日　時：令和５年 12 月 21 日（木）10：30～
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、加藤委員、藤原委員、
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、梶田委員が御欠席です。
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266回個人情報保護委員会を開会いたします。
本日の議題は一つでございます。
議題１「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、本日は電子情報技術産業協会（JEITA）並びに全国商工会連合会（全国連）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）
それでは、出席を認めます。JEITAからお願いいたします。
（電子情報技術産業協会入室）
○丹野委員長　それでは、本日は、JEITAの吉田様並びに小泉様に御出席いただいております。それでは、早速ですがお二方から御説明をお願いしたいと思います。どうぞよろしくお願いします。
○JEITA　本日は、資料に従いまして、JEITAとしての３年ごと見直しに関する意見を御説明させていただきたいと思います。
２ページ目をお願いいたします。
「はじめに」ということで、今まで個人情報保護委員会様のほうからガイドライン、Ｑ＆Ａ等で非常に充実した情報提供をいただいておりまして、事業者の実務に大変有り難く活用させていただいております。このような方向性を今後とも維持していただくということを希望いたします。
次ページ以降、二つの■の項目について意見を述べます。
一つ目は、「政令、規則、またはガイドラインを通じて明確化をお願いしたい事項」、二つ目として、「その他、個人情報保護委員会様へのご要望事項」となっております。
次のページをお願いいたします。
３ページ目に参りまして「政令、規則、またはガイドラインを通じて明確化をお願いしたい事項」の一つでございますが、個人データの漏えい等の報告義務につきまして、まず、

現状では、不正の目的によるおそれがある漏えい、具体的には不正アクセス、サイバー攻撃等については、件数にかかわらず、また、漏えいした内容にかかわらず報告しなさいという義務になっておりますが、例えば、一般に公開されている氏名等の情報だけとか、本人の権利利益を侵害するおそれが必ずしも大きいとは言えない場合については、例えば、一定件数を超える漏えいの場合だけなど、もう少し条件を付けていただけないかという検討をお願いしたいと考えております。

二つ目の■に参りまして、報告対象となる四つの事態に、それぞれ「おそれがある事態」という対象が追加されておりますけれども、特にサイバー攻撃の場合では、個人データが漏れたおそれがあるかどうかという判断が非常に難しくて、時間がかかるということで、さらに、サイバー攻撃を受けて、おそれがある事態において、実際に個人データの漏えい等になるケースというのは比較的少ないということもありますので、この「おそれがある事態」の定義に関して、個人の権利利益のリスク、事業者の負担とのバランスを考慮した見直しをお願いします。具体的に言うと、個人データが漏れたとほぼ確実な場合に報告してくださいという程度をガイドラインにしていただけると有り難いと思っております。

次、４ページ目に参りまして、これは契約書のひな形を例示していただきたいというお願いになります。委託先の監督義務につきまして、日本の法律に合った標準的な委託条項の記載例をガイドライン又は別資料等で示すことを検討していただけないかと。この背景としては、特に外国系の事業者について、日本法に必ずしも合致しない、GDPR準拠の契約書を、一方的に、これじゃないと駄目だと言ってくる場合があって、なかなか対応に苦労されている会社があるということで、お願いになっております。

その次の「外国にある第三者への提供の制限」、あるいは、クラウド事業者が個人データを扱わないことになっている場合の契約条項の記載例の例示についても同じ趣旨でございます。

ただ、最後に書いてありますように、GDPRのSCCのように、この契約ではなくては駄目だとされますと、民間で既に締結している契約等に大きな影響を与えます。ですので、あくまでガイドラインで、全く同一でなくても良いと。民間の自主的な契約の取組を尊重していただきたいという、その方向の記載でよろしくお願いしたいと思います。

では、次、５ページ目に参りまして、こちらはPIAとDPOの努力義務化ということで、一つは、PIA（プライバシー影響評価）というのを求められる案件が大分増えてまいりましたので、PIAを自主的に導入するケースが増えて、安全管理対策としても有効であるため、対象案件を、リスクの高い案件に限定した上で努力義務規定化してはどうかという提案でございます。

二つ目のDPO（データ保護責任者）につきましても、多くの海外法令で、GDPRで言う第三者の資格のある人というDPOではなくて、一般的な社内の責任者で可能という意味でのDPOの設置が義務化されております。日本において、プライバシーマークではこれが必要になってまいりますので、そこら辺の背景を考えた上で、対象事業者、事業分野を限定した上

でDPOの設置を努力義務に規定してはいかがかと考えております。

続きまして、６ページ目に参りまして、こちらは生成AIに関するお願いでございます。

最近は、御承知のとおり急速に生成AIの利用が広がってまいりまして、個人情報保護委員会様でも６月に注意喚起等を出したところでございますが、事業者におけるAI利用を促進する上でも、以下の点を含めてガイドライン、Ｑ＆Ａ等での明確化をお願いしたいと考えております。

一つは、入力したプロンプトに含まれる個人データが、当該プロンプトに対する応答結果の出力以外の目的で取り扱われる場合は第三者提供に当たるとか、応答結果の出力のみで取り扱われる場合は委託に当たり得るのかどうかです。

