日　時：令和６年３月 22 日（金）15：30～
場　所：個人情報保護委員会　委員会室
出席者：藤原委員長、小川委員、大島委員、浅井委員、清水委員、加藤委員、梶田委員、
髙村委員、小笠原委員、
松元事務局長、山澄審議官、大槻審議官、森川総務課長、吉屋参事官、
香月参事官、小嶋参事官、片岡参事官、石田参事官

○森川総務課長　それでは、定刻になりましたので、会議を始めます。
本日は、全委員が御出席です。
以後の委員会会議の進行につきましては、藤原委員長にお願いいたします。
○藤原委員長　それでは、ただいまから第277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「いわゆる３年ごと見直し　実効性のある監視・監督の在り方①について」、事務局から説明をお願いいたします。
○芦田企画官　それでは資料に沿って御説明をさせていただきます。
本日の委員会におきましては、３年ごと見直しに関する検討項目の個別論点の検討の２回目として、検討項目の「実効性のある監視・監督の在り方」のうち、刑事罰の在り方と課徴金制度の導入について御議論をお願いできればと考えております。
これから資料に沿って順次御説明いたします。
１ページを御覧ください。現行法において、個人情報の取扱いについて、直接罰則が適用される、いわゆる直罰規定をまとめたものとなります。法第４章の民間規律が適用される個人情報取扱事業者については、第179条に個人情報データベース等不正提供等罪が規定されるとともに、第184条に法人等への両罰規定が設けられています。第179条は、個人情報取扱事業者（その者が法人等である場合にあっては、その役員等）若しくはその従業者又はこれらであった者が、その業務に関して取り扱った個人情報データベース等（その全部又は一部を複製し、又は加工したものを含む。）を自己若しくは第三者の不正な利益を図る目的で提供し、又は盗用したときに成立し、１年以下の懲役又は50万円以下の罰金に処することとしています。
２ページを御覧ください。令和２年の個人情報保護法改正においては、罰則規定について法定刑の引上げが行われました。同改正においては、法第184条第１項第１号に規定する両罰規定については罰金の上限を30万円から１億円に引き上げています。
他方、個人情報データベース等不正提供等罪に係る行為者に対する罰則については、平成27年の個人情報保護法改正によって創設された罰則であり、施行されてから十分な期間が経過していないことも踏まえ、令和２年改正においてはその法定刑を維持することとしました。
３ページ目を御覧ください。昨今、個人データの取扱いについて、内部的な不正行為に

起因する悪質な事例が増加傾向にあるように見られます。例えば事例①として、個人情報取扱事業者の元従業者が、元勤務先が管理する名刺情報管理システムのログイン認証情報を不正に転職先の従業者に提供し、同システムを第三者が利用可能な状態に置いた事例があります。事例②として、大手学習塾の元塾講師が当該学習塾の児童の個人情報をSNSのグループチャットに投稿したとされる事例があります。このうち、事例①については個人情報データベース等不正提供等罪（法第179条）等により、元従業者が逮捕・起訴され、有罪が確定しております。

こうした状況を踏まえ、個人情報保護委員会としても、個人情報取扱事業者として講ずべき安全管理措置の内容や、個人データの漏えい等が発生した場合の報告体制等について注意喚起を行っております。

４ページを御覧ください。３ページで御紹介したもの以外にも、個人データが不正に取り扱われ、個人の権利利益が侵害されるおそれが生じた事例が見られます。例えば事例Ａは、複数の個人情報取扱事業者の従業者が、個人の身体の一部を含む動画であって個人データに該当するものを、不正に第三者に提供しており、当該提供が個人情報取扱事業者に無断で行われていた場合もあったというものです。

また、事例Ｄは、個人情報取扱事業者の従業者が、当該個人情報取扱事業者に業務を委託した委託元の顧客等の個人データ等を、不正に持ち出したものです。持ち出された個人データ等は、名簿業者に売却された可能性が高いと見られています。当該個人情報取扱事業者は、委託元から依頼を受け調査を実施し、当該委託元に対して個人データの漏えい等は確認されなかった旨を報告していましたが、実際には、上記不正な持ち出しが、当該調査以前のみならず、それ以降も行われていたというものです。

