個人情報保護委員会（第２６３回）議事概要

１　日　時：令和５年 12 月６日（水）１４：００～
２　場　所：個人情報保護委員会　委員会室
３　出席者：丹野委員長、小川委員、中村委員、大島委員、浅井委員、
藤原委員、梶田委員、髙村委員、
松元事務局長、三原事務局次長、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
４　議事の概要
（１）議題１：マイナンバーカード等に係る各種事案に対する個人情報保護委員会の対応について

事務局から、資料に基づき説明を行った。

中村委員から「マイナンバーカード等に係る各種事案に関して、それらの再発防止策の一部については、システム改修を予定しているといったものや特定個人情報保護評価のように継続的な対応が求められるものなどが含まれており、当委員会としては、こうした再発防止策について適切に取り進められているのか、フォローアップしていくことが必要であると思う。また、今後、新たな課題が顕現化した場合には、個人の権利利益の保護の観点から、適時適切に対応していくことが肝要であると思う」旨の発言があった。

髙村委員から「健康保険証及び障害者手帳におけるマイナンバーの紐付け誤りについては、制度の所管省庁及び事務の実施者が適切な運用を徹底していたかといった組織的・人的安全管理措置とともに、ヒューマンエラーが起き得る前提に立って、安全に登録を完了することができる技術的安全管理措置を講じていくことが求められる。こうした観点から、再発防止策を評価すると、それぞれの責任主体において、これらの着眼点を踏まえ、適切に対策が進められているものと一定の評価ができる。

もっとも、再発防止策のなかで、データの正確性を確保するためには特に重要と考えられるシステム改修は、今後実施予定とされている。このため、当委員会としては、保険者や地方公共団体の取組状況とともに、所管省庁等によるシステム改修の確実な実施について、引き続き注視していくことが必要であると考える」旨の発言があった。

丹野委員長から「マイナンバーカード等を活用したサービスは、全ての国民に関わるものであり、何よりも国民の信頼を得ることが重要である。このため、当委員会としては、マイナンバーカード等に係る一連の問題について、発生当初から極めて重要な問題として捉え、遺漏なく調査分析を行った上

で、明らかになった事実に基づき、必要に応じて権限行使を行ってきた。今般、当委員会から指導を受けた富士通 Japan 株式会社とデジタル庁からの報告書について、現時点において一定の改善策が講じられていることが確認できたほか、健康保険証及び障害者手帳に係るマイナンバーの紐付け誤りについても、関係自治体に対する指導を行うことなどにより、マイナンバーカード等に係る一連の事案対応は、現時点において一定の整理を行うことができたものと思う。

今後、それぞれの事案関係者においては、当委員会からの指導等を踏まえて、策定された再発防止策をまずは着実に実行していくなど、国民の信頼と理解を得られるよう、真摯に対応していくことが求められている。また、当委員会としては、事案関係者の取組について引き続き注視していくとともに、計画的な立入検査や研修の実施等により、特定個人情報の適正な取扱いの確保に努めていくこととしたいと考える」旨の発言があった。

原案のとおり、決定することとなった。

なお、本議題については、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非公表とすることとなった。

（２）議題２：いわゆる３年ごと見直し（ヒアリング）

個人情報保護委員会議事運営規程第９条の規定に基づき、欧州ビジネス協会（以下「EBC」という。）のキルヒホフ氏及び中崎氏が会議に出席した。

EBC から、資料に基づき説明があった。

大島委員から「一つ目は、日本や欧州以外でも、米国など、様々な法制度が存在していることを踏まえると、相互運用性のある国際環境の構築を目指すことが重要だと考える。日 EU 間あるいは日英間には相互認証が存在して、お互いの個人情報保護制度の水準が同等であるといって良いと思う。一方、米国などの相互認証のない国においては、個人データの利用及び管理について、事業者はどのような取組を行っているか、お話いただきたい。

二つ目だが、日 EU 間の共同研究時に、学術研究分野の十分性認定が無いことによる課題・問題等があれば、教えていただきたい」旨の発言があった。

これに対し、EBC から「一つ目の御質問についてだが、相互認証が存在しない場合における手続は、基本的に、GDPR において定められている。その場合には、データ保護の水準を同レベルにするために、例えば、標準的契約条項（SCC：Standard Contractual Clauses）という、欧州委員会が決定したデータ移転契約のひな型を使う。第三者に個人データを移転したい場合

には、第三者とその SCC を基にした契約を締結する。SCC の内容は法律で規定されており、変更できないため、第三者は SCC にサインすることにより、GDPR と同等の水準で個人データが保護されるということが確認できる。このように、手続としては簡単である。なお、米国への個人データ移転に関しては、基本的にはほかと同様であるが、欧州からすると心配な点も存在しているため、少しではあるが差異がある」旨の回答があった。

