日　時：令和５年 12 月６日（水）14：00～
場　所：個人情報保護委員会　委員会室
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

○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、加藤委員が御欠席です。
以後の委員会会議の進行につきましては、丹野委員長にお願いいたします。
○丹野委員長　それでは、ただいまから、第263回個人情報保護委員会を開会いたします。
本日の議題は四つございます。
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　議題１について、資料１－１に沿って説明させていただきます。
コンビニエンスストアでの住民票等の誤交付、公金受取口座の誤登録、健康保険証及び障害者手帳等の各種サービスにおけるマイナンバーの紐付け誤り等の一連の事案について、詳細な事実関係を把握するとともに、確認された問題点に応じて、指導等の権限行使の要否を検討し、適時に対応を行ってきましたが、それぞれの事案に対する対応の概要を説明させていただきます。
まず、コンビニエンスストアでの住民票等誤交付についてです。これまでの経緯は（１）及び（２）に記載させていただいております。
次に、富士通Japanから10月31日に提出された報告書について、詳細を別紙１で説明させていただきます。
一つ目の指導事項、「１．技術的安全管理措置」に関しては、富士通Japanは、令和５年６月17日までにトラブルの点検を実施済みでありまして、令和６年１月を目処に、コンビニ交付サービス内において、申請から証明書出力までの一貫性を保証するための、取り違えを防止する機能といった異常検出機能を開発予定です。
二つ目の指導事項、「２．組織的安全管理措置」に関しては、令和５年６月より、富士通グループの最高品質責任者（CQO）を設置し、月に１回、リスクコンプライアンス委員会を開催するといった、品質保証に関するマネジメント体制を強化しております。さらに、令和５年10月より、CQO直轄組織が専門的視点から監査を行う第三者評価の仕組みを導入し、運用を開始しております。また、地方公共団体を含む委託元への情報提供の改善策として、障害等に関する情報提供を全社一元的に管理するため、令和５年度中に、運用基盤（情報提供Web）を新設し、適切に委託元へ情報提供する仕組みを構築する予定としており

ます。

以上より、今回、富士通Japanから報告を受けた改善策の実施状況に関して、現時点において一定の取組が認められるものであり、当委員会としては、今後も改善策が確実に実施されることを引き続き注視していきたいと考えております。

資料１－１に戻ります。

次に、別人のマイナンバーと銀行口座情報を紐付けた、公金受取口座の誤登録事案ですが、（１）の後半部分、従来、漏えい等の人数については940人とされておりましたが、デジタル庁における誤登録の検知モデル開発の過程で、新たに誤登録の可能性がある227人分の公金受取口座が確認されました。それに対して、増加した2277人分の誤登録の原因は、従前の誤登録と同じであるため、追加して問題点を指摘する必要はないと判断しておりますが、デジタル庁から提出された10月31日付の報告書について、詳細を別紙２で説明させていただきます。

一つ目の指導事項、「１．本人確認の措置」に関しては、デジタル庁は地方公共団体における支援窓口でのログアウト忘れ防止対策の不十分性を振り返り、システム面での対応に加え、令和５年11月２日、地方公共団体に対して事務連絡を発出し、運用面での対策を行っております。

二つ目の指導事項、「２．保有個人情報の漏えい等発生時における報告体制」に関しては、従前は２名で個人情報保護担当を担っていましたが、専門的知識を保有する職員を登用し、９名と体制強化しており、総括保護管理者等の責任者への報告に関して、個人情報管理規程を見直しました。また、リスク事案ホットラインと称したメーリングリストの整備により、庁内報告体制を整備し、庁内へ周知しております。さらに、教育研修、幹部層における働きかけといった取組も行っております。

三つ目の指導事項、「３．取扱手順の見直し」に関しては、令和５年５月23日と11月２日にデジタル庁から市区町村向けに事務連絡を発出するなど、情報共有を行いまして、支援窓口の利用者へのログアウトの徹底を要請しております。

四つ目の指導事項、「４．個人情報保護委員会に対する漏えい等の報告」に関しては、規程等の見直しとして、個人情報保護担当対策チームより速やかに当委員会へ報告する旨を具体的に明記したフローチャートと情報セキュリティインシデント手順書を作成しまして、デジタル庁内の周知、教育研修といった取組を行っております。

五つ目の指導事項、「特定個人情報保護評価」に関しては、環境変化に応じて特定個人情報保護評価書の見直しを行うことへの意識が十分ではなかったことを踏まえまして、環境変化やリスク事案等が発生した場合には、担当部署だけでなく、個人情報保護担当対策チームも加わって評価書の見直しに係る検討を行うこととし、さらに、環境変化やリスク事案等の発生有無にかかわらず、１年に１回、評価書の記載事項を実態に照らして見直し、又は変更が必要か否かを検証することとし、その旨を明文化した文書を令和５年12月までに発出を予定しております。

その他の取組といたしましても、従前、デジタル庁では情報セキュリティ監査等は行っておりましたが、保有個人情報の取扱いに関する監査を実施していなかったため、監査実施のための体制を整備しました。また、従前、セキュリティインシデント発生時の有事の際にログ確認を行うこととしておりましたが、保有個人情報を多く保有・保管するシステムについては、定期的にログ分析を行うこととするといった取組が行われています。