このように、内部的な不正行為に起因する悪質な個人データの漏えいが発生しており、中には悪質と見られる事例も含まれることを踏まえ、抑止力を高める観点から法定刑を引き上げるべきか、また、現実に発生する多様な事例を踏まえ、法第179条がその趣旨に照らして過不足なく処罰対象となるべき行為をカバーしているか検証し、必要に応じて処罰範囲を見直すべきかが論点となるかと考えられます。

５ページを御覧ください。個人情報の不正取得行為については、国内の他法令において規律が設けられている例があります。例えば番号法は、第51条において「人を欺き、人に暴行を加え、若しくは人を脅迫する行為により、又は財物の窃取、施設への侵入、不正アクセス行為その他の個人番号を保有する者の管理を害する行為により、個人番号を取得すること」について、３年以下の懲役と150万円以下の罰金刑を定めています。そのほか、割賦販売法、統計法、不正アクセス禁止法等において、情報の不正取得行為の処罰規定が設けられています。

６ページを御覧ください。個人情報の不正取得行為については、当委員会の個人情報保護法相談ダイヤルに対して相談が寄せられている例があります。例えば事例Ａは、PCが突然操作できなくなり、メッセージが流れ、電話番号が表示され、電話するよう誘導された。

電話するとテープが流れ別の電話番号に誘導され、その電話番号で契約者名、住所、電話番号等を聞かれ、その内容を伝えた。心配になり、契約先に確認したところ、詐欺かもしれないと言われたというものです。ほかにも、事例ＢからＥにあるように、詐欺等により個人情報を提供してしまったという相談事例が見られます。

加えて、行政機関が実施する調査であるかのような紛らわしい説明をして、個人情報等を聞き出す、「かたり調査」のトラブルも見られます。このような個人情報の詐取等の不正取得行為の相談状況等を踏まえ、個人の権利利益の侵害を防止する観点から、個人情報の詐取等の不正取得行為を直罰規定の対象とすることをどう考えるかが論点となるかと考えられます。

続いて、課徴金制度について御説明いたします。今回は概括的な説明として資料を準備しております。本日の委員会での御議論等も踏まえ、今後、更なる資料等を準備することができればと存じます。

７ページを御覧ください。ここでは個人情報保護法上の監視・監督の流れを記載しています。当委員会は、総合的な案内所、個人情報取扱事業者からの漏えい等報告、その他メディア報道等の外部の情報源から監視・監督に係る情報を得ています。こうした情報を踏まえ、必要に応じて報告徴収・立入検査を行います。その結果により、指導・助言、勧告を行い、勧告を受けた個人情報取扱事業者等が正当な理由なく勧告に係る措置を執らなかった場合において、個人の重大な権利利益の侵害が切迫していると認められるときは、命令を発出するという枠組みになっています。個人の重大な権利利益を害する事実があるため、緊急に措置を執る必要があると認めるとき等の一定の要件を満たす場合には、勧告を経ずに命令、いわゆる緊急命令を発出することも可能です。

８ページ目を御覧ください。７ページで御説明した命令について、これに違反した場合には法第178条により罰則の対象となります。法定刑は、行為者は１年以下の懲役又は100万円以下の罰金刑であり、第184条の両罰規定により法人等も１億円以下の罰金刑の対象となります。また、当委員会への虚偽報告等についても、第182条により行為者は50万円以下の罰金刑の対象となるほか、第184条の両罰規定により法人も50万円以下の罰金刑の対象となります。

９ページを御覧ください。ここでは、法令に基づき賦課される金銭の種類等を記載しています。法令に基づき賦課される金銭としては、課徴金のほか、先ほど御紹介した個人情報データベース等不正提供等罪等の罰金、科料、過料があるとされています。課徴金とは、一般には、国がその司法権又は行政権に基づいて国民に賦課し国民から徴収する負担で租税以外のものであり、刑罰ではなく行政上の措置とされています。課徴金には独占禁止法、金融商品取引法等に規定されているような罰金その他の処罰収入のように一方的に賦課徴収するもの、河川法、道路法等に規定されているような公益のため必要な特定の事業に特別の関係を有する者に対してその経費の全部又は一部を強制的に負担させるものがあるとされています。

また、罰則については、犯罪に対して課せられる制裁である刑罰、行政法上の義務に違反する行為に対して、一般統治権に基づく制度として科せられる罰である行政罰があります。