また、EBC から「まず補足だが、欧州を本拠地とし、グループ会社を持っている事業者の場合は、グループ内のデータ取扱いに関する同意を多くの場合は結んでおり、その中において、各社に対してデータ保護の水準が同等となる取扱いとなるようにお願いをしているケースが多いと認識している。

次に、二つ目の御質問についてだが、共同研究を進めていく上で、学術研究分野の十分性認定が無いことにより、若干、支障が出てきているところはあるのではないかと認識している。もちろん、匿名化等の手法を用いることにより今のところは乗り切っていると理解しているが、同意を取り切れないことを理由に、共同研究に支障が出るということはあり得るので、課題だと思っている」旨の回答があった。

小川委員から「最近の日本の大規模な漏えい等事案の例に鑑みると、事業者の安全管理措置について、大きく三つの課題があると思っている。一つ目は、委託先の事業者や派遣職員を含めた安全管理体制の整備、二つ目がシステム設計や運用を含めたヒューマンエラーの防止策、三つ目が不正アクセス対策だと思っている。

日本では、これらの課題を踏まえた漏えい等防止対策が特に重要だと考えているが、欧州では、事業者が漏えい等を防止するために、どのような取組を行っているか教えていただきたい」旨の発言があった。

これに対し、EBC から「把握している限りでも色々な取組があるが、例として、欧州の事業者では、基本的には派遣社員の場合にはデータアクセスが制限される。例えば、勤務先の全部のデータにアクセスできないようなセッティングがされる。また、ほかの例として、多くの人は携帯電話等のデバイスを持っているが、業務に際しては、基本的には自身のデバイスは使用が許されておらず、事業者から支給されたデバイスのみを使用している。その支給されたデバイスには、事業者側がデバイスに記録されているデータを遠隔で消すことができるようなセッティングもされている。

ほかにも色々な例はあると思うが、私自身の経験として、基本的に、欧州の事業者におけるデータの取扱いは、日本の事業者と比べると非常に厳しいと感じている。その理由だが、欧州はデータ保護に関する歴史が長く、ドイツの場合では 30 年ほどの歴史があり、認識が違うと思っている」旨の回

答があった。

また、EBC から「まず、若干の補足だが、アクセスコントロールについて、欧州の場合は本当に意識が高く、また、かなり厳しく監督されている。特に病院関係ではアクセス権の設定に問題があったことを理由に当局から制裁が科されるということが何回か行われている状況である。そういった技術的なコントロールはかなり厳しい。

もう一つ、委託先の管理に関する話としては、サプライチェーンを含めたデータセキュリティについては、かなり慎重に対応していると認識している」旨の回答があった。

中村委員から「EU と海外の状況を踏まえた、ペナルティの強化について質問をさせていただく。令和２年改正のヒアリングの際に、有識者の方々から、『国内企業はレピュテーションリスクを非常に恐れているので指導で違法体制が是正されるという評価もあり得るが、EU 等海外ではすでに事業者に対し課徴金等の金銭的なペナルティが導入されており、海外事業者に対してはいわゆる指導ではなく、課徴金等の金銭的な制裁が有効ではないか』という趣旨の指摘を頂いた。

現実に、EU・GDPR には、制裁金が規定され、１か国で年間２桁から３桁の執行件数があると認識している。こうした EU における状況も踏まえ、海外企業を含む内外の企業に個人情報保護法の遵守を促す観点から、課徴金等が検討されることに対してどのように考えているか」旨の発言があった。

これに対し、EBC から「まず、日本と欧州ではシステムが違う。欧州の場合、日本と同様に行政指導を行うこともあるが、日本よりもその件数は少ないと認識している。欧州では、当局が重大な違反を発見した場合、基本的には直ちに罰金が科される。それが欧州のシステムである。

日本の場合には、基本的な手続の流れが決まっている行政指導が主であるが、私の個人的な意見だが、日本の制度の方が欧州よりも良いと思っている。欧州には、後で罰金を科される可能性があるビジネスを、とりあえず試すという事業者もある。日本の場合は、現在は欧州と比べるとまだ罰金の金額は少額であるが、それでも、日本国内で事業活動を行っている外国企業も含め、法律を守る傾向にある。そのため、行政指導を主とする日本の制度の方が良いと思う。

例えば、コロナ禍において、欧州ではマスクの着用が義務となった。もし、電車内等でマスクを着用しなかった場合に罰金が科されるということになり、欧州の人々は不安になった。しかし、日本ではマスク着用の義務化はされておらず、マスクをするようにお願いをしただけで、約 90%の国民がマスクを着用した。日本はそのような社会であり、とても良いところだと思う。

そのため、日本社会の特徴も踏まえ、直ちに罰金を科すようなことにはならないよう、お願いしたい」旨の回答があった。

浅井委員から「GDPR の『正当な利益』は、各事業者が、個人の権利利益との比較衡量の上、自主的に判断して個人情報を取り扱うものの、その正当性については、最終的に執行当局が判断することになると認識している。