以上より、今回、デジタル庁から報告を受けた改善策の実施状況に関しまして、現時点において一定の取組が認められるものであり、当委員会としては今後の改善策が確実に実施されることを引き続き注視していきたいと考えます。

次に、健康保険証及び障害者手帳等の各種サービスにおけるマイナンバーの紐付け誤り事案ですが、詳細について、資料１－２に沿って説明させていただきます。

本件は、個人番号利用事務等実施者である健康保険組合や地方公共団体が保有する個人情報と個人番号との紐付けを行う際に、誤って別人の個人番号を紐付けたことにより、マイナポータル等のシステムを通し、本人の情報が第三者に閲覧された、又は閲覧され得る状態にあったという事案でございます。

個人情報保護法上の報告義務の対象となる事態のうち、本件で問題となり得る事態としては、①から③として記載しております、個人情報の保護に関する法律施行規則第７条第１号及び第43条第１号に係る要配慮個人情報の漏えい等、また、同規則第７条第４号に係る民間で1,000人、同規則第43条第４号に係る行政機関等で100人以上の漏えい等が発生した場合となります。

今回、保険者及び地方公共団体からは、健康保険証情報又は障害手帳情報について、①又は③の事態が発生したとして、当委員会へ漏えい等報告が提出されております。

これらの漏えい等報告につきまして、その内容を精査するとともに、関係者へのヒアリング等を実施し、事実関係や問題点の分析を行っております。

まず、事実関係について、「第２　事実関係」のとおり整理しております。

健康保険証情報と個人番号との紐付けに関しては、保険者が被保険者から直接又は勤務先である事業主を通して個人番号の提供を受け、登録処理を行うこととなっております。ただし、被保険者から個人番号の提供がない場合は、保険者が住民基本台帳ネットワークを通して氏名等により照会を行い、被保険者の個人番号を取得することが認められております。

２ページ目を御覧ください。

今回報告された事案のうち、健康保険者情報の紐付け誤りの発生原因としましては、次の（１）から（３）に記載しておりますとおり、三つが報告されております。

次に、障害者手帳情報の紐付け誤り事案の事実関係についてです。障害者手帳情報と個人番号との紐付けにつきましても、健康保険証情報と同様に、手帳の交付主体である地方公共団体、主に都道府県、政令市、中核市等が、手帳交付対象者から直接又は窓口となる他の地方公共団体、特に管内市町村を通して個人番号の提供を受け、登録処理を行うこと

となっております。また、こちらでも本人から個人番号の提供がない場合は、住基ネット照会等により個人番号を取得することが認められております。

今回報告された紐付け誤りの発生原因としましては、次の（１）から（４）に記載しておりますとおり、四つが報告されております。（１）から（３）に関しましては、健康保険証の事例と同様です。健康保険証と異なる点としましては、（４）、手帳番号の重複が複数の地方公共団体から報告されております。これは、障害者手帳の手帳番号をシステム上で個人番号と紐付ける処理に使用していた地方公共団体において、一意であるべき手帳番号が実際には一部重複していたということで、交付対象者の情報が同じ手帳番号に紐付いた別人の手帳情報として登録されたというケースでございます。

続いて、法律上の問題点についてです。

まず、健康保険証につきまして、前提となる法律上の整理は、（１）のアからウに記載しているとおりです。この整理上において、保険者が番号法に定める本人確認義務を負うのは、本人から直接個人番号を取得した場合又は保険者が住基ネット照会等により個人番号を取得した場合となります。

次に、資料４ページ、（２）の法律上の問題点についてですが、本件では大きく２点の問題があったと捉えております。一つは、番号法上の本人確認措置の不備、もう一つは、番号法及び個人情報保護法上の安全管理措置の不備です。

本人確認措置につきましては、住基ネット照会等により被保険者の個人番号を直接取得する際の本人確認は保険者が行う義務がございます。この点につきまして、厚生労働省より、住基ネット照会を行う際は、４情報、氏名、生年月日、性別、住所による照会を行い、４情報が一致しない場合は、個人番号を取得せず本人への確認を行うよう通知がされておりました。しかしながら、一部の保険者においては、実務上、氏名と生年月日と性別で検索するといったような通知に従っていない運用が見られ、また、結果の照合も十分に行われないままに別人の個人番号を取得しているというケースが報告されております。この点につきましては、番号法第16条が求める本人確認措置として不備があったものと認められます。

次に、資料５ページにかけて記載しておりますが、番号法及び個人情報保護法上の安全管理措置の不備について検討を行いました。番号法及び個人情報保護法、また、ガイドラインでは、保険者に対し、規律に従った運用や取扱状況の把握等を安全管理のための措置としてとることを求めております。しかしながら、住基ネット照会を行う等の手順につきましては、先ほど申し上げたとおり、厚労省から手順が通知されていたにもかかわらず、実態としてそれに沿った運用がされていない、別人の個人番号を誤って取得したという保険者がございました。これらの保険者におきましては、番号法及び個人情報保護法が求める安全管理のために必要かつ適切な措置に不備があったものと認められます。

次に、資料５ページから６ページにかけ、障害者手帳情報についても同様に法律上の整理を行っております。

こちらにつきましても、当該地方公共団体が番号法に定める個人番号を取得する際の本人確認義務を負うのは、本人から直接個人番号を取得した場合又は住基ネット照会等により個人番号を取得した場合となります。

