

第3回パーソナルデータに関する検討会 議事要旨

日 時：平成25年10月29日（火）14:00～16:00

場 所：中央合同庁舎第4号館 12階 全省庁共用1208特別会議室

出席者：堀部座長、伊藤委員、佐藤委員、宍戸委員、新保委員、鈴木委員、滝委員、
松岡委員、森委員、安岡委員、山本委員
第二東京弁護士会消費者委員会
消費者庁 消費者制度課 個人情報保護推進室
山本 IT 政策担当大臣
総務省 総合通信基盤局 消費者行政課 玉田課長
経済産業省 商務情報政策局 情報経済課 佐脇課長
内閣官房 IT 総合戦略室 遠藤政府 CIO、向井副政府 CIO、二宮参事官、
吉川参事官、瓜生参事官、濱島参事官、村上調査官、神成政府 CIO 補佐官、
楠政府 CIO 補佐官、満塩政府 CIO 補佐官

1. 開会
2. パーソナルデータに関する検討会の論点について
3. 閉会

[資料]

【資料1】個人情報保護制度の実効性を担保するための執行体制の整備

- 世界に通用する個人情報保護制度の構築へ向けて - (新保委員提出資料)

【資料2】パーソナルデータに関する独立第三者機関について (宍戸委員提出資料)

【資料3】パーソナルデータの利活用について (伊藤委員提出資料)

【資料4】パーソナルデータの取り扱いルール整備について (松岡委員提出資料)

【資料5】パーソナルデータの利活用に関する消費者からの意見 (長田委員提出資料)

【資料6】パーソナルデータを巡る現状の問題点 (参考人提出資料)

(参考資料1) 第2回パーソナルデータに関する検討会 議事要旨

1. 開会

(山本 IT 政策担当大臣) 本日はお忙しい中、堀部座長を初め委員の皆様にお集まりいただき、ありがとうございました。前回に引き続き、第1回目に事務局から提示した論点について、今日も貴重な御意見をいただけると聞いている。

2回目は途中からの出席となったが、大変、中身の濃い議論をしていただき、私も委員の方々の御意見を読み、かなり長い時間、大臣レクも受け、2回目で相当議論の骨格が整

理をされたと、そんな気がしている。次回は論点に対する方向性を見直し方針案の提示ということになると思う。引き続き、現行制度で分かりづらいと言われている、いろいろな点、あるいは日本版 FTC の 3 要件の話もちょっと勉強させていただいたが、国際的な整合性、必要性等々の重要な点についても委員より指摘がなされたようであるが、今回もぜひ密度の濃い御検討をしていただくようお願い申し上げ、一言御挨拶とさせていただきたいと思う。

2. パーソナルデータに関する検討会の論点について

【資料 1 に基づき、新保委員より説明】

【資料 2 に基づき、宍戸委員より説明】

【資料 3 に基づき、伊藤委員より説明】

【資料 4 に基づき、松岡委員より説明】

【資料 5 に基づき、第二東京弁護士会消費者委員会より説明】

(堀部座長) どうもありがとうございました。

最初に申し上げたように、資料 5 に長田委員のペーパーがある。今日御欠席ということので、ここで御発言いただけないが、適宜ごらんになっていただきたいと思います。

これまでの委員、それから、水町弁護士からの説明につき、これから意見交換をしたいと思う。いろいろな観点から意見、あるいは質問をお出しいただきたいと思います。いかがか。

(森委員) 伊藤委員のプレゼンテーションについてお伺いしたい。2 ページ目だが、3 番の「我が国におけるパーソナルデータ活用推進に向けて」というところで、2 段落目に「データの利活用とプライバシー保護の両立を、匿名化等の技術のみで解決することは不可能であり、サイバーセキュリティ上のリスクも存在する。そこで、制度としては、プライバシー保護の観点から必要となるセキュリティ技術要件を明示し、その要件充足をデータ利活用の条件とし、プライバシー侵害が結果として生じた場合には、別途ペナルティを科すこととすべきである。結果責任を問うことでプライバシー保護の実効性を高め、また、利活用者の努力を促すことでセキュリティレベルが進化することも期待できる」とお書きいただいているが、ここにお書きのペナルティというのはどういうものを想定しているのか。それから、結果責任を問うことでとあるが、これはセキュリティ技術要件を充足していた場合でも、結果が発生すれば責任を問うという御趣旨なのかどうか、2 点お聞きしたい。