また、上記と関連して、生成AIサービスに個人データに当たるプロンプトを入力する場合、先ほど御説明したガイドライン、Ｑ＆Ａ7-53、事業者側が個人データを扱わないとする場合との関係で、第三者提供、委託に当たらないケースがあり得るのかについて、ガイドライン、Ｑ＆Ａで明確化をお願いしたいと考えております。

次、７ページ目に参ります。

引き続き、AI等の新技術への対応ですが、プロファイリングによって推測された個人データの位置付けについてでございます。

AIによるプロファイリングで、既知の個人データから新たな個人データを推測したり、サイトの閲覧履歴から内定辞退率を算出してプロファイリングしたり、あと、宗教に関する書籍の購買履歴から信仰を推測するといったことが個人データの取得に該当し得るか否かについて諸説ありますけれども、AI時代にプロファイリングの利用拡大が予想されるため、こちらについては、また、ガイドライン等において明確化をお願いしたいと。

宗教関係の書籍の購買履歴自体については、今、要配慮個人情報には当たらないというところはガイドラインで明記されておりますけれども、それ以外にも、AIのプロファイリングはいろいろ拡大する可能性がございますので、明確化をお願いしたいと考えております。

次、「生成AIの出力した個人情報の取扱い」ということで、生成AIが個人データを出力した場合、どう扱うべきか。あるいは、出力内容に含まれる正確性をどのように確保したらよいか等について、ガイドライン、Ｑ＆Ａにおいて明確化、また、そこまで行かなくても論点整理等をお願いできたらと考えております。ただし、その過程で、事業者の義務が強化される可能性がある場合は、技術面や運用面について事業者に十分ヒアリングを行っていただくことを希望します。

次、８ページに参ります。

こちらは「学習済みモデル（生成AIを含む）の学習時における公開情報の扱い」です。

学習済みモデルの開発に当たって、ウェブで公開されている個人情報は、利用目的を公表していれば学習データとして取得、運用することができると考えております。ただし、要配慮個人情報を除くということですが、このような考え方について、Ｑ＆Ａ等で明確化

をお願いしたいということです。

あと、要配慮個人情報につきましても、法第20条第２項（７）で、一定のものを公開されている場合は、本人同意なく取得可能とされておりますので、これが、例えばインターネット上の百科事典等で公開されている情報であれば、本人同意なくAIで学習できるかどうかなど、そういう点についてＱ＆Ａ等で明確化をお願いしたいと思っております。

次、９ページ目、その他の御要望事項でございます。

一つは「日EU間・日英間のデータ越境移転」ということで、昨年４月施行の改正によりまして、学術分野、公的分野にも対象が拡大されましたので、日EU・日英の十分性認定につきましても、これらの分野・部門にも拡大するよう働きかけをお願いしたいと考えております。

また､CBPR等のグローバルな越境データということで､今こちらに記載してあるとおり、データの越境移転を規制する国がアジアを中心に非常に広がってきていますので、これらの国からのデータ移転をスムーズにできるように､Global CBPRの参加国増加や､CBPRを活用した移転方法の明示等をしていただけるよう働きかけてほしいと思っております。

同様に、グローバルなデータ移転ツールのハーモナイゼーションに向けた働きかけも引き続きお願いしたいと考えております。

最後、10ページ目でございますが、累次の改正を重ねるごとに、個人情報保護法における個人情報の情報区分がどんどん増えております。直近では、仮名加工情報や個人関連情報が追加されたところでございますけれども、これらの関係が結構複雑で、事業者内部でも、事業部門に説明するのが結構難しかったり、管理業務が複雑化する等の管理負担が生じておりますので、少なくとも、これ以上は情報区分、定義等は増やさないでいただきたいというお願いでございます。

私からの説明は以上です。

○丹野委員長　ありがとうございました。

追加の御説明はございますか。

○JEITA　大丈夫です。

○丹野委員長　それでは、ありがとうございました。

ただいまのJEITAからの説明について、御質問等をお願いいたします。

藤原委員、お願いいたします。

○藤原委員　新しい問題を含めて御説明いただき、ありがとうございました。

漏えいに関して二つほどお伺いしたいことがございます。

まず、最初に資料の３ページですが、漏えい等報告義務に関しまして、「不正の目的によるおそれがある漏えい等」を対象とする個人データを一定件数超えた場合に限定するという御提案だと理解いたしました。もう少し教えていただきたいのですけれども、漏えいのおそれの段階からの報告が必要であるということと、そもそも限定するということですけれども、おそれの段階から報告が必要であるということも踏まえますと、発生の段階で

漏えい件数等の全体像が把握できているのかと。できないケースが多いのではないかと。そうすると、ここで要件を限定してみても、報告対象の絞り込みに果たしてつながるのかという印象ですけれどもいかがでしょうか。

二つ目は、「おそれのある事態」において、「漏えい等事案」となったケースは少ないとの記述がありますが、これは客観的に、具体的にどのくらいの比率なのか、定量的にお示しいただける数字はないでしょうか。

それから、事業者として、漏えい等がほぼ確実になった段階など、提案の基準について、具体的にどういったケースであれば漏えい事案になり得るのかといった、その判断を行うに際して、JEITAとして、漏えい事案になり得るという基準の想定がお有りなら、それも併せてお示しいただきたいと思います。よろしくお願いいたします。

