

消費者委員会 個人情報保護専門調査会（第5回）

議事録

内閣府消費者委員会事務局

消費者委員会 個人情報保護専門調査会（第5回） 議事次第

1. 日時 平成23年4月13日（水） 10:00～12:10

2. 場所 消費者委員会大会議室1

3. 出席者

（専門委員）

長谷部座長、藤原座長代理、宇賀委員、臼井委員、大谷委員、岡本委員、柿原委員、
角委員、新保委員、杉浦委員、飛山委員、長田委員、三木委員、三宅委員、吉川委員

（担当委員）

川戸委員

（説明者）

経済産業省 相川課長補佐

内閣官房セキュリティセンター 高田参事官

独立行政法人産業技術総合研究所 高木主任研究員

全国消費者団体連絡会 阿南事務局長

（事務局）

齋藤審議官、原事務局長

4. 議事

1. 開会

2. 個人情報保護の状況に関するヒアリング

- ・経済産業省
- ・内閣官房情報セキュリティセンター
- ・独立行政法人産業技術総合研究所
- ・全国消費者団体連絡会

3. 閉会

《 1 . 開 会 》

○原事務局長 おはようございます。それでは、時間がまいりましたので、始めさせていただきます。

本日、年度初めのお忙しいところお集まりいただき、ありがとうございます。前回3月15日にこの個人情報専門調査会を予定しておりましたが、大きな震災で中止をさせていただきました。震災に遭われた方々、本当にお見舞いを申し上げます。

3月の専門調査会を中止とさせていただきます。今日が第5回の個人情報保護専門調査会ということでよろしくお願ひしたいと思ひます。

本日は専門委員の須藤委員、別所委員、山口委員が御欠席と承っております。担当委員の下谷内委員が所用により御欠席となっております。

始まります前に配付資料の確認をさせていただきます。配付資料は議事次第と書かれたものの裏のページに一覧を載せております。本日もヒアリングを予定しております。ヒアリングの関係ということで資料1が経済産業省、資料2が内閣官房情報セキュリティセンター、資料3が産業技術総合研究所の高木さんからの資料、資料4が全国消費者団体連絡会からの資料ということで、最後に参考として今後のスケジュールについてをお付けをしております。不足がございましたら事務局までお申し出いただければと思ひます。

それでは、長谷部座長、どうぞ議事進行をよろしくお願ひいたします。

○長谷部座長 どうもおはようございます。先ほど原事務局長からお話でしたが、去る3月11日に東日本大震災が発生しました。この場を借りまして被災者の皆様に心からお見舞いを申し上げますとともに、被災地が1日も早く復興されることをお祈り申し上げたいと存じます。

和田委員が退任をされまして、新たに消費者委員会の松本委員長から飛山委員が専門委員の指名を受けて、このたび個人情報保護専門調査会の審議に参画をされることになりました。最初に飛山委員から簡単に自己紹介をお願ひできますでしょうか。

○飛山委員 千葉県総務部政策法務課長の飛山でございます。よろしくお願ひいたします。

《 2 . 個人情報保護の状況に関するヒアリング 》

○長谷部座長 ありがとうございます。

それでは、議事に入らせていただきます。本日も前回に引き続きまして、個人情報保護の状況に関するヒアリングを議題として取り上げたいと存じます。今回はまず関係省庁による施策の実施状況等に関しまして、経済産業省、内閣官房情報セキ

ユリティセンターからそれぞれ御説明をちょうだいしまして、その後、情報通信分野における個人情報保護につきまして独立行政法人産業技術総合研究所から、そして消費者から見た実態につきまして、全国消費者団体連絡会から御説明をちょうだいしたいと存じます。

それでは、まず経済産業省から信用分野におけます施策の実施状況について、御説明をお願いいたしたいと存じます。それでは、経済産業省の商務情報政策局商務流通グループ取引信用課の相川課長補佐、よろしくお願い申し上げます。