10ページを御覧ください。ここでは、国内の他法令における課徴金制度の概要を記載しています。我が国では、独占禁止法が昭和52年に課徴金制度を導入したのを皮切りに、金融商品取引法、公認会計士法、景品表示法、薬機法に順次導入されています。また、独占禁止法については、制度導入後、累次の改正により対象行為の拡大、算定率の引上げ等を行っています。

この表では、課徴金の対象となる行為とともに課徴金額の算定方法、対象となる規模の基準をまとめています。例えば独占禁止法については、違反行為を抑止するため、違反行為に基づく不当利得相当額をベースとしつつ、不当利得相当額以上の金銭を徴収する仕組みとされています。

11ページを御覧ください。個人情報保護法の過去の改正においても課徴金に関する議論がされています。平成27年の改正時には、制度見直し方針の段階において第三者機関に行政処分等の権限を付与するとともに、罰則の在り方等を検討するとされた上で、制度改正大綱においては課徴金制度の導入については、引き続き検討することとされました。

12ページを御覧ください。こちらは令和２年改正時のものですが、制度改正大綱において、「我が国の法体系、執行の実績と効果、国内外事業者の実態、国際的な動向を踏まえつつ、引き続き検討を行っていく」とされました。

加えて、法案審議においては、参議院の内閣委員会における附帯決議で、「違反行為に対する規制の実効性を十分に確保するため、課徴金制度の導入については、我が国他法令における立法事例や国際的な動向も踏まえつつ引き続き検討を行うこと」とされました。

このように、これまでの検討の経緯や国内法制度の状況等を踏まえ、個人情報保護法違反行為を実効的に抑止するための手段として課徴金制度を導入するべきかが論点となるかと考えられます。また、仮に導入するとした場合には、対象となる行為、課徴金額の算定方法等の考え方についても論点となるものと考えられます。

事務局からの説明は以上となります。よろしくお願いいたします。

○藤原委員長　ありがとうございました。

それでは、ただいまの御説明について御質問、御意見をお願いいたします。

清水委員、どうぞ。

○清水委員　ありがとうございます。

個人情報保護法は、個人情報の有用性に配慮しつつ、個人の権利利益を保護することを目的としています。しかしながら、現在の刑罰は、この目的の前者の有用性、特に経済的価値に重きを置いているように思います。後者の個人の自由や権利に対する侵害にも注目して、抑止力としての刑罰や政策目的の達成のための行政処分を考える必要があると考えています。

以上が基本的な私の考え方なのですが、その上で２点、コメントさせていただきたいと思います。

まず、刑罰についてなのですが、現行の法第179条は、個人情報取扱事業者における個人情報データベース等の不正提供等罪を規定していますが、その根拠として、個人情報データベース等の利用価値が高いことが前提にあります。しかし、まとまったデータベースでなくとも、個人情報の不正取得による重大な人権侵害を及ぼすケースが、御説明にありましたように出てきています。したがって、不正取得行為を刑罰の対象とすることが考えられます。以上が１点目です。

次に、課徴金についてですけれども、私の意見としましては、政策目的達成のために、多様な行政処分の手段として課徴金を導入することを検討すべきと考えています。ここにおいても不当に得た利得に限りますと、これは経済的に測定可能な利益に限定されてしまいます。しかしながら、現実には、適切な措置をとらなかったことにより、人権侵害等の経済的には測定が難しい被害も起きています。このような場合には、不作為による節約額を基準値として、故意・過失等を勘案して課徴金を算定するということも検討すべきではないかと考えます。

以上です。

○藤原委員長　ありがとうございました。

ほかにはいかがでしょうか。よろしいですか。

それでは、いわゆる３年ごと見直しについて、事務局から実効性のある監視・監督の在り方の対象として､刑事罰の在り方及び課徴金制度の導入について説明があったわけです。私からも一言申し上げておきますと、刑事罰の在り方のうち、個人情報データベース等不正提供等罪の法定刑について、現実に発生している事案における個人の権利利益への影響等も踏まえ、類似の行為に係る罰則の法定刑にも目配りをしつつ、十分な抑止力を有するかという観点からさらに検討を深めていけばいいのではないかと思っております。

また、直罰規定の対象となる行為の範囲について、個人情報が不正に取り扱われた悪質事案を、先ほどの説明にもありましたけれども、過不足なく対象とし得るのかという観点から、現実に発生している事案等を踏まえ、検討を行っていくことが適当であろうと思います。