○JEITA　ありがとうございます。

２番目の質問につきましては、今、即答が難しいので、持ち帰り、JEITAの中で検討させていただきたいと思います。

１番目の質問に関してですけれども、確かに漏えいのおそれが発生したときで、個人データの件数が分からないという事態は非常に多いです。その件数の確定まで時間を要するとか、そもそも、個人データが含まれているかどうかすら分からないと。そこの判断に結構、調査の手間暇を要するという実態がありますので、せめて個人データが含まれていそうだという、この蓋然性が高い状態となってから報告というのが、事業者の実務上妥当かと考えております。

というのは、近年、サイバー攻撃というのは非常に頻発しておりまして、何かのデータが持っていかれたかもしれないという、いわゆるそのおそれの時点というのは結構多いです。その中で、個人データが持っていかれたかどうかというのは、調べるのに結構手間がかかります。そうなると、３から５日以内の速報というのは、やはり、個人データを持っていかれた可能性が高いと分かってから３から５日以内とか、そういう形にしていただくのが多分実務上と整合するのかなと考えております。１番目の質問についてはそういう回答でよろしいでしょうか。

○藤原委員　今の点ですけれども、どのようなデータが漏えい等したか分からないから蓋然性が高まってから報告するということになりますと、逆に言うと、例えば、個人データが含まれているかどうか不明であるという報告の仕方等、報告方法を少し工夫すれば、報告は可能だということになりますか。

○JEITA　工夫というのは、個人データが含まれているかどうか不明といった報告の方法でしょうか。

○藤原委員　そういう事案であるとか、あるいは、業務に差し支えのない範囲で、こういう事故でという話です。そういう形でなら可能であるということですか。もちろん、どうなるか分からないのですけれども、工夫の余地がある話なのか、要件の解釈をきっちりやれという話なのか、どちらかなと思いましたので。報告の在り方に工夫を加えれば報告で

きるという話なのか、そもそも、そういう蓋然性がまだ分からない段階では、事業者にとっては大変負担であるというお話なのでしょうか。
○JEITA　ちょっと補足になりますけれども、いただいた２点目の御質問に関しましては、あるJEITAの会員企業の方からは、大企業としては日常的に頻繁にサイバー攻撃を受けているということでございまして、そういったサイバー攻撃を受けるということで、インシデントのおそれがあるということのアラートが上がるわけですけれども、そのアラートが上がったとしても、実際に調べてみると、漏えい等が発生しているケースというのは、ほぼゼロ％ということですので、そのゼロ％のものを、全ておそれがある段階で報告するのは、やはり負担が大きいということで、ある程度、漏えいが確実になった時点で報告というようにしていただいたほうが有り難いと聞いております。
○JEITA　追加の御質問の回答としては、個人データの漏えいした蓋然性が高い段階を認識してから３～５日以内と。まだ分からないという段階では、やはり調査のほうを優先すべきということになりますので、蓋然性が高まった時点から３～５日以内に報告としていただいたほうが、事業者の実務と整合するかと思います。
　以上です。
○藤原委員　ありがとうございました。
　もう一つ、二つ目の質問のほうは持ち帰っていただけるということですけれども、具体的な数や基準も併せて後日御検討いただくことなのですか。この漏えい事案になり得るというのは、具体的にどんなケースを想定しておられるのでしょうか。
○JEITA　そこは持ち帰って確認の上、事務局から回答したいと思います。
○藤原委員　よろしくお願いいたします。ありがとうございます。
○丹野委員長　藤原委員、よろしいですか。
○藤原委員　はい。結構です。
○丹野委員長　ほかにどなたか。
　浅井委員、お願いします。
○浅井委員　浅井です。よろしくお願いします。御説明、どうもありがとうございました。
　御説明の資料の５ページ目ですけれども、PIAについて、対象案件を限定した努力義務化が望ましいとの御意見ですが、具体的にはどのような分野や案件において特に有効だとお考えなのでしょうか。例えば、生成AIなどの新たな技術を利用する際、PIAとしては、個人情報保護法やガイドラインへの適合性を評価する以外に、具体的にどのような点について事前に評価を行うことが考えられるのでしょうか。
　２点目として、また、同じページに、DPO設置の努力義務規定化についても言及がございます。対象とすべき事業者や分野はどういったものを想定しているか。また、その理由はどうお考えでしょうか。
　最後の質問でございます。PIA、DPOとも努力義務によることを御提案いただいています。なぜ、義務ではなく努力義務なのか。むしろ明確な義務としたほうが事業者の取組が進む