そこで、例えば、生成 AI などの新たな技術を活用して個人情報の処理を行う場合、事業者は何をもって『正当な利益』と判断するのか。また、その判断を自主的に実施する際のリスクや懸念はどのようなものがあるのか。もう一つ加えて、欧州では大半の事業者が法的根拠として『正当な利益』を使用しているとのことだが、それはなぜなのか、教えていただきたい」旨の発言があった。

これに対し、EBC から「まず、事業者が『正当な利益』を使用する理由についてだが、これは、基本的に使いやすいからである。『同意』は、要件が厳しく無効になるリスクがあり、また、個人が同意後に取り消す権利を有していることもあり、基本的に弱い法的根拠である。契約書が存在している場合は、それも個人情報を処理する根拠にもなるが、契約書が存在しない状態で個人情報を処理することも多い。そうした場合における、絶対的に準拠できる根拠を考えると、それは『正当な利益』になる。

次に、新しい技術の活用に関してだが、基本的に、欧州の事業者は最新のテクノロジーの開発前の段階で法律的な根拠について考えている。まず、個人情報については、必要以上に利用しないという考え方が浸透しているため、技術の開発に際しては、個人情報の取得・利用を最小限化するようにしている。その上で、もしビジネスモデル上、個人情報を取得する必要がある場合には、基本的に、開発期間中に、個人情報を取得することに問題がないかどうか等の法律的な根拠について考える。そうすると、例えば事業者がビジネスモデルのための個人情報を利用したいが、オプションが無い場合、『正当な理由』の観点から考えると合理的でないことから、恐らく個人情報の取得が認められないという結論になる。

AI は様々なことに使用することができるが、開発前の段階で、開発側が個人情報処理の法的根拠を考えなくてはいけない」旨の回答があった。

また、EBC から「補足として、今、個人情報の取得・利用を最小限化するという話が出たが、これは、プライバシー・バイ・デザインのところと関係すると考える。また、自主的判断のリスクについてだが、このあたりは各事業者が全面的にリスクを負うことになるため、リスクを最小限にする観点からは、先ほど挙がった話に加え、プロフェッショナルとともに検討する、あるいは社内で検討を行い、後で当局から説明を求められた際に回答する

ことができるように内部での対応をされている。また、「正当な利益」の判断において考慮すべきファクターについては、バランスを取って判断するという非常に一般的な回答になるが、事業分野によっても、多様な変数があるところ、事業者ごとに適切な判断を個別にされていると認識している」旨の回答があった。

藤原委員から「『正当な利益』があるかどうかは、最終的にはデータ保護当局が判断することになることは認識しているが、『正当な利益』に対して、個人情報を収集される側であるドイツ国民側は一般的にどのように考えているのか、情報自己決定権の考え方に基づく反発等はないのか、教えてほしい」旨の発言があった。

これに対し、EBC から「事業者においては『正当な利益』を使用して個人情報の処理を行っているが、確かに、個人情報を収集される国民側においては、自身の個人情報のため、何をするかを決定しなくてはならないという考え方がある」旨の回答があった。

梶田委員から「欧州企業が GDPR を遵守することは当然であると思うが、GDPR の規定を超えて、個人の権利利益を図るような欧州企業間の取組は存在するのかどうか。存在する場合には、どのようなものがあるかを質問させていただく。

また、企業が GDPR の規定を遵守する観点、または、安全管理などにおいて特に遵守を促進する観点から、欧州企業間での連携した取組などは存在するかどうか。存在する場合には、どのようなものか、教えていただきたい」旨の発言があった。

これに対し、EBC から「一つ目の質問に対してだが、例えば、最近では、法令上個人情報を取得する根拠が存在する場合であっても、事業者は使用しない個人情報については、取得したくないと考える。そうした場合、そのように情報の取得を最小限としている事業者が、別の事業者よりも倫理的な感覚を有している、compliant であるというアピールしているケースが存在している」旨の回答があった。

また、EBC から「補足であるが、今は個人情報の取得に関する話であったが、観点としては、セキュリティやレピュテーション等、事業者として考えなくてはいけないリスクをできるだけ抑えるという視点が含まれている。そうした意味で、事業者によって対応レベルに差はあるが、法令よりも厳しい対応をする取組が例として挙げられる」旨の回答があった。

髙村委員から「PIA の実施義務についての質問である。先ほど、プライバシー・バイ・デザインに関する話が上がったが、PIA は個人の権利利益の保護の観点からどの程度効果があるか、実効性があるか、教えていただきたい」

旨の発言があった。

これに対し、EBC から「率直に申し上げると、GDPR が発行された５年ほど前は、多くの事業者は PIA が複雑だと考えており、何を行えばいいのかがわからない状態にあった。