（２）でも同様に法律上の問題点の検討を行いました。

内容につきましては、資料６ページから８ページにかけて記載しているとおりです。問題点につきましては、保険証情報と同じく、一つは、番号法上の本人確認措置の不備、もう一つは、番号法及び個人情報保護法上の安全管理措置の不備です。健康保険証情報の事例と異なる点としましては、資料８ページの（ウ）の部分でございます。

一部の地方公共団体においては、本人確認自体は適切に実施されていたものの、情報連携の作業手順やシステムの設計等において事前に十分な確認がされておらず、結果として多数の紐付け誤りが発生したというケースがございました。

また、担当者一人が紐付け事務を行う等、ヒューマンエラーがあった場合、事後的に検知をする、防止するという体制を取られていないという団体も複数報告されております。

これらの地方公共団体においては､特定個人情報及び保有個人情報の安全管理のために、必要かつ適切な措置に特に不備があったものと考えております。

健康保険証情報及び障害者手帳情報について、問題点の分析と再発防止策として報告された内容を、資料８ページから９ページ、「第４　再発防止策」に記載しております。

健康保険証情報については、個人番号取得時の手順の誤りと、紐付け後の事後的な点検が十分に行われていなかったことが、要配慮個人情報の漏えいまたは漏えいのおそれが発生した原因と分析しております。

これに対応する再発防止策が、（２）の部分でございます。

当委員会においても、これらの再発防止策が適切に実行されるかどうかについて、保険者及び関係機関の状況を注視してまいりたいと考えております。

次に、資料10ページを御覧ください。

障害者手帳情報についても同様に、問題点の分析と再発防止策として報告された内容を記載しております。問題点については保険証とおおむね同様ですが、多数の紐付け誤りが発生した原因として、手帳情報と個人番号との紐付け作業を行うに当たって、事前の検証や検知するための仕組み、体制の整備といった点について適切に行われなかったことが問題であると分析しております。こちらについても、対応する再発防止策を（２）に記載しております｡当委員会においても､こちらの状況も注視してまいりたいと考えております。

次に、11ページを御覧ください。

最後に、本事案に対する対応を記載しております。

まず、健康保険証情報の紐付け誤り事案につきましては、先ほど申し上げたとおり、個人番号取得時における本人確認等の不備が認められたものの、本年11月末時点で当委員会に報告を提出している11の保険者においては、いずれも要配慮個人情報が閲覧された、又は閲覧されたおそれがあるという点に関しては、本人の数はいずれも１人又は２人で報告

されております。また、その発生原因につきましても、その多くは個人番号取得時や入力時の手順の誤り、ヒューマンエラー等に起因するものでございました。こうした点については、制度全体を通して、点検や予防のための措置がとられておりまして、一定の再発防止策が講じられたものと考えております。こうした状況を踏まえ、保険者につきましては、今回、番号法及び個人情報保護法に基づく指導を行わないこととしたいと考えております。

次に、障害者手帳情報の紐付け誤り事案についてです。こちらに関しても、健康保険証情報と同様に、個人番号取得時における本人確認不足等の問題点はあったものの、11月末時点で報告を提出している21の地方公共団体において、発生原因の多くは、同様にヒューマンエラー等に起因するものが大半を占めておりました。この点につきましては、デジタル庁におきまして、紐付け処理のための横断的なガイドラインが設定され、それに沿った運用を行うといったことを地方公共団体も再発防止策として挙げてきております。

こうした取組に関しては、一定の措置がとられているものと認められますが、一方、先ほど申し上げたように、一部の地方公共団体においては、多数の紐付け誤りが発生した事例が報告されております。これらについては、ヒューマンエラーだけで発生したものとは言えず、個人番号及び保有個人情報の必要かつ適切な取扱いが組織的に確保されていなかった、個人の権利利益を害するおそれが特に大きいものであると考えております。したがって、特に漏えい等に係る本人の数が多数であり、組織的安全管理措置に不備が認められた地方公共団体に対しては、今回、番号法及び個人情報保護法に基づく指導を行いたいと考えております。指導対象及び指導内容につきましては、資料12ページに記載しております。

それでは、資料１－１に戻ります。最後に、その他といたしまして、マイナンバーカード等に係る各種事案のうち、マイナポイントの誤交付事案については、誤交付に伴いまして、マイナポイントアプリ上の決済サービスIDが第三者に閲覧される事象が発生しましたが、決済サービスIDは、マイナポイントに関するデータを保管するデジタル庁においても特定の個人を識別できない情報であり、保有個人情報の漏えいには該当しないことが確認されました。

また、健康保険証及び障害者手帳以外の各種サービスにおけるマイナンバーの紐付け誤り事案のうち、年金情報の紐付け誤り事案については、個人情報保護法及び番号法上の漏えい等報告の義務の対象となる事態は確認されませんでした。

このほか、マイナンバー情報総点検本部における個別データ点検の中では、これ以外の事務においても、マイナンバーの紐付け誤り事案が確認されておりますが、いずれも個人情報保護法及び番号法上の漏えい等報告義務の対象となる事態は確認されておりません。

最後に、本議題については、事案の重要性と社会的影響の大きさに鑑みまして、資料１－１、別紙１、別紙２並びに健康保険証及び障害者手帳情報に関する紐付け誤り事案に関する説明であります資料１－２の範囲で公表することとしたいと事務局としては考えております。