その際には、３月６日の個人情報保護委員会において小川委員から、我が国の経済社会の情報化・デジタル化の発展を阻害するような個人情報の取扱い、例えば特殊詐欺やフィッシングなどについては個人情報の取扱いを厳しく規律すべきであるという意見があったこと、それから本日、清水委員からも、個人情報保護法の二つの柱のうちの個人の権利や自由の侵害の側面も重く見るべきではないか、人権侵害といった点から、データベースだけでなく不正取得行為を罰するべきではないか、といった意見があったということも踏まえることが重要ではないかと思います。

また、課徴金制度の導入につきましては、今日整理いただいたように多くの領域で課徴

金制度は導入されておりますので、国内の他法令における課徴金制度に関する理解を深める観点から、有識者に対するヒアリングを行うことが適当ではないかと思います。ヒアリングの実施に向けて、事務局において所定の準備を進めていただきたいと思います。

また、今後の検討の際には、清水委員から課徴金の捉え方について、経済的に測定可能な利益以外の点も考慮すべきという御意見があったということも踏まえておいていただきたいと思います。

ほかに特に御意見がないようですので、私から申し上げましたけれども、こういう観点・内容を踏まえて、事務局において検討の準備を進めていただきたいと思いますが、よろしいでしょうか。

ありがとうございます。

それでは、今、申し上げたような観点を踏まえて更に検討を深めてください。よろしくお願いします。

○芦田企画官　承知しました。ありがとうございます。

○藤原委員長　それでは、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たいと思います。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。

ありがとうございます。御異議がないようですので、そのように取り扱うことといたします。

それでは、次の議題に移ります。

議題２「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５年度の取組状況等について」、事務局から説明をお願いいたします。

○事務局　それでは、議題２「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５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２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年改正法が昨年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今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。

資料中ほどにありますとおり、令和５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29日の第238回委員会で御説明させていただいておりまして、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・強化を通じた地方公共団体等の行政運営の適正かつ円滑な運用の確保」を掲げ、令和５年度における取組の方向性として、「①実態を踏まえた運用の更なる検討及び制度の浸透に向けた周知・啓発活動の展開」、「②改正法施行後の地方公共団体等における適正な対応の確保」を挙げております。こちらに基づいて、当委員会は今年度、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ございます。

２ページ目を御覧ください。今年度の取組状況について御報告いたします。取組の方向

性①「実態を踏まえた運用の更なる検討及び制度の浸透に向けた周知・啓発活動の展開」については、まず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４団体、京都府、岡山市、宮崎県都城市、埼玉県上里町に対し、制度の運用状況や課題、意見等について聴取すべく、先日２月14日の第272回委員会においてヒアリングを実施いたしました。

また、地方公共団体を直接訪問し、制度運用の実態や好事例、当該団体の抱える課題、制度や委員会への要望を把握すべく、対面での意見交換を実施いたしました。44団体と意見交換を実施し、Q&A等を改正し、照会への回答例や具体的事例を充実してほしい、委員会による研修機会や研修資料の提供、相談窓口の体制確保など、引き続きサポートを充実してほしいなどの御意見を頂戴したところでございます。

次に、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、Q&A（行政機関等編）の追加・更新を今月中に実施するほか、自治大学校、地方公共団体情報システム機構等と連携し、各種の研修の実施や広報パンフレット、動画等を地方公共団体等が広く活用できる周知・啓発資料を作成・公表したところでございます。

３ページ目を御覧ください。「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、昨年度構築した地方ブロックごとの担当窓口を令和５年度も維持し、当該窓口において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、今年度は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1,927件となっております。

また、「地方公共団体に対する研修の企画・検討」として、地方公共団体の意見交換の結果を踏まえ、令和６年度から地方公共団体向け研修を実施すべく、地方公共団体から出向され、委員会事務局経験のある職員を招集し、研修内容について検証・意見交換を実施するなどして当該研修の効果的な研修手法等について企画・検討を進めており、併せて都道府県に対して研修開催希望調査を実施いたしました。