(伊藤委員) ペナルティということについては、どの程度厳しくするかというのはあると思うが、罰則規定のことを意味している。

それから、結果責任の意味合いは、プライバシーの侵害が結果として生じた場合に責任を問うという意味合いである。しかし100%安全なセキュリティというのは難しいと思う。例えば、ある程度のセキュリティ対策を講じていて、外部からのサイバーアタックを受けた時に、そこについてまで責任を負えるかどうかというのは、ちょっと難しいのかなと思う。

(森委員) そうすると、結果責任というのは、必ずしも結果が生じたら常に責任をとということではなくて、それはセキュリティがどうだったかということにも依存してということなのか。

(伊藤委員) セキュリティのレベルは一定の基準を設けないといけないと思うが、その基準を超えた対策を講じていた場合、例えば、サイバーアタックで情報が漏えいしたときに、そこまで責任を負えるかどうかという、そこまでは負いきれないのではないかという気がする。

(森委員) 御趣旨はよくわかった。ありがとうございました。

(山本委員) 伊藤委員に少しお聞きしたいのだが、いわゆるデータを保護するためのセキュリティ対策だけで全てできるわけではないというのは私もそのとおりだと思うのだが、結果的に生じた場合のペナルティは一体誰に係るのかというのがよくわからなくて、例えば、データを盗まれて、そのデータを悪用したら、データを悪用した人が本来罰せられるべきで、適切な対策を講じていて、それを破られた人は、確かにセキュリティレベルが十分でなかったという過失はある場合もあるのだろうが、その人が悪用したわけではない。プライバシーの侵害というのはデータが盗まれることによって起こるわけではなくて、データをその人が不本意な目的で使うことによって初めて起こるわけだから、実際に侵害を侵した人とは別なわけである。そういう意味でこれを書かれているのかと思ったのだが、そうではないのか。

(伊藤委員) そういう意味で言っているつもり。

(山本委員) ということは、このセキュリティ対策とペナルティとは直接関係するわけではなくて、実際にプライバシー侵害が起こったことに対して、別の制度をつくるべきだということか。つまり、データ保護法というか、個人情報保護法とプライバシーの侵害の間には少しギャップがあると思って、これがかなり難しくしている原因だと思っているのだが、それを分けて議論するという話とお聞きしてよいか。

例えば、医療機関で考えると、医療機関は応召義務があって、患者が来たら必ず診なけ

ればいけない。その際に個人情報をあずかるので、医療機関といえ、半ば強制的に個人情報を取得しなければいけない機関で、それはもちろん非常に大事な情報なので、それなりのセキュリティ対策をとるのだが、例えば、そこにトラックでぶつかってきて壁を壊して、中身を盗んでいった人がいて、患者の情報を悪用したら、医療機関に責任があるのではなく、情報を盗んで悪用した人が一義的には責任がある。そういうことが明確にならないと、結局は実効のあるプライバシー保護はなかなか難しいのではないかと思うのだが、これはそういうことか。

(伊藤委員) はい。

(安岡委員) 2つある。新保委員に1つ質問。3ページの個人情報データ保護規則が10月21日に欧州委員会で採択ということだが、話を伺っているところによると、2015年以降に施行と聞いている。イギリスは先延ばしにしてきたと認識している。そこで、日本でちゃんとやっていく上で合わせておかないと相手にされなくなるものは何なのか。要は優先すべきことは何なのかということをお願いしたい。

あと、宍戸委員に、第三者機関に関してだが、前回、私から、業界の認定団体とかにもかわりにやってもらうというのでもいいのではないかと提言したのだが、そういうのは憲法上、大丈夫なのかどうか。だめな場合はどうだめなのかをお願いしたい。