説明は以上です。
○丹野委員長　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。
中村委員、お願いいたします。
○中村委員　マイナンバーカード等に関わる各種事案に対する個人情報保護委員会の今後の対応についてコメントを述べます。
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います。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います。
以上です。
○丹野委員長　ありがとうございます。
ほかにどなたか御質問は。
高村委員、お願いいたします。
○高村委員　健康保険証情報及び障害者手帳情報についての再発防止策について、一言申し上げます。
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ます。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ます。
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ます。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ます。
以上です。
○丹野委員長　ありがとうございました。
ほかにどなたか御質問、御意見等はございますでしょうか。
よろしいでしょうか。
それでは、私からも一言申し上げます。
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まして、何よりも国民の信頼を得ることが重要であります。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ました。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ましたほか、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います。

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おります。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ます。

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。

御意見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いたします。

それでは、次の議題に移ります。

議題２「いわゆる３年ごと見直し（ヒアリング）」について、前回に引き続き、本日は、欧州ビジネス協会（EBC）へのヒアリングを実施したいと思います。

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、欧州ビジネス協会の方に会議に出席いただきたいと思いますが、よろしいでしょうか。

（異議なし）

○丹野委員長　それでは、出席を認めます。

（欧州ビジネス協会入室）

○丹野委員長　本日は欧州ビジネス協会のキルヒホフ様並びに中崎様に御出席いただいております。それでは、早速ですが、御説明をお願いいたします。

○EBC　こんにちは、キルヒホフと申します。どうぞよろしくお願いいたします。

我々の協会は、基本的に、日本でビジネスをされている欧州の事業者と欧州でビジネスをされている日本の事業者をサポートしています。そのサポートの中には、データ保護に関すること、例えば一般データ保護規則（GDPR）と日本における個人情報の保護に関する法律（APPI）に関するサポートも含まれています。本日は、我々のその経験を基にお話していきたいと思います。

APPIとGDPRの適用を受ける事業者と話した際に、いろいろな心配点があるとよく言われます。今日はその心配点について、三つお話しさせていただきたいと思います。

その三つの心配点とは、一つ目は、GDPRとAPPIの定義についてです。二つ目は、個人情報の処理/取扱いの法的な根拠についてです。三つ目は、欧州におけるAPPIの域外適用になります。その三点について、もう少し詳しく説明します。

まず、一つ目のGDPRとAPPIの定義についてです。GDPRとAPPIは、両方ともデータ保護法、法律になりますけれども、異なる定義が使用されています。例えば、GDPRの場合には「個人データ」と規定されていますが、APPIの場合には「個人情報」と規定されています。また、ほかの例として、GDPRの場合には「処理」と規定されていますが、APPIの場合には「取扱い」と規定されています。

このような定義の違いは、弁護士や専門家には分かるかもしれません。しかし、事業者の方と話をすると、その違いが分からないという声が多いのです。そうすると、法律の使い方が難しくなります。事業者側の希望としては、異なる定義による曖昧さは可能な範囲で回避したいのです。

次に、二つ目の心配点である、個人情報の処理/取扱いの法的な根拠についてです。

GDPRでは、基本的に、個人情報を使うために法律的な根拠が要求されています。例えば、「同意」も根拠の一つになります。ほかには、契約書の履行のため、法的な義務の遵守のための必要性、「正当な利益」の目的の処理の必要性があるときなどです。欧州では、第三者への移転も含めて、個人情報を処理する法的な根拠として、GDPRの「正当な利益」を一番使用します。

APPIの場合には、個人情報を取得するときに、個人に利用目的をしっかりと説明したら、基本的に個人情報を使うことができます。しかし、GDPRは違います。GDPRの場合には、利用目的をしっかりと説明しても、根拠がないと個人情報を使えません。大きく違うところはその部分だと思います。

そうすると、一つは、欧州の事業者の方と話すと、APPIは使いやすいのですけれども、基本的に個人情報を取得することはGDPRより簡単になるので、もし、事業者が欧州から日本に来た場合、普通のGDPRの考え方が前提にあるので、個人情報を第三者へ移転したい場合には利用目的が足りないという声があります。その上、基本的に「同意」が必要になりますので、その「同意」をもらうために、企業側から見たらいろいろと管理コストが増大することになります。

もう一つは、なぜ欧州では「正当な利益」が一番よく使用されるかの考え方についてです。欧州の場合には、consent、「同意」はあまり使いません。なぜなら、法律的に有効なconsentを得ることは難しいからです。consentを得るために、いろいろな条件があります。

例としてよく挙げられるのが、インターネットです。例えばオンラインショッピングをする場合、事業者が、このウェブサイトを使いたい場合には、ちゃんと同意してください、我々もあなたの個人情報を使いたいので、もし同意をもらえないと、このウェブサイトは

使えませんと言う場合です。これは、バンドリングというよくあるパターンです。しかし、欧州の場合、基本的に、consentはあまり強い法的な根拠にはなりません。そのため、基本的に、「同意」ではなく別の根拠を使います。