(1) 経済産業分野のうち信用分野における個人情報保護の取組について（経済産業省）

○相川課長補佐 おはようございます。私は経済産業省商務情報政策局取引信用課で課長補佐をしております相川と申します。本日はよろしくお願いいたします。

私の方から右肩に資料1と書いてございます資料に沿って、御説明をさせていただきたいと思っております。経済産業分野のうち信用分野における個人情報保護の取組みについて、御説明をいたします。

1 ページ目、本日の目次でございますけれども、当方では個人情報保護法の関係でガイドラインを策定していますので、まず1でそのガイドラインについて、2で認定個人情報保護団体の取組みについて、3で事業者に対する指導・監督について、そして当方はクレジットの分野につきましては個別法の割賦販売法の中でも、こういった個人情報保護に関する取組みもございまして併せて4で御説明をさせていただきたいと思っております。

2 ページ目、ガイドラインといたしまして「経済産業分野のうち信用分野における個人情報保護ガイドライン」というものを策定しております。平成16年12月に告示をされております。

概要といたしまして、経済産業省が所管をいたします分野のうち、信用分野（物品または役務の取引に係る信用供与に関する分野）における個人情報保護のための格別の措置を講ずるものでございます。この信用分野は、主にクレジット業を念頭に置いていただければと思っております。※に記載しておりますけれども、「個人情報の保護に関する基本方針」におきましても医療、金融、情報通信と並びまして、格別の措置を講ずる必要がある分野として掲げられていることを踏まえまして、措置を講じているところでございます。

また、「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」というものがございまして、当方のガイドラインはこちらを基礎として規定をしております。すなわち、この経済産業分野ガイドラインの上乗せの措置という形で記載をしております。

ガイドラインの規定の内容といたしましては、まず義務規定といたしまして、第三者提供・信用情報機関の利用を行う場合は、書面で同意を取得するというものがございます。クレジットの分野ですと信用情報機関というところがございまして、信用情報を集めて与信に役立てるという制度がございますので、他の分野とは異なり、その辺りを重点的に措置しているところが特徴的なところでございます。

あとは、個人情報に係る同意条項と契約条項を分離するであるとか、保存期間を設定し、その期間経過後、消去するであるとか、安全管理措置、従業員の監督、委託先の監督等について措置を講じております。

3 ページ目、引き続きガイドラインの規定についての御説明ですが、努力規定として、5,000 件未満の小規模事業者のガイドライン遵守につきまして、努力義務としております。こちらはガイドライン共通化の取組みの前から、努力義務として規定しているものでございます。あとは、センシティブ情報の取得の禁止であるとか、共同利用を行う場合は書面で同意を取得するであるとか、個人信用情報機関における会員管理というものも別途、別紙という形で1つくり出して規定するなどしております。また、申込原票につきましても、申込原票だけですと個人情報には該当するものの個人データには該当しないのですが、こちら個人データと同じように安全管理措置を行うよう上乗せで規定をしております。

ガイドラインの策定・見直しの状況でございますけれども、平成 16 年に新規策定をいたしまして、その後、平成 18 年 10 月 16 日に個人信用情報機関に関する部分について、産業構造審議会での議論を経まして、個人信用情報機関自らの安全管理措置であるとか、個人信用情報機関による会員管理について規定しております。

2 回目の改正がございしますが、平成 21 年 10 月 9 日にガイドライン共通化への対応、経済産業分野ガイドラインの改正に伴う技術的改正を行っておりまして、これまで合計で 2 回の改正を行っているところでございます。

4 ページ目、クレジットの分野でも認定個人情報保護団体の認定を行っております。現在、社団法人日本クレジット協会を認定しております。

団体の概要でございますけれども、当時の社団法人日本クレジット産業協会、社団法人全国信販協会、クレジット個人情報保護推進協議会、これら 3 つの団体の組織・機能を統合いたしまして、平成 21 年 7 月 1 日にこちらが設立されたものでございまして、同日に認定個人情報保護団体として認定をしております。この平成 21 年の認定以前のクレジット分野における認定個人情報保護団体といたしましては、※のところに記載をしておりますが、クレジット個人情報保護推進協議会が平成 17 年 5 月に認定を受けておりまして、認定業務を行ってきたところでございます。