４ページ目を御覧ください。続いて、取組の方向性②「改正法施行後の地方公共団体等における適正な対応の確保」につきまして、「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対応」として、地方公共団体の手数料条例を含む法施行条例について、整備状況調査等により、28の一部事務組合が令和５年４月１日時点において未措置の状況にあることを把握し、当該未措置団体に対して個別アプローチを行い、法施行条例の整備が完了したことを確認しております。

また、地方公共団体が定めた法施行条例は、いずれも個人情報保護法第167条第１項に基づき委員会に届出がなされ、委員会において同条第２項に基づき3,338件の条例を公表いたしました。

次に、「法施行条例の内容に関する分析及び地方公共団体等への支援」として、委員会へ届出がなされた法施行条例の内容について、現在、精緻な分析を行い、その実態や傾向を調査しております。今後、この調査結果を踏まえて、必要に応じ、制度運用に関し留意

すべき点の全国的な周知・助言や、課題を有する団体の個別アプローチの実施について検討することとしています。

５ページ目を御覧ください。続きまして、「令和６年度の地方公共団体等に対する対応の方向性について」を御説明いたします。まず、目標を「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」とさせていただきました。

具体的な取組について、「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」として、地方ブロックごとの担当窓口を引き続き設置し、地方公共団体等の照会や相談に寄り添い、適切にサポートを実施することに加えて、先ほど御説明いたしました法施行条例の内容分析を踏まえた地方公共団体等へのフォローアップを実施していきます。

「地方公共団体の機関の実務に即した研修等の実施」として、自治大学校、地方公共団体情報システム機構等と連携し､様々な媒体を活用して各種の研修等を実施していきます。

「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、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、地方公共団体等が制度を運用するに当たって有用な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保有個人情報の取扱いに関する施行状況や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くことといたします。

以上で事務局からの説明を終わりますが、資料につきましては、委員会終了後、当委員会のホームページにて公表することを予定しております。

以上でございます。

○藤原委員長　ありがとうございました。

ただいまの説明について御質問、御意見をお願いいたします。

では、清水委員、お願いいたします。

○清水委員　御報告ありがとうございました。私からは、５ページに書いていただいています目標のうち、二つ目の研修について一つ意見を申し上げたいと思います。

地方公共団体等におけます個人情報の適正な取扱いを確保する上では、職員の法制度の理解浸透が大変重要だと認識しております。しかしながら、残念ながら今年度も各所で漏えい事件が起きているのも事実です。

したがって、記載していただいているとおり、研修をぜひ充実させていただきたいと思っています。特に、研修に当たりましては、講師が制度を解説するｅラーニングの形式を利用するという方法が効果的であると考えます。

令和５年度は、既に地方公共団体情報システム機構と連携した研修を行っていただいておりまして、講師が制度解説する動画を用いていただいておりますが、今年度の実績で約３万８千人が受講したと伺っております。

今後はこうしたコンテンツをできる限り多くの職員に受講していただくことができます

ように、階層別、あるいは内容別に分けるなど、ターゲットを明確化するとともに、それに合わせた解説内容の見直しを行うなどの工夫を凝らして、より積極的に取組を進めていただきたいと思います。

よろしくお願いします。

○藤原委員長　ありがとうございます。

ほかにはいかがでしょうか。特にないですか。

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いたします。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いたします。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。

ありがとうございます。御異議がないようですので、そのように取り扱うことといたします。

それでは、次の議題に移りたいと思います。次の議題は、監督関係者以外の方は御退席願います。

（監督関係者以外退室）

○藤原委員長　議題３「株式会社エムケイシステム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」です。本議題については、個人情報保護委員会議事運営規程第11条の規定に基づき、梶田委員には御退室いただきます。よろしくお願いいたします。

（梶田委員退室）

○藤原委員長　それでは、事務局から説明をお願いいたします。

（内容について一部非公表）

○事務局　では、資料３－１に基づき、説明いたします。

まず、事案の概要です。株式会社エムケイシステム（以下「エムケイ社」という。）は、主に社労士事務所を対象に社会保険や人事労務の業務支援システムをクラウドにて提供しておりましたところ、昨年６月、ランサムウェア攻撃により、管理していた個人データが暗号化され、個人データの漏えい等のおそれが発生いたしました。本件システムには、社労士の顧客である企業や事業所等の従業員等の個人データが大量に保管されておりました。