(新保委員) 今、御指摘の点については、個人データ保護規則ができなくても、実は対応しなければならない部分が、17ページ目以降に資料として今回入れさせていただいた。これがさらに個人データ保護規則という形で、あくまで指令レベルで、EU加盟各国は指令に従うということにはなっているが、規則のように直ちに適用されるということではなかったが、この指令の段階から既に我が国の個人情報保護法との関係においては、私は、17ページ、18ページの部分については、早急に対応しなければならないと従来から考えている。

簡単にかいつまんで御説明すると、まず、個人情報の範囲について、とりわけセンシティブデータの取り扱いについて、我が国は特段の規定を置いてないので、今後、国際的に見た場合に、センシティブデータの取り扱いについての規定はやはり何らかの形で定めなければならないであろうという点であるとか、個人情報取扱事業者の義務規定の適用を受けない事業者が存在するという点についても、オーストラリアが十分性の基準について、不適合という、29条委員会の判断を受けている。

これは正式な判断ではなく、あくまでEU個人データ保護指令に基づく委員会の意見という形で表明されているわけだが、その点で我が国も適合しないのではないかとと思われる点としては、義務規定の適用除外事業者が存在すること、それから、18ページ目以降の個別の適用除外事由の解釈によって免除される範囲が非常に多い。とりわけオプトアウトに

については、EUは今回さらに個人データ保護の観点から、本人同意の要件を原則課すという上での手続をより明確にしているのので、我が国はそれとは正反対にオプトアウトで第三者提供は全てするようになってしまうという手続があるので、こういった点についても、国際的な観点から、オプトインによる本人同意手続というものが必要だろう。

それから、監督機関は本日申し上げたとおり。

その他、本人関与の法的性格については、欧州では、個人情報、プライバシー保護については、プライバシーの権利に基づく、つまり、権利としての位置づけをかなり明確にしている。その一方で我が国は本人関与という形で、具体的な請求権としての根拠となり得るかどうかということについては、判例においても従来から消極的な見解をとっているのので、この点についても今後、具体的に請求権の行使の根拠となり得るかどうかということについても、EUの権利としてのプライバシーという観点からの点についても考慮が必要だろう。

最後に、データの移転でだが、現行、我が国は個人データの第三国移転については一切制限がない。これについては、クラウドコンピューティングを初めとして、越境してデータを移転する際の制約になっていないと従来は考えられていたわけである。ところが、EUの規制が厳しいということで、現在はデータの移転が厳しいと言われながらも、規制が厳しいところに個人データ保護の基準を合わせなければならないというところがあるので、最後に結論としては、規制が厳しいところに結果的によらなければならないところであれば、我が国もその点を踏まえた規制の見直しが必要だろうと思っている。

(宍戸委員) 今、御指摘の、業界団体あるいは民間団体に行政作用を一定程度渡すことができるかということ、最近の公私共働の中で、さまざまな観点からいろいろ議論されてきている分野である。そして、行政作用にも非常に多様なものがあるので、実際、どこからどこまで、民間団体にそういった作用を渡すことができるか、できないか、その場合の条件はどうかという問題は、文脈ごとに、ある場面ごとにいろいろ分けて考えて検討する必要がある。その意味では全く不可能ということはないし、現に、例えば、登録や認定について、民間団体にお任せし、それを行政機関のほうで基本的には尊重するといった例は実際にもあるだろうと思う。

ただ、これに対して、行政作用の中でも非常に権力的な作用を民間団体に完全に渡してしまうことについては、法治主義の観点から見て強い問題がある。おそらくそれが認められるのは、例えば、弁護士会における弁護士の懲戒のようなレアケースで、その業界、あるいはメンバーの自律性を尊重するといった、相当強い正当化が必要ではないかと考えられる。

逆に言えば、非権力的作用についてお任せするが、最終的には行政の側でちゃんとチェックするということできていれば、ある程度可能だろうと思う。要は、ここで問題となっている分野、とりわけこの場で問題になるプライバシーは国民の基本的な人権にもかかわ