欧州の事業者がよく言うのは、基本的に、日本ではAPPIによる「同意」だけがあるので、もし、個人情報を移転したい場合には、例えば、事業者のグループ間で、日本の事業者から欧州の本社まで移転したい場合には、基本的に「同意」を基にします。実はほかにも、例えば共同利用等の方法もあるのですが、共同利用は、GDPRから見たら、正しく理解していない事業者が多く、どうやってセットアップすればよいのかが分からないので、後になるのです。GDPRから見たら、基本的に法的な根拠があっても、日本のAPPIの場合には、それでは足りないのです。その上に何か必要になりますので、基本的に管理が増えてきます。だから、欧州の事業者は、できれば「同意」だけではなくて、別の根拠、できれば「正当な利益」を使いたいということです。

最後に、三つ目の心配点、欧州におけるAPPIの域外適用についてです。

一つは、皆さん御存じのとおりですが、もし、欧州にある事業者が、日本にいる個人からサービス提供、販売のため個人情報を取得した場合、基本的に欧州の事業者であってもAPPIが適用されます。外国にある事業者にも適用されること自体はGDPRと同じですので、別に問題ないと思います。GDPRは、日本の事業者が、欧州にいる人たちから個人情報を取得した場合GDPRが適用されていますので、それは全く同じですけれども、欧州の立場から見たら、基本的によく言われているのは、GDPRとAPPIを比べると、GDPRのほうが厳しいということです。

なぜかというと、先ほど説明したのですけれども、最初から個人情報を使いたい場合には、法的な根拠が必要になります。利用目的の明示だけでは足りないのです。そうすると、皆、もっと厳しくしてほしいと思っているのです。

もう一つは、例えば、GDPRではいろいろ規定されているのですけれども、データ侵害が72時間以内に通知しなければいけないなど、多くの規制が厳格です。そうすると、そのような厳しいGDPRがある中、その上にAPPIを使わなければいけないということになったら、欧州の人々はあまり理解ができません。基本的に両方適用されていますので、二つの法律ではなくて、もっと厳しい法律のGDPRだけで十分ではないかと思っています。

私からは以上です。

○EBC　若干補足をさせていただきます。

先ほどの法的根拠のところ、「同意」が弱いということを申し上げたのですけれども、その辺り、御案内のとおり、実際、欧州の事業者が同意を取った、「同意」に基づいていろいろされた後で、実際に欧州のデータ保護当局から、あなたのところの「同意」は無効であると、度々御指摘を受けています。そういうことで、欧州の事業者としては、やはり「同意」に頼るのは非常に厳しいという御判断があるということだけ補足させていただければと思います。

以上です。
○丹野委員長　ありがとうございました。
それでは、ただいまのEBCの方々からの御説明について、御質問等をお願いしたいと思います。
大島委員、お願いします。
○大島委員　本日はお越しいただきまして、ありがとうございます。今、御説明をお伺いしたところでありますけれども、私から２点質問をさせていただきます。
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ますと、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ます。日EU間あるいは日英間には相互認証が存在しており、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います。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、お話しいただきたいと思います。
二つ目は、日EU間の共同研究時に、学術研究分野の十分性認定がないことによる課題・問題等があれば、教えていただきたいと思います。
以上であります。
○丹野委員長　お返事をお願いいたします。
○EBC　一つ目の御質問についてですが、相互認証が存在しない場合の手続は、基本的に、GDPRで定められています。その場合、データ保護の水準を同レベルにするために、例えば、日本語でいうと標準的契約条項、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います。第三者に個人データを移転したい場合については、第三者とそのSCCを基にした契約を締結します。SCCの内容は法律で規定されていて、変更できないので、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ます。このように、プラクティスとしては簡単です。なお、米国への個人データ移転に関しては、基本的には他と同様でありますが、欧州からすると心配な点も存在しているため、少しですが差異があります。
○EBC　まず補足ですが、欧州を本拠地としているグループ会社を持っておられる事業者の場合は、インターナルな、グループ内のデータ取扱いに関する「同意」を多くの場合結んでおりまして、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になるようにお願いをしているケースが多いと認識しております。
次に、二つ目の御質問についてですが、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ないことにより、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ます。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ますが、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、課題だと思っております。
以上です。

○丹野委員長　よろしいですか。
○大島委員　はい。ありがとうございます。
○丹野委員長　それでは、ほかの委員から御質問等をお願いしたいと思います。
　小川委員、お願いします。
○小川委員　御意見、ありがとうございます。
　御提案の内容から少し離れるのですが、一つだけ質問させてください。
　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おります。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おります。
　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ますが、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です。よろしくお願いします。
○丹野委員長　お願いします。
○EBC　私が把握している限りでも、いろいろな取組があると思いますが、例としては、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ます。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ます。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ますけれども、業務に際しましては、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ます。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ます。
　他にも色々な例はあると思うのですが、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ます。その理由ですが、欧州はデータ保護に関する歴史が長く、ドイツの場合は30年ほどの歴史があり、認識が違うと思っています。
○EBC　まず、若干の補足ですが、アクセスコントロールについて、欧州の場合は本当にその辺りの意識が高く、また、かなり厳しく監督されています。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す。そういった技術的なコントロールはかなり厳しいです。
　もう一つ、委託先の管理に関する話としましては、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ます。
　以上です。
○小川委員　ありがとうございました。
○丹野委員長　ほかにどなたか御質問はございますでしょうか。
　中村委員、お願いします。
○中村委員　大変示唆に富むプレゼンテーションをありがとうございました。

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きます。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きました。

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ます。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お考えになりますか。