団体の特徴といたしまして、認定個人情報保護団体の機能のほか、割賦販売法に基づく認定割賦販売協会の機能、こちらは割賦販売法に基づきまして自主規制などを行う機関という制度でございまして、そちらの認定を受けておりまして、

また、業界団体としての機能も併せて持っているという特徴がございます。対象事業者数は今年1月1日現在で967社となっております。

主な活動内容といたしまして、個人情報保護指針の策定、改正があります。対象会員の個人情報の取扱いに関する顧客からの苦情等への対応について、実績は以下のとおりでございます。また、個人情報の漏えい等の発生時の経済産業大臣への報告について、実績は以下のとおりでございます。

5ページ目、引き続き認定個人情報保護団体の取組みの主な活動内容でございますけれども、平成22年度の実績を掲載しております。まず上のところ、会員の個人情報管理責任者等を対象といたしまして、個人情報保護法令及び個人情報保護指針に関する知識の習得のために、全国4地区にて研修を開催したところでございます。大阪、札幌、東京、福岡の4地区で、修了者といたしまして433名となっております。テーマといたしましては、改正割賦販売法と個人情報保護を巡る動向ですとか、個人情報保護に係る企業の対応、認定個人情報保護団体の活動と個人情報保護対応について研修を行っております。こういった研修においては、当方の担当官ですとか、個人情報保護関係の弁護士の先生、大学の先生など有識者の方から講演をいただいております。

また、下のところに記載しておりますが、個人情報の取扱いに関する相談・苦情処理業務の担当の方々を対象といたしまして、全国3地区にて研修を開催しております。大阪、福岡、札幌の3地区で合計134名の修了者数となっております。テーマは右に記載のとおりでございます。

6ページ目、続きまして当方における事業者に対する指導・監督について御説明いたします。

まず研修・セミナー等での講演ということで、先ほど申し上げました認定個人情報保護団体主催のセミナーにて、改正割賦販売法と個人情報保護を巡る動向というテーマで、全国4地区にて当方の担当官が講演をしております。併せましてクレジット関係団体主催のセミナーなどにおきましても、クレジットカード番号などを含む個人情報保護の重要性について講演をしております。平成22年度ですと以下の2箇所、一般社団法人日本電機工業会、流通系クレジット会社協議会のセミナーなどにおきまして、講演をさせていただいております。

クレジット業者からの個人情報の漏えい等の報告の対応といたしまして、クレジット業者からの当省への個人情報の漏えい等の報告は約1,300件ございます。平成21年度ベースでございます。それぞれ原因は右の円グラフに記載をさせていただいておりますけれども、郵送などの送付ミスが83%、紛失・書類が9%、FAXの送付ミスが3%という状況になっております。事案ごとに原因究明をし、必要に応じて再発防止策の指導を行っております。

割賦販売法による対応ということで、次ページ以降に記載をさせていただいてお

ります。当方でクレジット業を所管する法律といたしまして、割賦販売法という法律を所管しております。こちらの関係で個人情報保護に関する規定もございますので、こちらも併せて御説明をさせていただきます。

まず指定信用情報機関の関係でございますけれども、前提となる制度の概要といたしまして、クレジット業者に対しまして事前に指定信用情報機関を利用した支払能力調査を義務づけておりまして、指定信用情報機関への情報の登録も併せて義務づけてございます。

制度の考え方といたしましては、与信する前に消費者の方がどれだけのクレジット債務を負っていらっしゃるのかというのを、指定信用情報機関にちゃんと見に行き確認をした上で与信をしてくださいというものです。一方で、ちゃんとその方の債務の総額がわかるように、クレジットの情報については指定信用情報機関に登録をしてくださいということを義務づけているという枠組みとなっております。