る問題なので、完全に行政の側から外に出してしまうことは、やや問題がある。ただ、登録とか認定のうちとか、とりわけ技術的な要件について、民間団体の力を使う、最近はやりの言い方で言うと共同規制をうまく仕組みれば、非常に有効で効果的であり、法治主義の観点からも認められるようなものであれば、よいのではないかというのが私の考えである。

(安岡委員) 1点だけさらに質問だが、民間設定団体の場合に、前回、プライバシー・トラスト・フレームワークのことを最後にお話しさせていただいた。ターゲット広告をちゃんとやる企業と、訪問販売でずるく情報をとってくる企業と、十把一からげで考えてはまずいと思う。それをちゃんとレベル分けしていかないと、情報を渡す上でも、相手側の信用も当然あると思う。法律でそこまでやるか、もしくはガイドラインでもう少しブレークダウンしてからなのかもしれないのだが、それらのレベルを認定する場合は、宍戸委員の言うまさに登録、認定になると考えられる。従って、例えば、レベル1、2、3ぐらいを認定するというのは、民間認定団体としては可能だと認識したかどうか。

(宍戸委員) それは、つくり方としてあり得ると思う。実際のつくり方は、いろいろなやり方があると思う。今、御指摘の点で言う、業界団体に入って、一生懸命に巡視している企業は、コントロールを受けてしまうのに、団体の外にいる企業は、ルールメイクにもルールの遵守にもかかわってこないのが野放しになってしまうということが、この種の事例で起きる最大の問題だと思う。そういう場合には、今、議論されているプライバシー・コミッショナーあるいは第三者機関が、業界団体に入らずルールを順守しない企業についてはしっかり監督する。しかし、団体のルールを遵守しているメンバーについては、規制機関が権限を行使するのは例外とする、事実上のアグリーメントを結ぶ等、いろいろなやり方があるだろうと思う。

(鈴木委員) 新保先生に確認したい。新保先生の資料の18ページに国外への個人情報の移転というのがある。現在、直接、間接に事業者からいろいろ相談を受けているが、日本企業自体がもはやデータセンターや研究拠点を海外に持っていきたいということが多く出ている。それから、さまざまなウェブサービスの使用事業者がほとんど外資になってきて、国外から直接サービス提供するとなると、主権の範囲内に事業者がいないので、ことに行政規制においてはなかなか実効性が確保できない。これは多分、日本がビッグデータビジネス等、情報処理サービスに敗退を続けると、ほとんどデータが海外に行く時代になってしまう。特に医療データも早晩そうなる可能性がある。同じく人権思想を持つ国々であれば最悪な事態は避けられるが、人権保障すら確保できない国々にデータが漫然と流出すると、日本人のデータだけではなくて、EU、米国からいただいたデータもまた日本がバックドアになりかねないリスクもあるのだろうと。その場合、国外移転を禁止する規定が存在しないことに関して、何か有効な手だてはあるのか。

(新保委員) この点について、従来から、日本から海外に個人データを移転するに当たっては、例えば、暗号の輸出規制などがあるので、暗号化をすることについては逆に制約があるという部分もある。だから、現行の個人情報保護法では、個人情報の、正確には個人データの第三者提供としての第三国移転については禁止する規定はないけれども、それ以外の制約がある部分が一部ある。その点についての見直しも含めて、第三国移転についての問題については検討が必要であろう。とりわけ、個人情報のみならず、技術情報の流出防止という観点からも、データの移転、とりわけデータの漏えいに近いような移転については、これは規律をするためのルールが必要だろうと。

海外から指摘されてきたところとしては、日本はデータの移転については第三国移転の規定がないので、結果的にデータロンダリングが可能である。そのため、日本を経由して第三国に移転されるということについては、逆に他の国に迷惑をかけるという状況にもなりかねないという状況がある。

したがって、今後の対応としては、国内の事業者が国外にデータを提供することについては、こちらの 18 ページの資料にあるとおり、「漢字」を認識できる近隣諸国と書いたが、どういう国かというところではあるが、近隣諸国にデータの処理を委託する事業者がふえている。事実上、データのエントリーなどについては、ほとんど国外で行われているという状況がある。そうすると、そういった国に対してデータを移転して処理をすることについては、国内法上は委託先の監督責任が発生するが、それ以上の義務は発生しない。一方で国外から見た場合には、日本を経由した第三国移転が禁止されていないことについては、安心してデータを預けることができないという問題が出てくるわけである。