なお、現時点で個人データの悪用は確認されておりません。

次に、事案の規模についてです。エムケイ社からの情報によりますと、本件システムの利用実績は、２の（１）に御説明しております値のとおりでございます。

当委員会が受領した漏えい等報告の件数につきましては、資料３－２の概要図で御説明いたします。漏えい等報告総数は、右下の表のとおり、報告者ベースで3,067件、本人数合計は約750万人でした。漏えい等報告の大部分は社労士事務所からの提出でした。なお、本

人数につきましては、社労士事務所とクライアントの双方が漏えい等報告を提出した場合は、本人数が重複して数えられている可能性がございます。

それでは、資料３－１の２ページに戻りまして、項目３として、エムケイ社が本件において個人データを取り扱っていたとの判断に至った経緯について御説明します。まず、個情法ガイドラインQ&Aでの記載内容の確認です。ガイドラインQ&Aでは、「クラウドサービス提供事業者が、当該個人データを取り扱わないこととなっている場合とは、契約条項によって当該外部事業者がサーバに保存された個人データを取り扱わない旨が定められており、適切にアクセス制御を行っている場合等」と記載されております。

続いて、本システムの利用規約についてです。利用規約には、エムケイ社によるユーザの個人データの取扱いについて規定されている条項があり、本件システムの利用に当たり、ユーザにはこの規約への同意を求めておりました。

続いて、エムケイ社における実際の個人データの取扱いの状況についてです。エムケイ社は、ユーザから本件システムの利用に関する調査や支援要請があった場合、「個人情報授受確認書」を取り交わした後、個人データを取り扱っておりました。授受確認書には「媒体　お客様の委託データ」「授受の形態　保守用IDによるデータ調査」などと記載されております。授受確認書によるエムケイ社による取扱実績は、令和５年上半期で合計20件でございました。

それでは、以上を踏まえた検討結果を御説明いたします。

１点目として、利用規約についてです。利用規約には、エムケイ社が必要であると判断した場合、ユーザが提供するデータについて必要な行為を行うことができるとの規定があり、また、エムケイ社がユーザの顧客の個人データを使用等できることが前提となっている規定も見受けられました。

２点目として、アクセス制御についてです。エムケイ社は、保守用IDで本件システム内の個人データにアクセス可能な状態であり、エムケイ社の取扱いを防止するためのアクセス制御等の措置は講じられておりませんでした。

３点目として、サービスの性質についてです。本件システムは、社会保険業務等をオールインワンで提供するという性質から、大量の個人データが保管・管理されることが前提となっているシステムでした。

４点目として、エムケイ社による個人データの取扱いの状況についてです。先ほど申し上げましたとおり、エムケイ社はユーザと授受確認書を取り交わした上で、ユーザの個人データを取り扱っていたという実績がございました。

以上の事実より、本件においてはエムケイ社がガイドラインQ&A記載の「個人データを取り扱わないこと」となっていたとは言えず、また、取扱いを防止するための適切なアクセス制御が行われていなかったことが認められます。したがって、エムケイ社は個人情報取扱事業者としてユーザから個人データの取扱いの委託を受けて個人データを取り扱っていたと言えます。

続いて、４ページ目の項目４にて、法律上の問題点につき、個情法の観点からエムケイ社、ユーザ、クライアントの順で検討し、加えて番号法上の観点からの検討結果を御説明いたします。

まず、エムケイ社について、法第23条の安全管理措置に関する点でございます。法第23条は、「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」と規定しております。ガイドラインでは、技術的安全管理措置として、アクセス者の識別と認証の観点では、「個人データを取り扱う情報システムを使用する従業者が正当なアクセス権を有する者であることを、識別した結果に基づき認証しなければならない」こと、また、外部からの不正アクセス等の防止の観点では、「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」ことを規定しております。

しかし、本件システムは、パスワードルールが脆弱であったこと、深刻な脆弱性が残存していたこと、ログが適切に管理されていなかったこと等が判明しており、エムケイ社には技術的安全管理措置に不備があったと認められます。

続いて、エムケイ社の委託元である社労士事務所等ユーザについて検討いたします。まず、技術的安全管理措置についてですが、本件はエムケイ社の不適切な運用管理が原因であることから、ユーザには技術的安全管理措置の不備は認められません。