のではないかとも考えられますが、御意見をいただきたくお願いいたします。
○JEITA　一番答えやすい３番からお答えしますけれども、いきなり事業者の義務にしてしまうと、非常に負担がかかるという事業者さんも多いので、まずは努力義務ぐらいから始めるのがよろしいのではないかということで、こういう記載にしました。
　２番目の質問と関係して、事業分野、対象分野の限定ということでございますけれども、こちらについては、やはり一般個人のプライバシー侵害リスクが高い情報をたくさんお持ちの分野、医療・金融とか、そういった分野が想定されるのかと。正直言って法人顧客の名刺情報しか持ちませんというリスクの低い事業者は当初は外していただきたいという趣旨でございます。
　１番目のPIAでございますけれども、努力義務規定化することが望ましいと考えた背景としては、日本でPIAをやろうとしたときに、何に準拠して良いかという、そのよりどころというのがなかなかなくて、やるとしたらGDPRのDPIAを参考にしてやるしかないとか、そういう状態ですので、できれば、日本版PIAの標準的なよりどころというのを、この際、お示しいただけると有り難いのではないかという趣旨でございます。
　以上でよろしいでしょうか。
○浅井委員　どうもありがとうございます。
○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はございませんでしょうか。
　藤原委員、どうぞ。
○藤原委員　今の浅井委員の御質問の後半の部分に関連してですけれども、JEITAの言っておられるDPOの趣旨はよく分かったのですけれども、先ほど、Ｐマーク事業者、つまりＰマーク規定の中には確かにありますから、そういうことになりますと、事業者限定というよりは企業規模のお話なのかなと思ったのですけれども、そうではないかということと、もう一つは、実際に、義務規定ではなくて、GDPRのような第三者でもないということになると、ほぼ既に、今、JEITA傘下の企業であれば置いておられるのではないかと思ったのですが、いかがでしょうか。
○JEITA　おっしゃるとおりです。
　ですから、後段のDPOに関しては、ごく小規模の事業者を外すとか、一定の配慮をしていただければ、義務規定にしていただいてもあまり企業への影響はないと思っております。
○藤原委員　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す。
　ほかにどなたか。
　小川委員、お願いいたします。
○小川委員　委員の小川です。よろしくお願いします。
　生成AIの御説明がプレゼン資料の６ページから８ページにありました。これについて質問させてください。

資料には、生成AIのデータの入力、あと、生成AIが出力するデータですね。８ページは生成AIによる学習と、それぞれに関して、個人データの取扱いに関する基準を明確化してほしいと、そのように述べられています。生成AIについては、御存じのとおり文章中心のサービスや技術というのは注目されているのですが、ほかにも画像や音声の生成AIというのもあります。また、同じ技術やアルゴリズムを使った機械翻訳をはじめとして画像の認識とか、資料にもありましたけれどもユーザーのプロファイリングなど、様々なサービスや技術が今展開されている最中だと思います。

そのため、現時点で、個人データに関して生成AIの基準を明確化するということは、もちろん明確化の内容とか粒度にもよるのですけれども、技術やサービスの進展を妨げてしまうのではないかという可能性があるとの指摘もあります。

そこで質問したいのですけれども、生成AIに関するデータ入力・出力・学習で、それぞれ現状でどのような課題が生じているのかということを、もし分かれば具体的に教えていただければと思います。また、それらの課題が、ほかの技術やサービス分野でも共通しているのか。あるいは、生成AIだけの課題なのか、どのような考えもお持ちなのか教えてください。よろしくお願いします。

○JEITA　１点目で御質問をいただきました、事業者の中でどのような課題が生じているかにつきましては、今、生成AIの使い方等については事業者の内部でも内部規定などを決めて取組を進めているところでありますけれども、やはり、様々な事業部門、開発部門のほうからの、特に個人データとか著作権に関するデータに関する質問というのが多く寄せられている状況かと思います。

その中でも、ここに挙げた事例というのは、JEITAの会員企業の中から挙げられてきた、いろいろと事業を進める上で悩むところが多いので明確化してほしいということを意見として挙げておりますけれども、この意見の中に挙げていない例で申し上げますと、例えば企業の中で、自社でAIモデルを開発するという場合、自社以外の事業者が提供する基盤モデルに対しまして、API経由で個人データを含む学習データを入力して追加学習を行いまして、医療や金融とか、特定目的に特化した独自モデルを開発して、それを提供するような場合がございます。こういった場合につきまして、どうしても個人データを入力しないといけないというところ、それを他社の基盤モデルに入力しないといけないというところで、これが第三者提供に当たるのか委託に当たるのか、あるいは、そもそも提供に当たらないのか、そういったところを明確化していただけると、そういった開発部門のほうでそれを進める上で、開発してAIを提供して利用を進める上でのハードルが下がるということがございますので、そういったところでの明確化、つまり、事業を進める上での明確化をお願いしたいという趣旨でございます。

２点目の御質問の、生成AI以外の技術との関わり合いにつきましては、現時点では、生成AIの中でも文字・テキストを生成するものに意見が集中しておりますけれども、７ページ目で挙げたようなプロファイリングに関しましては、生成AIに限らず以前からある課題

といいますか、問題だと思っておりますので、こちらにつきましても、当然、プロファイリングで推測された個人データは個人データの取得に当たるものというような、事業者側としてはそういった理解、整理で事業を進めております。

その辺りにつきましても、実態に即した形で解釈を明確化していただいたほうが、事業者として、プロファイリングを利用する上での、そういった引っかかりの部分がなくなってスムーズに進むのではないかということで意見させていただいております。十分な答えになっているか分かりませんけれども。