以上から、今後はデータのロンダリングという観点からの海外からの批判、国内の事業者が単に委託先の監督責任を果たすということでも果たされている第三国へのデータ移転ということについては、何らかの対応が必要だろうと考えている。

(堀部座長) よろしいか。そこをどのように規定するかという問題はあるということか。

(新保委員) なお、1点だけ、今後、第三国移転は制約をせざるを得ないという部分が出てくると思うが、その際に、先ほどのように、技術情報の流出・移転防止であるとか、個人情報だけでなく、第三国にデータが移転されることについての検討が必要であることと、先ほど安岡委員から御指摘あった EU の個人データ保護規則では、域外適用が定められているわけである。だから、こういったところについて、我が国ではそういった観点からの検討は行われていなかったが、EU では域外適用というところでかなり思い切った規定を置いているということも参考にすべきところはあるだろうと考えている。

(森委員) 私もやはり第三者提供絡みで新保先生に教えていただきたいと思う。前回、鈴木委員が言われて、今回、伊藤委員からも御提案があったが、第三者提供の例外として、ラピッドチェンジの報告書の FTC 3 条件を使って、第三者提供できる範囲を確保してはどうだという提案があり、特に技術検討 WG のほうでは割と喫緊の課題となっているわけなのだが、そういうものをつくった場合に、新保委員のスライドの 18 ページの一番上のポツの義務規定の除外規定に関し、23 条 1 項 1 号の第三者提供の制限の除外規定になってしまい、うまくいかないということにはならないか。

(新保委員) うまくいくかどうかということは、現在の時点では明確にわからない。ただ、段階として、現在、オプトアウトで全て可能となっている手続については、これはほぼざるだろうというところなので、このようにほとんどスループスのようにいってしまうという手続については、これはなかなか認められない。国際的に見ても、オプトアウトの手続によって対応しているものは、例えば、米国の金融サービス近代化法を初めとして、一部の法令があるが、EU からはやはりこの部分については、現在でもセーフ・ハーバーの観点からも充分性の基準は認められていないところである。

次の段階としての一定の要件または条件を課した上での第三者提供の例外を設けるといことについては、これは最近のいわゆるマルチ・ステークホルダー・プロセスの検討の過程において唱えられているところである。だから、いわゆる法規制によらないガイドラインレベルでの規制、それによって結果的にそれが法規制の趣旨にかなうという観点からの目的を達成することができるのであれば、その一定の要件、または条件のもとに適用除外事由を、例えば、第三者機関が明確にそれを示すということは当然あり得るかと思う。

ただし、注意点としては、例えば、FTC の 3 要件と呼ばれているが、あくまであれは一定の条件を示したものであって、ガイドライン的な要件を示したものではない。ですから、そういった一定の条件が示されたものを参考にして何らかの適用除外事由を検討することは当然必要になってくる部分があるかと思うが、そのような要件に過度に依拠して、それがあたかも一定の、我が国で言うガイドライン的なものと判断をして適用除外事由を定めると、18 ページの義務規定の免除という観点からは、例えば、EU の充分性の基準から考えた場合には適合しないと判断される可能性はあるかと思う。

(森委員) ありがとうございます。可能性としては、うまく両立できる余地があることとして理解した。具体的な内容はちょっとわからなかったところもあるので、後で教えていただきたいと思う。

(堀部座長) 今日説明していただいた中では、1 つは、第三者機関というか、これをどうするのかということがあった。宍戸委員からは非常に具体的に提案といたしますか、この点を明らかにしていただいた。このあたりについて、もう少し御意見などをいただければい

と思うが、今日の説明の中で、伊藤委員はその点については余り明示されていなかったのですが、どうお考えなのでしょうか。

(伊藤委員) 経済同友会には、特にこの問題について議論している委員会がなく、これまでの提言の内容を踏まえた発言に留まっているため、本会としてここで明確にこういう形がいいというお話は控えさせていただきたい。ただし、個人的には、きちっとした第三者機関があれば、それはそれでいいと私は思う。