○丹野委員長　よろしくお願いします。

○EBC　まず、日本と欧州ではシステムが違います。欧州の場合、日本と同じ様に行政指導を行うこともあるのですが、日本よりもその件数は少ないと認識しています。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ます。それが欧州のシステムです。

日本の場合には、手続の流れが決まっている行政指導が主でありますが、私の個人的な意見としては、日本の制度の方が欧州よりも良いと思っています。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ります。日本の場合は、現在は欧州と比べるとまだ罰金の金額は高くありませんが、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ります。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います。

例えば、皆様御存じだと思いますけれども、コロナ禍に、欧州ではマスクの着用が義務となりました。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って、欧州の人々は不安になったのです。しかし、日本ではマスク着用は義務化されていなくて、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ました。日本はそのような社会であり、とても良いところだと思います。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、お願いしたいと思います。

○中村委員　ありがとうございました。

○丹野委員長　ありがとうございました。

ほかにどなたか。浅井委員。

○浅井委員　浅井でございます。御説明、どうもありがとうございました。

私から「正当な利益」について、御質問させていただきます。

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おります。

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ですが、それはなぜなのか、教えていただきたいと思います。

○丹野委員長　お願いします。

○EBC　まず、事業者が「正当な利益」を使用する理由についてから説明します。これは、基本的に使いやすいからです。「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ります。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のですが、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です。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」になります。

次に、新しい技術の活用に関してですが、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ます。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ので、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ます。その上で、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ます。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使用したいが、オプションが無い場合、「正当な利益」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ります。

AIは様々なことに使用することができますが、開発前の段階で、開発者側が個人情報処理の法的根拠を考えなくてはいけません。

○EBC　若干補足させていただきますと、今、個人情報の取得・利用を最小限化するという話が出ましたが、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ます。また、自主的判断のリスクについてですが、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りますので、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対応をされています。また、判断ファクターについては、もちろん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りますが、多様な変数があるため、恐らく事業者によって対応が変わってくると思います。

私からは以上です。

○浅井委員　どうもありがとうございました。

○丹野委員長　ありがとうございました。ほかにございますでしょうか。

藤原委員、お願いします。

○藤原委員　時間が押していると思うので、非常に単純な問題を。

「正当な利益」というのは、大変興味のある考え方だとは思うのですけれども、ドイツの方であれば、「レヒト　アウフ　ゼルプストベシュテミング」という考え方との関係はどうなるのでしょうか。そちらを優先すると。EUはそういう考え方を取っていないと思っているのでしょうか。以上、質問はそれだけです。ドイツなら「同意」ではないのですか。

○EBC　ドイツの場合は「同意」ではないです。

もちろん、一つのオプションですけれども、一般的に企業は「同意」は使いません。

○藤原委員　企業は使わないけれども、国民の側が、自己決定権の立場から反論するのではないのかというのが私の質問です。

○EBC　個人について考えたら、もちろん、ビジネスだと「正当な利益」になると思います。

○藤原委員　情報収集される側の国民の側に立つと、ドイツであれば、やはり、「インフォマチオネル　ゼルプストベシュテミング」が出てくるのではないのですか。

○EBC　そうです。そのとおりだったと思います。

考え方は、自分の個人情報ですので、自分で何をするか決めなければいけません。

○藤原委員　であるとすると、「正当な利益」といっても事業者の「正当な利益」だけでは決められませんね。

もちろん、最終的にはデータ保護当局が決めるということは分かっておりますけれども、導入するというのは非常に興味のある御指摘でしたので、ちょっと伺いました。

○丹野委員長　よろしいですか。

お答えはよろしいですか。

○藤原委員　はい。

○丹野委員長　ほかにございますでしょうか。

梶田委員、お願いします。

○梶田委員　御提案、ありがとうございました。

欧州企業がGDPRを遵守することは当然であると思いますが、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きたいと思います。

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と思います。

以上です。

○丹野委員長　お願いいたします。

○EBC　一つ目の質問に対してですが、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ます。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をしているケースが存在しています。

○EBC　補足でありますが、今は個人情報の取得に関する話でありましたが、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ます。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ます。
○丹野委員長　よろしいですか。
○梶田委員　はい。ありがとうございました。
○丹野委員長　ほかにございますでしょうか。
　髙村委員、お願いします。
○髙村委員　貴重な御意見、ありがとうございました。
　PIAの実施義務について質問があります。先ほど、プライバシー・バイ・デザインに関する話がありましたが、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と思います。
○EBC　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でした。
　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ですが、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り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まして、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ます。
○髙村委員　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いて、法律上PIAの実施は義務付けられていません。その点につきまして、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です。
○EBC　欧州では、基本的に、義務付けされることは良いと思います。欧州の事業者は義務がないとやらない傾向にあります。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ります。ですから、日本においては、法律上で義務付ける必要があるかどうかは微妙で、義務までは不要ではないかと考えます。
○髙村委員　どうもありがとうございました。
○丹野委員長　ありがとうございました。
　ほかに皆さん、追加の質問等はございませんか。
　よろしいですか。
　それでは、せっかくの機会ですから、私も一つお聞きしたいと思います。
　法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ます。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ます。

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ますが、こ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です。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と思います。

○EBC　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ますと、ほぼ同レベルであって、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います。

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聞きます。

○EBC　やはり事実としてAPPIとGDPRの間に差分は存在しておりまして、EUの事業者からはわかりにくいという声も挙がっています。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、そこについては、使い勝手の面からの話であると思っています。

