクセスによる個人データ漏えいの原因としてイセトーの安全管理措置の不備が指摘された事案で、指導の対処方針は理解いたしました。

本件にかかわらずですが、委託元にとって委託先の状況がリスクになることを考えますと、委託元の委託先に対する監督の重要性は大きいといえます。契約書等において安全管理措置に関する規定や実地確認の実施などは重ねて強化されるべき対処方法だと考えます。

以上です。

○大島委員長代理　ほかにはいかがでしょうか。

清水委員、お願いします。

○清水委員　ありがとうございます。

権限行使の御提案の内容につきましては、賛成いたします。

一言コメントなのですけれども、説明がありましたように、当該会社では保管ルールが遵守されていない状況を経営層が認識できていないという問題がありました。また、ログ取得が十分ではなかった、あるいはVPN機器のアップデートに問題があったと聞いております。

これらのことから、会社ではIT環境の適切な運用のための内部統制が適切に機能していなかったということがうかがえます。内部統制に係る責任は経営者にあることを改めて認識していただき、適切な運用を行っていただきたいと思います。

以上です。

○大島委員長代理　ほかはよろしいでしょうか。

それでは、特に修正の御意見がないようですので、原案のとおり決定したいと思いますが、よろしいでしょうか。

御異議がないようですので、そのように取り扱うこととします。事務局においては所要の手続を進めてください。

また、本議題の資料、議事録及び議事概要の取扱いについてお諮りします。本議題は、事案の社会的な影響を勘案し、配付の公表資料と当該資料に係る議事録、議事概要の部分を、準備が整い次第、委員会のホームページで公表し、それ以外の資料と当該資料に係る議事録、議事概要の部分については公表しないこととしてよろしいでしょうか。

御異議がないようですので、そのように取り扱うこととします。

それでは、次の議題に移ります。

議題３「監視・監督について」、事務局から説明をお願いします。

（内容について非公表）

本日の議題は以上です。

それでは、本日の会議は閉会といたします。