○小川委員　最初の御回答の中で、自社以外の事業者が提供する基盤モデルのAPIを使って独自のモデルを追加するというお話なのですけれども、別に生成AIだけではなくて、APIでほかに提供することがたくさんほかの技術でもあるところ、そのときの扱いはどのように考えていらっしゃるのですか。

○JEITA　例えば、顔のデータとか個人識別符号を含むようなものもありますが、一般的にはやはり個人データが含まれているものを、つまり、第三者のほうに渡して、その第三者のほうが独自目的で使っているような場合には第三者提供に当たるという理解ですし、もし、提供元の指定した目的内で、特定した目的内で提供先が使うということでは、委託という整理で行っておりますので、そこについてはそういう理解でおりました。

○JEITA　生成AI以外の従来型のAPIの場合は、やはり委託ないし第三者提供の考えできれいに整理ができるのですけれども、生成AIは、プロンプトで入力すると、何かやって勝手に戻ってくるという今までの技術と違う面があるので、どう解釈したら良いかというところで、今迷いが生じているというところかと思います。

○小川委員　よく分かりました。ありがとうございます。

○丹野委員長　ほかにどなたか。

大島委員。

○大島委員　大島と申します。よろしくお願いいたします。

いろいろと御説明をありがとうございます。

私は、９ページで述べられている越境関係で、学術研究分野とか公的部門への十分性認定の範囲拡大について、それぞれの分野・部門について十分性認定がないということで、実務的にどのような問題が起きているのか教えていただければと思っております。加えて、今後、どういったニーズが見込まれているか、これについても教えていただければと思います。よろしくお願いいたします。

○JEITA　こちらにつきましては、JEITAの中の一般的な意見ということでまとめておりまして、例えば、JEITAに加盟する民間企業が学術研究機関と共同で研究を行う、医療分野等で研究を行うような場合に、欧州のほうの研究機関、医療機関から医療データなどの個人データを受けるような共同研究を行う場合があります。その場合に、欧州側の研究機関から、日本側の民間企業に個人データの移転を行うよりも、学術研究機関同士で移転を行ったほうがスムーズだという事情もございますので、そのような観点から、事業者としては

十分性認定の、これらの分野への範囲拡大をお願いしたいという趣旨でございます。
○大島委員　今後についてはどうでしょうか。これからも同様のパターンというかケースは想定されていらっしゃいますか。
○JEITA　医療分野等ではAIを使ったそういった研究などを行う際に、そういった幅広い分野というか、幅広い国の方々のデータが必要になってきますので、これからもそういったニーズが増えていくと考えております。
○JEITA　医療系の学術分野とか､あと､公的部門に所属する病院等の十分性認定があると、よりスムーズかなというところが意見の趣旨になっているかと思います。
　以上です。
○大島委員　ありがとうございます。
○丹野委員長　ほかにどなたか。
　加藤委員、お願いします。
○加藤委員　私のほうからは、少し話が変わりますが、安全管理措置等の事業者側のインセンティブについて教えていただければと思います。
　最近の漏えい等の事案の例に鑑みますと、委託先事業者や派遣社員を含めた安全管理体制の整備やシステム設計を含めたヒューマンエラーの防止策、不正アクセス対策等の安全管理措置を講じることが重要だろうと考えられます。対象事業者における漏えい等を防止するために何か自主的に行っている取組などがあれば教えていただければと思います。また、そのような取組を行うインセンティブ、又は行わないことに伴うディスインセンティブとなるものがあれば、併せて教えていただければと思います。
　よろしくお願いします。
○JEITA　ありがとうございます。
　事業者側が自主的に取り組んでいる安全管理として、一番有名というか多いのはISMSです。ISO27000に準拠した認証を取得する、あるいは、プライバシーマークを取得するといった第三者認証を取得するということがあります。
　それのインセンティブですけれども、特に民間同士の取引において、委託先にISMS又はＰマークを求めるという事例が増えておりますので、それが実質的なインセンティブになって、サプライチェーン全体の安全管理レベルが上がるという方向になっているのかなと考えております。
　以上です。
○丹野委員長　ほかにどなたかよろしいでしょうか。
　藤原委員。
○藤原委員　先ほどの大島委員の御質問に関連してですけれども、学術分野あるいは公的分野、医療データ、医療に係る個人データの越境流通というのは、ある意味で旧法の時から問題で、いろいろ議論を発表されておられたと思うのですけれども、先ほどの答えで、医療・学術分野等とおっしゃった「等」がどのぐらいありますか。つまり、医学、薬学、