○丹野委員長　ありがとうございます。

それでは、皆さん、追加の質問はないでしょうか。せっかくの機会ですので。

では、お二方とも、御説明、ありがとうございます。

さきほど頂いた御意見も含めまして、個人情報保護をめぐ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と思います。

EBCのキルヒホフ様、中崎様、本日は誠にありがとうございます。御退室いただけますか。

（欧州ビジネス協会退室）

○丹野委員長　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いたします。

それでは、次の議題に移ります。

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」、事務局から説明をお願いいたします。

○事務局　まず、資料の構成について御説明します。

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の調査結果報告書（案）の概要として、資料３－１を作成しています。そして、報告書（案）の本体として、資料３－２を作成しています。御説明は、資料３－１の概要資料（案）に基づいて行います。

「1. アンケート調査の目的と概要」を御覧ください。アンケート調査の目的等について記載しています。

「○背景と目的」を御覧ください。当委員会は、個人情報が安全・円滑に越境移転できる国際環境の構築を目指す観点から、事業者側のニーズを把握した上で、ビジネスの様態

や規模に応じて、複数の選択肢から利用しやすい越境移転のスキームを選ぶことができるような環境構築を図ることとしています。そして、様々な業種・規模の民間企業から、どのような個人情報の越境移転が実施されているか、越境移転規制を含む海外個人情報保護法制への対応に当たり、どのような課題があるのか等の情報を収集し、今後の委員会での政策検討の材料とすることを目的にアンケート調査を実施しました。

「〇概要」を御覧ください。アンケート調査期間は昨年11月から12月まで、業種分類は製造業をはじめとした10業種、調査対象企業は経団連（経済団体連合会）加盟企業58社、新経連（新経済連盟）加盟企業８社でした。

「1. アンケート調査の目的と概要」に続き、アンケート調査について、「2. 回答企業情報」、「3. 選択式設問の回答結果」、「4. 記述式設問の回答結果」、「5. 業種別回答状況」に分けて報告しています。

「6. 調査結果を踏まえた当委員会の施策への示唆」を御覧ください。各回答を踏まえた調査結果をもってまとめ、調査結果全体及びアンケート設問分類ごとのサマリ並びに調査結果を踏まえた今後の国際戦略など委員会の施策への示唆を取りまとめています。また、各回答企業から自由記述で寄せられた委員会に対する要望及び意見を掲載しています。

「〇調査結果全体サマリ」を御覧ください。調査結果全体サマリについては、五つの観点で整理しています。

１点目として、個人データの移転の実施状況について、多くの企業が日本から海外、海外から日本への移転をしており、地域別には、アジア全域・オセアニアを指すAPAC地域、北米・メキシコを指すNORAM地域、ヨーロッパ・中東・アフリカを指すEMEA地域との相互移転が横並びで多く確認されました。また、EUとの間の移転について、多くの企業が十分性認定を根拠とする一方で、相手先企業からの求めや認定が取り消されるリスク等への備えのため、標準的契約条項、いわゆるSCCを根拠として併用する企業が多く見られました。

２点目として、越境移転対象の個人データについて、要配慮個人情報、個人関連情報、匿名加工情報を対象とする企業が、限定的ではありますが存在しました。

３点目として、DFFT等の認知状況について、DFFT、Global CBPRともに過半数の企業が認知しており、それぞれへの期待感として、DFFTには越境移転をより円滑に実施できるようになる仕組みの整備、CBPRにはEUを含む多くの国や地域の枠組みへの参画等が挙げられました。

４点目として、ガバメントアクセスの課題として、対応すべき事項の内容、規制動向が不明確であるため、一企業のみでは対応が困難であること、データローカライゼーションの課題として、規制対応のために当該国内にデータ保管用のサーバを確保することに伴うITコストの上昇への懸念が挙げられました。

５点目として、ガバナンス体制の整備について、社内規定等の整備、弁護士等の外部有識者の活用は行われているものの、データ保護影響評価、いわゆるDPIAの実施や、プライバシー担当者の任命等の積極的な対応を行っている企業は限られていました。また、課題

として、海外法令に関する情報の取得や対応リソースの確保が困難であることが挙げられました。

「〇委員会の施策への示唆」を御覧ください。設問項目ごとに、当委員会の施策への示唆をまとめています。

「各企業における個人データの越境移転・利活用状況」への示唆として、企業によるデータの越境移転は、先ほど説明した地域で積極的に行われているものの、法令対応に必要な情報が得られていない等の課題が確認されたこと、国境を超えて活動する企業が円滑な法令対応を進めることができるような情報のより一層の提供が求められていることの２点が得られました。

「EU圏からの個人データの越境移転状況」への示唆として、日EU間・日英間における既存の相互認証については、円滑な個人データの越境移転において広く活用され、企業に利益のあるものと考えられること、そして、相互認証のメリットの更なる拡大が求められており、EU、英国以外の国との相互認証推進、我が国による認定対象国の拡大が期待されていること、また、日EU間・日英間においても、相互認証の対象となっていない分野の拡大、特に適用範囲の学術研究分野への拡大が期待されていること、多くの企業でSCCについても移転根拠で採用されており、企業間契約の締結の課題への対応として、定型化の推進が挙げられていること、相互認証の対象分野の拡大や企業間契約における定型化の推進等、企業にとってどのようなメリットになるかも考慮した上での議論や、各国当局との意見交換が求められていることの４点が得られました。