これらを前提といたしまして、クレジット業者の義務として、まず同意の取得の義務でございますけれども、加入クレジット業者に対しまして指定信用情報機関への情報照会、情報登録に関する事前の同意取得を義務づけております。併せて、罰金などのサンクションが規定されています。目的外使用等の禁止ということで、加入クレジット業者の役職員や、これらの職にあった者に対しまして特定信用情報、クレジット情報でございますけれども、その目的外使用を禁止しております。

指定信用情報機関の義務でございますけれども、秘密保持義務として指定信用情報機関の役職員またはこれらの職にあった者に対しまして、特定信用情報提供等業務、こちらは情報の登録を受けて提供をするという業務でございますが、これに関して知り得た秘密を漏らし、または盗用することを禁止しています。

加入クレジット業者に対する監督義務といたしまして、指定信用情報機関に対して、加入クレジット業者が指定信用情報機関から提供を受けた特定信用情報を目的外使用しないように指定信用情報機関の方でちゃんと監督をしてくださいということを義務づけてございます。

8 ページ目、クレジットカード番号等の保護に関する規定もございます。

安全管理措置ということで、クレジットカード会社（イシューア及びアクワイアラ）に対しまして、クレジットカード番号等の安全管理措置について義務づけをしているところでございます。クレジットカード番号単体でも、個人情報保護法及び同法ガイドラインと同等の保護措置を講じるということで、規定をしているものでございます。

背景といたしましては、クレジットカード番号等の場合、番号と有効期限で氏名が分からなくてもインターネット上で買い物ができるしまうというところが散見されていたところ、番号と有効期限のみでは個人情報には該当しないんですけれども、それらを用いて消費者被害が起こってしまうというところを踏まえまして、ク

クレジットカード番号単体であっても個人情報保護法や同法ガイドラインと同程度の措置をとってくださいということを義務づけているところがございます。イシューア-は上記に加えまして、不正使用検知モニタリング等の二次発生防止策を実施する必要のあるとしております。

クレジットカード会社は自社や加盟店、加盟店の委託先等に対しまして、クレジットカード番号等の適切な管理が図られるよう措置を講ずる必要があるということで、クレジットカード会社は当然大量の個人情報を保有することになりますので、自身がちゃんと保護措置を講ずるといのは当然であります。その加盟店ですとか委託先に対しても、ちゃんとした指導をしてくださいということを義務づけてございます。

加盟店に対しましては、事前の措置といたしまして、①漏えいなどの事故が発生した場合はそれについて連絡すべき旨の通知をあらかじめしておくことを義務づけています。すなわち、できるだけ漏えいが起こった場合に早期にそれが発見されるような措置を、あらかじめ講じておくという趣旨でございます。②でございますが、漏えい等の事故が実際に発生した場合には、再発防止のために必要な指導を行うということ、あらかじめ通知をしておくことを義務づけております。加盟店の委託先に対しましては、これと同じことを、加盟店を通じて委託先に措置することを義務づけております。

事後措置といたしまして、実際にその漏えいが起こってしまったといった場合には、類似の漏えいなどの事故の再発防止のために、必要な措置を講ずることについて、指導をちゃんと加盟店にするということを義務づけております。加盟店の委託先に対しましては、加盟店を通じて、同等の措置を講じていただくことになっております。また、クレジットカード会社の委託先に対しましては、委託先に対する必要な監督を行うことを義務づけております。これらの委託先というのは、何次にもわたる委託先というのが想定されますので、二次以上にわたる数次の委託先まで含んでございます。