それから、疫学、遺伝子が関係してくれば考古学もそうかもしれませんけれども、JEITAという組織の特異性もあるでしょうけれども、「等」といったときに、実際、医療以外で何か問題になっているのかという具体的な質問です。
○JEITA　JEITA内での議論の中では、学術分野の中で医療データ以外に特定の分野が出たということはないです。
○JEITA　藤原委員の御指摘のとおりだと思います。JEITAの加盟企業としては、ほとんどが医療データだと思っています。
○藤原委員　ありがとうございます。
○丹野委員長　ほかによろしいですか。
　私からも一つお伺いしたいと思います。
　先ほどから話題に出ていますプロファイリングの件でお聞きしますが、７ページに資料が出ておりますけれども、御指摘のような出力に加えて、ターゲット広告やプロファイリング等、データの最終的な利用の在り方によっては、個人の権利利益の侵害につながる可能性があると考えています。どういった事例においてそのような問題が生じ、不適正利用が当たると考えられるか、御存じであれば教えていただきたいというのが一つです。
　もう一つは、また、技術レベルが向上すれば、それとともに突合する情報量が当然増加する傾向にあることから、その懸念もますます強くなると思うのですが、技術的にそういった可能性を排除することができるのかどうか、その辺についても教えていただければありがたいです。
○JEITA　いただいた１点目の御質問につきましては、こちらは、JEITAの中で特定の事案が生じたということではなくて、ここの意見書の中にも書きましたとおり、就職希望者の内定辞退率を個人のレコードに追加してしまったという事案がございましたけれども、これについて、これそのものが要配慮個人情報に当たるわけではないですけれども、個人の人生を左右するような情報でありますし、個人情報の取得に当たるということが明確化されていれば、このような個人関連情報においても第三者に提供するというような事態は防げたのかもしれないという、そういった思いもございまして、そういった観点から明確化していただきたいという趣旨でございます。
○丹野委員長　お聞きしたかったのは、どういった事例においてそのような問題が生じて不適正利用に当たるのか、そのように考えるのかという点について御存じであればということでお願いしました。
○JEITA　不適正利用は、先程申し上げた事案ぐらいかと。
○JEITA　ここに挙げた意見の中では、不適正利用に当たるというところまでは強く述べていません。取得かどうかというところの明確化になります。
○丹野委員長　では、２点目のほうをお願いします。
　２点目は、技術レベルが向上するとともに、突合する情報量が増えるから、その懸念が増えるのだけれども、技術的にそういった可能性も排除することができるのでしょうかと

いうお尋ねです。
○JEITA　プロファイリングを通じて推測されたデータの中に、個人データが含まれたり要配慮個人情報が含まれたりするわけですけれども、そういったことを技術的に事前に排除するようなことができるかということにつきましては、これはそういった情報が出てきたとしても、個人のプロファイルなどをレコードの中に追加しないということになりますので、技術的にはそこは可能だと思います。技術の実現方法によって様々だと思われますが、レコードに加えないという処理は可能だと思っております。
○丹野委員長　了解いたしました。
　ほかに御質問される方はよろしいでしょうか。
　それでは、吉田様、小泉様、本日は御説明をありがとうございました。本日いただいた御意見も含め、個人情報保護をめぐる様々な状況について、さらに各方面の意見を聞きながら課題を整理、審議してまいりたいと思います。
　それでは、御退席いただけますでしょうか。
○JEITA　ありがとうございました。
（電子情報技術産業協会退室）
○丹野委員長　それでは、続いて、全国連に御出席いただきます。
（全国商工会連合会入室）
○丹野委員長　本日は、全国連の塩田様に御出席いただいております。
　それでは、塩田様、早速ですが御説明をお願いしたいと思います。
○全国連　よろしくお願いいたします。
　それでは、今、お手元にあります個人情報保護委員会の説明資料に沿って御説明させていただきます。
　商工会という名称に、皆様方、どのぐらいなじみがあるかどうかよく分かりませんので、簡単に概要を御説明させていただきます。
　右に日本地図がございますけれども、その赤いところに所在しているのが、地域の商工会と我々は呼んでおり、我々の組織でございまして、グレーになっているところは商工会議所が地域としておありになるということで、基本的に大都市圏を中心とした商工会議所と、我々は地方部、郡部の商工会というような組織編成になっております。
　どのぐらいの関係者がいるかというと、左側のところに会員数としてグレーの網かけのところがありますけれども、79万人ぐらいの方が会員として登録をされていらっしゃいます。商工業者はもっとたくさんいらっしゃるわけですので、我々が把握している組織率で考えると、58.3％ということなので、割り戻していただくと、倍よりはちょっと少ないぐらいの方が商工業者としていらっしゃるということです。
　商工業者という用語なのですけれども、実際上、例えば製造業だと20人以下の企業、飲食やサービス業だと５人以下というような事業者を我々は小規模事業者と呼んでおり、そういう企業が、79万人の会員の方の約９割いらっしゃるということでございます。我々は、

中小企業､小規模事業者というように両方の呼称をもって会員の方を呼び分けるわけです。全国の都道府県に47ございまして、市町村に、先ほど申し上げた郡部等、あるいは市町村の商工会が1,635というような数字になっております。

そういったところで、どういったことを商工会でしているのかというところの経年変化を棒グラフで表させていただいたのですけれども、先ほど申し上げた中小企業・小規模事業者の方が商工会という、地域のアクセスポイント、サービスポイントのところにアクセスしていただいて、いろいろな相談をするとか情報を得るとかアドバイスを得るとか、そういう形のインターフェースがあるものでございます。

一番多いのは「経営一般」というところでございます。多くの場合、この「経営一般」という中に入っていることが多いと承知をしております。

こういった事業者の数とか地域の展開とかも含めますと、個人情報保護法の対象である事業者が、５年前のヒアリング以降どう変化したのかや、現在の断面がどうなっているかということについて本日は御紹介をさせていただきたいと思います。