「DFFTの実現に向けた取組状況及び期待感」への示唆として、DFFTの推進に伴い、より円滑に越境移転が可能となるようなルールの整備が期待されているものの、整備に伴う企業側でのコストの増大等への懸念も挙げられたこと、DFFT推進の観点から、越境データ移転ツールについては、企業グループ内での移転の円滑化のほか、国際的に統一されたルール形成の要望等のグローバル規模の移転に向けた取組が期待されていることの２点が得られました。

「国際的な標準認証への期待感」への示唆として、国際的な標準認証を取得することによるメリットが、現状では限られていると認識している企業が多いことを踏まえ、認証制度の理解の促進、取得に必要なコスト等に見合ったメリットを提供する制度の構築が求められていることの１点が得られました。

「Global CBPRへの期待感」への示唆として、参画国・地域の拡大、ひいては参加企業の拡大といった企業認証ネットワーク拡大によるメリット増大への期待感が確認されていること、企業の参加意欲が高まるよう、Global CBPR認証において、各国が提供するメリットの創出への期待感が確認されていることの２点が得られました。

「ガバメントアクセス/データローカライゼーションへの対応」への示唆として、海外でのガバメントアクセスについて、各国の法的枠組みに関し、透明性の向上が図られる必要があること、海外でのデータローカライゼーションについて、規制の強化が、国際ビジネ

スの阻害につながることとならないように、バランスのとれた内容となる国際ルールの形成が求められていることの２点が得られました。

「企業のガバナンス体制の整備状況」への示唆として、企業において、海外法令対応を念頭に置いたガバナンス体制の更なる構築が必要であり、そのための支援が求められていること、ホームページで公開している「データマッピング・ツールキット」等のより一層の周知・啓発を通じ、データガバナンス体制の整備、DPIAの実施、プライバシー担当者の任命等のプラクティス普及を図る必要があることの２点が得られました。

「〇委員会に対する要望及び意見」を御覧ください。当委員会に対する「要望及び意見の内容」を抜粋しています。

例えば、海外法令やSCC等の契約ひな形の日本語訳の充実、日本の個人情報保護法における越境移転時の対応事項に関する英語での解説資料の提供、当委員会で検討されているテーマごとのリンク集の作成、ホームページのどこに何があるかについて分かりやすさの向上等については、「委員会からの情報提供や、ホームページからのコンテンツの発信方法等について、いただいた意見を踏まえ、必要に応じて改善対応を検討してまいりたい」としております。

他方、「要望及び意見の内容」のうち、海外法令の各条文の解釈、詳細説明等の強化、海外の規制に関して分かりやすいガイドラインの作成、頻繁かつタイムリーな海外法令の調査については、「これらの要望に対応する調査・発信は、他の機関等で行われており、インターネットでアクセス可能なことから、そちらを参照・活用いただきたい」としております。

資料に基づく説明は以上です。

最後に、本アンケート調査に御協力いただきました、経団連及び新経連の事務局の皆様、加盟企業の皆様に対しまして、この場をお借りしまして厚く御礼を申し上げたいと思います。どうもありがとうございました。

本議題の資料、議事録及び議事概要は、準備ができ次第、全て公表したいと考えております。事務局からの説明は以上です。

〇丹野委員長　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。

藤原委員、お願いします。

〇藤原委員　どうも御説明をありがとうございました。

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の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と理解しています。そして、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と感じております。

委員会として、このような形での調査は初めてのことであると認識しておりますけれども、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ですから、今後も継続してい

ただきたいです。まずは、今般の調査から得られた結果を、当委員会の施策、国際戦略の参考とするべきですが、今申し上げたように、調査の継続的な実施が必要でないかと考えます。

○丹野委員長　ありがとうございます。

ほかにどなたか御質問、御意見等はございますか。

大島委員、お願いします。

○大島委員　御説明ありがとうございました。

総合的な越境移転ツールの開発推進について、述べさせていただきたいと思います。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、そして、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りますことが明らかになったと考えます。

また、相互認証が利用可能な場合には、よく利用されており、企業にも利益があるとされていますが、企業間契約を行う企業もあるという調査結果ともなっております。

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と思います。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とされており、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と認識した次第です。このような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ろうかと思います。引き続きよろしくお願いします。

以上です。

○丹野委員長　ありがとうございます。

ほかにどなたか御質問、御意見等はございますでしょうか。

よろしいでしょうか。

では、私からも今後の方針に関して、お話ししようと思います。

まずは、事務局からもありましたが、この場を借りて、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と思います。大変価値のある調査結果を得ることができたと思っております。

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した。調査結果は、今後の政策立案の参考として大いに活用していきたいと思います。

また、藤原委員の御発言にもありましたが、このような調査は、継続していくことが大切です。今後も定期的に、継続的に実施してまいりたいと思っております。

私からは以上です。

ありがとうございました。

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ます。本議題の資料、議事録、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いたします。

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

（監視・監督関係者以外退室）

○丹野委員長　それでは、議題４「監視・監督について」、事務局から説明をお願いいたします。

（内容について非公表）

○丹野委員長　本日の議題は以上でございます。

それでは、本日の会議はこれで閉会といたします。