他方、法第25条では、個人情報取扱事業者が個人データの取扱いを委託する場合は、委託先に対する必要かつ適切な監督を行わなければならない旨を定めています。また、ガイドラインでは、委託元である個人情報取扱事業者は、個人データが漏えい等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、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適切な委託先の選定、委託契約の締結及び委託先における個人データ取扱状況の把握について、必要かつ適切な措置を講じなければならないと規定しています。

本件発生当時のエムケイ社のサイトには、万全のセキュリティ管理や漏えい対策をしている旨が記載されておりました。本件において、ユーザの多くはエムケイ社に対する個人データの取扱いの委託を行っていたとの認識が薄く、委託先の監督が結果的に不十分となっていた可能性があります。

次に、ユーザの委託元であるクライアントについて検討いたします。社労士事務所に対して個人データの取扱いを委託していたクライアントも、個人情報取扱事業者として、安全管理措置と委託先の監督の義務を負います。クライアントにはユーザの場合と同様、技術的安全管理措置の不備は認められません。

他方、多くのクライアントは社労士事務所に対する委託及びエムケイ社に対する再委託を行っていたとの認識が薄く、委託先等への監督が結果的に不十分となっていた可能性があります。

続きまして、番号法上の問題について御説明します。本件システムではマイナンバーも取り扱われておりましたが、電子申請時等にマイナンバーを入力しても保管されない仕組みとなっておりました。ユーザがオプションサービスを利用する場合は、高度に暗号化された状態でマイナンバーが保管されておりましたことから、番号法による指導は行わないこととといたします。

最後に、対応方針について御説明します。エムケイ社は、本件を機にセキュリティが強化されている環境でのシステム再構築などの対策を実施の上、サービスを再開しております。しかし、エムケイ社が大量の個人データの取扱いの委託を受けていること及び安全管理措置に不備が認められたことから、法第147条の規定により指導し、再発防止策の実施状況を含む安全管理措置の改善状況について報告を求めることといたします。

ユーザ及びクライアントに対しては、委託先等の監督が不十分となっていた可能性を踏まえ、実際に個人データの取扱いがあったユーザ及びクライアントを中心に継続して調査し、必要な対応を検討いたします。

また、クラウドサービスの利用が委託等に該当する場合があることの周知のために、資料３－３の注意喚起を発出することといたします。

以上で説明を終了いたします。

○藤原委員長　ありがとうございました。

それでは、ただいまの説明について御質問、御意見をお願いいたします。

小川委員。

○小川委員　御説明ありがとうございました。

本件においては、利用契約においてエムケイ社の判断で個人データの保守や分析が行われるということが広範に認められていました。保守に関しては、例えば疑似データを利用するなどによって個人データを取り扱わないやり方も考えられるし、あるいは個人データの授受については、ユーザの同意を得てユーザサポートの一環として行うことが適当な場合もあります。

再発防止に向けて、アクセス制限の観点などからもより適切な個人データの取扱いのルールを検討していただきたいと思います。

以上です。

○藤原委員長　ありがとうございました。

ほかにはいかがでしょう。

清水委員、お願いいたします。

○清水委員　ありがとうございます。エムケイ社の事業者としての責任について、意見を申し上げたいと思います。

エムケイ社が保守・運用上又は技術上必要と判断した場合、若しくはユーザの要請による場合、クライアントの個人情報にアクセスすることができ、この範囲でユーザはエムケイ社に委託を行っておりました。そのような状況に鑑み、ユーザ側に対して、委託先であ

るエムケイ社に対する監督が不十分であったとして注意喚起が現在提案されているわけです。

しかしながら、エムケイ社は、ユーザに対し、万全のセキュリティ管理を講じていると説明していたことから、ユーザ、特に零細事業者がエムケイ社に対して、踏み込んだ監督権限を行使できるかといった点については実務上難しい点があると思います。むしろ、クラウドサービス提供事業者であるエムケイ社の責任において、個人データの取扱い、特に委託に該当する部分の取扱いや、それに関するセキュリティ対策について、適切にユーザに説明することが、契約の透明性を高め、事業者としての責任を果たすために必要であると考えます。

以上です。

○藤原委員長　ありがとうございました。

ほかにはいかがでしょうか。

それでは、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。

ありがとうございます。御異議がないようですので、そのように取り扱うことといたします。事務局においては所要の手続を進めてください。

それから、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いたします。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。

ありがとうございます。御異議がないようですので、そのように取り扱うことといたします。

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。