(堀部座長) 今の点について、いかがか。

(森委員) それでは、余計なことながら申し上げると、宍戸委員の20ページ目のスライドに事務局体制のことを書いている。十分な予算・定員の確保が必要ということで、水町先生からも言及があったが、これは全くそのとおりで、今、第三者機関をつくって、そこでいろいろなことをしようということで、大体足並みがそろってきているところで、十分な予算・定員の確保をしないで存置してしまうということは、全ての努力を水泡に帰するものであると思うので、これについては強調をしておきたいと思う。

(鈴木委員) 意見が大体出てきたところだが、法改正はほぼ一致した意見ではないかと私は理解した。法改正は必須だということはぜひ確認いただきたいこと。それから、いつもどおりぐだぐだになっていくと、やはりビジネス的にも反転攻勢の機会を失うし、消費者保護的にも、全て海外にデータが行った暁には消費者保護も達成し得ることが困難になってくるということになると、必要なことは全てやらなければならない。ただ、1回で全ての改正はなかなか尽くし得ないということになると、2段階、3段階の改正は多分、必要になってくる。そうすると、水町先生から御提案があったように、現状のような形で法の主管があると、多分、なかなか改正が進まない。第三者機関がきっちりと法の主管をして、常に1丁目1番地になるようにして、継続して必要な法改正を続けていくということも、一応、今回、きっちり確認して、全て前に進めるということはやっていただきたいと思う。

(堀部座長) どのようにここの議論をまとめるか、次回以降させていただくが、そういう御意見をいただいたということで理解した。

(安岡委員) 別にソリューション(解決策)を持っているわけではないが、伊藤委員の話もあったように、どちらかというビジネス展開上の制約を強める方向のEUケースよりも、IT分野で経済成長を実現している米国ケースで実現していこうと御提案されている。EUのほうは厳しい規定がある中で、オプトイン前提というときに、現実論からすると、い

ろいろな企業がビジネスでアライアンスしていくときに、提携企業がふえていく。ポイントもそうだし、クーポンだって連携して提携企業がふえていく。そういう場合に、どうすればいいのか。どなたかアイデアがある方、お教えいただきたい。

(鈴木委員) 伝統的に事業者規制ですと、法人単位に1つ1つ分解的に捉えていくが、今日のビジネスは胴元がいて、加盟事業者がぶら下がっているということなので、ビジネスモデル総体を評価することなしに消費者のプライバシーインパクトは実は判明できない。小分けにしていくと特定個人の識別性がないとかという、部分的に適合性判断は実はもうできない時代に入っている。そうすると、トータルに見るという発想が必要になるし、具体的にはそういったものを紙でやっているわけではなくて、大多数は情報システムで実現しているから、ビジネスモデルを実現する情報システム全体を評価する中で、これが安全に、またプライバシー上配慮がなされている、または常に消費者が離脱できるような仕組みが整っているのであれば、共通ポイントカードであれ何であれ、これは認めていってもいいだろうということ。そういった消費者保護、総体評価ということがないままに、現状の法制度をそのまま惰性で引きずるということはもう限界に来ているのだと思う。そのあたりは、第三者機関がもしできれば、やはり研究して、新しい法制度にシフトしていく。EU・米国追随型ではなくて、日本が提案していくところの局面で、要はEUとの交渉の土俵に乗って、あとは交渉で頑張ってくれと。今は土俵にすら乗れない状況で、データがとまるかもしれないという状況だから、そのあたりを目指していくというのが大筋の考え方ではないかと思っている。

(安岡委員) 仰ったことには非常に賛成です。要は、日本のほうがEUよりはビジネスとしては先進的な部分があるから、ビジネスとして後進なところに全てを合わせる必要はないと思われる。日本ができるだけ先進的にやっていくべきかと、抽象的だが考えている。