ちなみに、今、経営相談というのが、中小企業とか小規模事業者だけではないのですけれども、コロナウイルスをようやく抜けたときに、ウクライナ情勢等に起因する燃料や物価高、もしくは、それ以前からあるのですけれども、地域の人材不足というのがありまして、非常に厳しい状況になっています。そういったことをどのように処理をしていくか、また、販路をいろいろ拡大していくということがどうしても必要でございますので、そういったものに取り組んでいるというところでございます。

そうした環境の中で、まず、商工会においてどういった情報セキュリティ対策をしているかというところでございます。

大きく分けて、一番下のところに矢印が添えられておりますけれども、これは個人情報保護委員会の枠組みに沿った形で、我々もそういう段取りで進めさせていただいているということでございますけれども、組織における体制整備をまず進めた上で、職員等の人材育成及び情報リテラシーの向上、さらに各種施策等ツール活用による支援環境整備というものを行ってまいります。

これは､なかなか情報化云々という話を小規模事業者の方にするのが､リテラシーとか、そもそもうちの事業にどのように役に立つのかというところから始まるものですから、そこの無意識の壁を解消するとか、お客様からいただいた個人情報を漏えいしてしまえばどういう形になるのかという危機意識を持っていただくとか、そういうことを考えて対応をしているところでございます。

そういった問題意識に基づいて、商工会組織内においての取組として、個人情報の保護規程、プライバシーポリシー、基準、方針、セキュリティアクション制度への登録ということがございます。

これは、我々が、以前、平成30年に御説明する機会を設けていただいたときよりも進展しておりまして、例えば個人情報の保護規程というのは、平成30年の段階では85.4％ぐら

いだったのですけれども、今年の12月調査時点ですけれども現在は100％になっておりまして、これは、我々47都道府県にある県連というのと、商工会という各市町村にあるところと一応分けて集計しておりますけれども、ほぼ同じような数字を今達成しているところでございます。

それ以外にも、プライバシーポリシーとか個人情報保護に関する基準では、例えば、プライバシーポリシーでございますと、県連の場合は、平成30年に78％という達成率だったのですが、それは令和５年の12月では100％に到達しております。

それから、個人情報保護に関する基準というところでございますけれども、個人情報保護に関する基準というところは、令和５年の調査で言いますと、80％に達成しているのですけれども、これから進めていく余地が残っておるというところでございます。

情報セキュリティ基本方針とかセキュリティアクションについても同じような状況に置かれているというところでございます。

今までが商工会の取組でございましたけれども、商工の業者、中小企業、小規模事業者に、今言ったような方針とか規程ということのアプローチだけではなくて、実際、事前に、インシデントが起きないような形で、幾つかフェールセーフの仕組みを我々は使わせていただいて進めさせていただいております。

一つは、我々商工会のメンバーに法人カードというのを持っていただいて、その法人カードにサイバーリスク保険というのが会費の中に自動附帯されておりますので、もしそういうことが起きたら、そこで補償をされるというような仕組みを設けておりますし、それから、全部ではなくて、賠償責任も一部分にとどまりますけれどもその補償をするとか、もしくは、必要なリスクを診断するサービスとか、トラブルが発生した後の電話サービスとか、それから、専門の業者を紹介するとか、情報ツールの提供サービスをするとか、そういうものについても含みながら、取組を進めているところであります。

まだまだ個別の商工会のベースに行きますと、達成しているところとしていないところの色分けがありますけれども、なるべくこうした範囲を我々は広げていきたいと考えております。

御説明は以上でございます。御質問がありましたら我々のほうで回答させていただきます。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。

ただいまの全国連からの説明につきまして、御質問等をお願いいたします。

加藤委員、お願いします。

○加藤委員　御説明、どうもありがとうございました。

商工会からいろいろと取組をされているというお話を伺ったのですが、私からは、中小企業における個情法の認知向上に関して質問させていただきたいと思います。

今、いろいろ御説明いただいたのですが、中小企業においては、必ずしも個人情報保護法の存在や、その規定内容が十分に認知されているということはなかなか言えないのだろ

うと。当委員会の実施したアンケート調査では、中小企業において個人情報保護法上の規定である漏えい等報告の義務を知らなかった事業者の割合が約80％に及んでいるというようなこともございます。事業者の適切な対応を促すインセンティブや周知活動として、どのようなものが有効とお考えになるでしょうか。単に分かりやすく説明するだけで十分なのか、そういった点について、もしお考えがあれば教えていただければと思います。よろしくお願いいたします。

○全国連　今の数値は我々も承知をしておりまして、この部分に関して、まだ、達成するまでに先が長いなとは思っておるのですけれども、今までの、ガイドラインの作成やパンフレットを発行しての配付という活動に加えて、今そこまでは進んでいないのですが、SNS等のメディア媒体等も活用するということも引き続き検討していきたいと思っております。また、情報漏えいリスク、企業リスクを周知してもらうということで、我々自身だけではなくて、損保会社がサイバーアタックのリスクの保険を御用意されていますので、そういった各種媒体も活用させていただきながら進めていきたいと思います。これを段階的に進めていければと考えております。