しかし、最近はプライバシー・バイ・デザインでも説明したとおり、新しい製品を販売・開発前の段階で、しっかりと個人情報の取扱いに関する法律的な根拠について考えるという慣習が根付いており、そのような考え方に基づいて製品を開発等することにより PIA が簡単になるということがあり、多くの事業者は PIA をしっかりと実施している」旨の回答があった。

髙村委員から「日本では、マイナンバーを含む個人情報を取り扱う場合を除き、法律上 PIA の実施は義務付けられていない。その点、マイナンバーを含まない個人情報を取り扱う場合であっても、事業者に対して PIA を法律上義務化する必要はあるか、考えを聞かせていただきたい」旨の発言があった。

これに対し、EBC から「欧州では、義務付けされていることは良いと思う。欧州の事業者は義務がないとやらない傾向にある。しかし、日本の場合は、法律上で義務付けられていない場合であっても、ガイドライン等に明示されている場合にはガイドライン通りに対応している傾向にある。そのため、日本においては、法律上で義務付ける必要まではないのはないかと考える」旨の回答があった。

丹野委員長から「他制度はそれぞれの文化や歴史等に基づいて、最善と考えられるものが、各国の法制度として定められているものであると思っている。それが日本であれば APPI、欧州であれば GDPR なのだと理解している。

その上で、日 EU は互いの制度を相互に評価して、それぞれの権利利益の保護のレベルが同水準にあると認めているが、そのような相互認証があっても、APPI と GDPR の差分には課題があるということなのか教えていただきたい。また、併せて、現状の相互認証に対する評価はどのようなものか教えていただきたい」旨の発言があった。

これに対し、EBC から「APPI と GDPR を比較した場合、データ保護の安全性の観点から考えると、ほぼ同レベルであり、また、APPI は基本的には使用しやすく、両方良いスタンダードであると思う。

欧州や日本の事業者の関係者と話をすると、日欧間のビジネスについて考えると、基本的にとてもやりやすくなっているという声を聴く」旨の回答があった。

また、EBC から「補足だが、やはり事実として APPI と GDPR の間に差分は存在しており、EU の事業者からはわかりにくいという声も挙がっている。

ただし、こうした声を課題としてどれほど評価すべき点については、データ保護の安全性のレベルはほぼ同レベルであるということが前提であるため、使い勝手の面からのお話もあるのではないかと思っている」旨の回答があった。

丹野委員長から「さきほど頂いた御意見も含め、個人情報保護を巡る様々な状況について、各方面の意見を聴きながら、課題を整理、審議してまいりたい」旨の発言があった。

（３）議題３：民間企業における個人データの越境移転、海外法規制対応に関する実態調査　調査結果報告書（案）について

事務局から、資料に基づき説明を行った。

藤原委員から「今般の調査は、当委員会の国際戦略に基づいて、国際動向の把握と情報発信に取り組むに当たり、企業ニーズを把握するために実施されたものであるが、その前提となる民間企業の実務の現状も把握することができ、委員会の政策立案の観点から有意義な結果が得られた。

委員会として、このような形での調査は初めてであるが、このような調査は継続的に実施してこそ意味を成すもの。まずは、今般の調査結果を、当委員会の施策や国際戦略の参考とするべきだが、調査の継続的な実施が必要である」旨の発言があった。

大島委員から「今回の調査を通して、相互認証には対象範囲や対象国の拡大、Global CBPR のような企業認証システムには参加国・参加地域や参加企業の拡大、企業間契約には SCC 等のような定型化の推進等、越境移転ツールごとに様々な要望があることが明らかになった。

また、相互認証が利用可能な場合、よく利用されており、企業にも利益があるとされているが、企業間契約を行う企業もあるとの調査結果もあった。

このような状況は、企業のニーズが多種多様であることを示している。したがって、様々な越境移転ツールのオプションが利用可能な環境を整備しておくことが必要であり、今後とも、様々な国際的な枠組みを通して、各ツールを総合的に開発していくことが大事である。既存のツールを基とした、グローバル規模のツールの開発を目指していくのが適当である」旨の発言があった。

丹野委員長から「まずは、アンケート調査に協力いただいた民間企業の皆様に、改めてお礼を申し上げたい。大変価値のある調査結果を得ることができた。

本調査の目的は、様々な業種・規模の民間企業において、どのような個人情報の越境移転を実施しているのか、越境移転規制を含む海外個人情報保

護法制への対応にどのような課題があるかといった情報を収集し、今後の当委員会での政策検討の材料とすることであった。調査結果は、今後の政策立案の参考として大いに活用したい。

　このような調査は、継続することが大切である。今後も定期的に、継続的に実施したい」旨の発言があった。

　原案のとおり決定することとなった。

（４）議題４：監視・監督について

　※内容について非公表

以上