(第二東京弁護士会(水町)) 共同利用者の範囲がわかりにくいということをプレゼンの中で申し上げたが、全ての段階で明らかにするというのは困難だとは思っている。なので、透明性の確保が一番大事かと思うので、同意取得のときに範囲が変更になり得ること、そして共同利用者の範囲がここで見られるよということをわかりやすい場所に明示する。それも長文の中で示すような形ではなくて、わかりやすい形に明示することが必要だろう。あとはクーポンもジャンルがあると思う。例えば、飲食店ジャンルであれば、何となく事前の包括同意というものも認められるかなと思うが、飲食店と保険会社だとか金融機関が共同利用者に含まれているとすると、全然違うジャンルであり、そこまでは同意していないだろうというものについては、オプトインで同意をとり直すとか、そういう柔軟な対応が求められてくるのではないかと考えている。

(堀部座長) 今日、先ほどから申し上げているようなことで、それぞれ意見を発表していただいた。これらをもとに、これをどういう形にするか、また事務局とも相談しながらまとめていきたいと思うが、第1回に出した論点について、それぞれの委員からの問題提起というふうにも受けとめられるので、それを踏まえて、こういうふうにしていったらどうかということは今後出していきたいと思う。

この問題といっても、グローバルな視点で見なければならぬというところがあり、2週間ほど前、経済産業省の佐脇課長と総務省の村上調査官などと一緒にヨーロッパに行ってきた。ブラッセルで、日本企業の関係者の集まりである JBCE (Japan Business Council in Europe) と私は随分前から意見交換をしているが、今回も会った。95年に現在のEUのデータ保護指令が採択され、98年10月24日に発効した。そのあたりからいろいろ、欧州にある日本企業の関係者が日本へのデータ移転はどうなのだろうかと非常に心配しており、そのころから、時々行くと意見交換をしてきた。ここのところもほとんど毎年のように意見交換して、今回もそういうことで意見交換してきて、その内容などもどこかでまとめてお話ししたいと思うが、一方では、先ほど新保委員から出たように、スタンダード・コントラクチュアル・クローズドということで、標準的な契約条項、これは当事者間でどうするか、また、内容について各国のデータ保護機関のオーソライズが必要になる場合があり、これで対応している。

それよりももう少し包括的なものがバインデング・コーポレート・ルーズというものなのだが、これも各国のデータ保護機関のオーソライズが必要だということで、これについても3年ほど前、消費者庁で実際に調査をして、報告書にまとめている。バインデング・コーポレート・ルーズは今のところ、少なくともイギリスのインフォメーション・コミッション・オフィスのホームページには日本の企業の名前は1つも出ていない。アメリカ企業中心に、この前見たところではたしか20ぐらいオーソライズされたものがあつたが、日本企業はない。だから、バインデング・コーポレート・ルーズというより包括的なものは、イギリスで見るとはなくて、いろいろ聞いてみると、日本の企業はそれにはよらずに、むしろスタンダード・コントラクチュアル・クローズドということで、当事者間で、ヨーロッパにある日本の現地法人と日本の本社との間でデータのやりとりをする、こういうことでやったりもしている。

それから、ヨーロッパ・データ・プロテクション・スーパーバイザーという、これは公的部門だが、欧州委員会のさまざまなデータ保護の監督をしているところ、それから、欧州委員会の司法総局のデータ保護の担当者などとも意見交換をしてきたし、また、日本の企業がクライアントになっているところが多いと見られているリンクレーターズというブラッセルにある弁護士事務所のパートナーとも意見交換をしてきた。

その他いろいろあるが、そういうことで意見交換すると、日本のデータの利活用と保護を図る上で、そうした国際的な動向を踏まえて議論をしておく必要があるであろう。個別

にはいろいろあるが、そういうことを感じた。このパーソナルデータに関する検討会でも、そうしたことが最初からいろいろ出ているが、ことし中にまとめるに当たり、そのあたりも踏まえていきたいと思う。それについては次回、できれば、最初の論点のものを骨子とした骨子案のようなものが出せればと思うが、これは事務局と相談した上で、次回以降、お話ししたいと思う。

次回については、追って事務局から連絡していただくということによろしいか。

それでは、予定の終了時刻を若干過ぎましたので、本日の第3回の会議は以上で終わらせていただく。どうもありがとうございました。

以上