○加藤委員　ありがとうございます。

○丹野委員長　ありがとうございました。

ほかにどなたか。

中村委員、お願いします。

○中村委員　中村です。御説明、ありがとうございました。

私からは、罰則に関連する質問をさせていただきます。

我が国において、個人情報の不適正利用事案や個人情報・データベース等の不正提供等の事案が発生しているところ、諸外国における直近の執行状況も踏まえると、実効的な個人の権利救済を行っていくためには、罰則の水準の引上げや直罰化、課徴金制度の導入を検討すべきと考えます。そこで質問ですが、罰則の強化について、どのようにお考えでしょうか。中小企業にとって、それが規律の理解や遵守のインセンティブとなり得るでしょうか。また、どのようなことが、中小企業にとって規律の理解や遵守のインセンティブとなり得るとお考えでしょうか。よろしくお願いします。

○全国連　ありがとうございます。

厳罰化云々ということは、我々だけでどうこういう話ではないので、全体の流れの中で御判断いただくことになろうかと思いますが、先ほど申し上げた中小企業とか小規模事業者というのは、大企業に比べると、人的・金額的リソースが全然違うので、そこの部分をどうやって埋め合わせようかというところが、まず大きな課題であります。規模的には非常にたくさんのデータを持っているところというのは限られているのかもしれませんが、それぞれCRMとかをやるときにはどうしてもそういうのが必要だということで、着手されている事業者はあると思いますので、そういうところをどうやって保全していくかということだろうと思います。

できれば、システムを小規模事業者が使う場合に、個人情報保護が一定担保されるようなサービスが世の中にあって、それが安心して利用できるような認証を付与していただくとか、そういうことがあれば、どうやったら良いのか分からないというボーダーラインにいる方を救えるかと思いますので、この手のアプリケーションは別に個人情報保護だけではないのですけれども､そういうものをパッケージとしてそういうことをしていただくと、一定のレベルに到達できるのかなとは思っております。

○中村委員　どうもありがとうございました。

○丹野委員長　ほかにどなたかコメントはありますでしょうか。

それでは、私のほうから質問をさせていただきます。

先ほどから、平成30年のときのお話をされていましたが、私も平成30年のときに委員席におりましたのでよく覚えています。ただいま御説明いただいたとおり、貴団体におかれては、個人情報保護についても非常に真摯に取り組まれていると感じておりますが、中小企業の経営者が、より一層個人情報保護に真摯に取り組める環境を実現するために、我々の委員会としてどういった取組を行うべきとお考えでいらっしゃるか、その辺を教えていただければというのが一つです。

二つ目は、最近の漏えい事案の例を見ますと、委託先事業者や派遣社員を含めた安全管理体制の整備、それから、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、それから、不正アクセス対策等の安全管理措置、この三つを講じることが非常に重要だと考えています。中小企業において、事業者として取り組んでいらっしゃるような内容、先ほど保険の話が出てきましたが、保険は後発的な手当てだと思うので、それも含めて、そういう自主的に取り組んでいる内容や措置を講じるに当たって、制度的な課題があれば御指摘いただければと思います。よろしくお願いします。

○全国連　１点目の御質問は、先ほどの中村委員からの御質問にも関連をすると思いますけれども、中小企業の方も、別にいろいろなサイバーのインシデントが起こって良いと思っているわけではないのですけれども、リソースの中でやったときには一定の割合でそういうことが起きてしまうということを、どうやって少なくしていくかということだろうと思います。

それに必要な枠組みは制度としてお作りいただいているのですけれども、そういった取組を小規模事業者とか中小企業が、自分だけではなくて複数共有することによって、ウィン・ウィンになって売上も上がるようなアプリができれば非常にうまく進むと思います。ただ、今の段階では、そういうECをやられている事業者や、CRMをお持ちの事業者は、非常にそういうところの問題意識が強いと思いますけれども、後続のグループをどうやって進めていくかというのは、何らかのバックアップがあると良いと思っております。

それから、２点目の件は、今おっしゃった三つのやり方というのは、それぞれアプローチが若干違うのですが、我々も、それぞれアプローチが違うことを承知しながら、やはり一番大きなことになってしまうのは、漏えいとかそういうことが起きてしまうと大変なこ

とになるということが、企業の意識に非常にクリティカルに認識していただくということだろうと思うので、そういうことが起きないほうが良いのですけれども、そういったようなところに重点を置いて進めていくのも一つかもしれませんし、今おっしゃった三つを総合的に組み合わせて進めていくということも当然あると思います。我々、どれに力点を置くかというのは、今の段階では明確なイメージを持っていないものですから、引き続き委員会の御議論等を踏まえて進めていければと思っています。

○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はございますか。

よろしいでしょうか。

それでは、御説明をありがとうございました。本日いただいた御意見も含めて、個人情報保護をめぐる様々な状況について、さらに各方面の意見を聞きながら課題を整理、審議してまいりたいと思います。

それでは、本日はありがとうございました。御退席いただけますか。

○全国連　失礼します。

（全国商工会連合会退室）

○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いたします。

本議題、ヒアリングが２件ございましたが、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。

本日の議題は以上でございます。

本日の会議はこれで閉会といたします。