9 ページ目、クレジットカード番号等を不正入手した者に対する罰則でございます。以下に該当する者に対しまして、懲役または罰金を科しているところでございます。

①クレジットカード会社、クレジットカード番号等保有業者またはこれらの従業員、退職者が不正な利益を図る目的で第三者へ提供・盗用した者、また、②クレジットカード番号等を詐取した者、管理者の承諾を得ずに複製した者、不正アクセスにより取得した者が該当します。このうち、クレジットカード番号等を詐取した者というところで、昨今インターネット上のいわゆるフィッシングと言われる疑似ホームページのようなものから個人情報を抜いてくるということに対して、ここでいうクレジットカード番号等を詐取した者が対応してまいりますので、そこが1つポ

イントとなっております。

③でございますが、正当な理由なくクレジットカード番号等を売買した者、売買する目的で保管した者についても、今回の罰則の対象となっております。

全体といたしましては、個人情報保護法に基づく対応をするとともに、併せて、割賦販売法で上乗せの規制をし、割賦販売法上は立入検査権限もございますので、そちらでも厳格な対応をしていくという全体としての対応となっております。

以上でございます。

○長谷部座長 どうも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きまして御質問、御意見がございましたら、どうぞよろしく願いいたします。白井委員、お願いします。

○白井委員 個人情報をも不正に入手したり、目的外利用をしたりしたというケースはどんなものがあるのでしょうか。それはまとめられていますか。

○相川課長補佐 例えば個人情報保護法に基づくものとしては、勧告を平成 19 年にしておりますけれども、そちらの場合ですと従業員の方が自分で個人情報を入手して、そのまま持って行ってしまうというケースはございました。その場合は従業員に対する措置ですとか、アクセスの認証をちゃんとやってくださいということ、勧告しております。

○白井委員 目的外使用はありませんか。

○相川課長補佐 先ほどの平成 19 年の勧告の件において、従業員が個人情報を持って行ってしまったということがありましたので、その中で何らか目的外使用があったかと思えます。

○白井委員 第三者提供の制限に引っかかるものはありましたか。

○相川課長補佐 個人情報保護法に基づく執行として勧告を行ったのが、クレジットの分野では先ほどの平成 19 年の勧告 1 件となっております。そこまで大きな違反行為というのは、それ以外のところでは今のところないのかなと認識しております。平成 19 年のときには、実際に従業員の方が個人情報を持っていったようなケースだったと思うので、何らか第三者提供していることもあったかと思えます。

○白井委員 ありがとうございます。

○長谷部座長 三宅委員、お願いします。

○三宅委員 資料の 4 ページに日本クレジット協会の主な活動内容の 2 つ目のポツで、対象会員の個人情報の取扱いに関する顧客等からの苦情等への対応ということで、苦情 2 件と問い合わせ 166 件でございますが、5 ページの研修での個人情報に関する相談・苦情への対応の留意点についてというのがございますけれども、要するに苦情について認定個人情報保護団体がどう対応しているのかについて、具体的に経済産業省として御報告を受けていらっしゃるのでしょうか。具体的な内容について、どれぐらい把握されているかということをお聞きしたいですが。

○相川課長補佐 資料の4ページの期間ですと、こちらに記載をしておりますとおり、苦情は2件処理をしていると聞いておりました、認定個人情報保護団体である日本クレジット協会は、クレジット業者に対してその情報の提供等を行うということをしております。例えばこの2件のうちの1件は、何か不正利用をされてしまって、その情報が個人信用情報機関に載ってしまっている、これを何とかならないのかという話がありました。それは友人にクレジットカードを不正利用されたようなケースでございまして、不正利用してしまいましたという友人とともにクレジット会社に行っていただいて、確かにこれは不正利用でしたねということで、認定団体の方ではクレジット会社につないで、クレジット会社の方ではそれらを受けて、情報は確かに間違っていたということを確認した上で情報の訂正をしているということが、具体的にこの苦情の内容はそういったものでございます。

○三宅委員 経済産業省所管の関係の認定個人情報保護団体というのは、この社団法人日本クレジット協会以外にも幾つかございますね。それぞれの団体で毎年どういふ苦情があつて、それに対してどういふ対応をしたのかということ、総括的にデータとして集積されていて、それに向けて具体的な改善指導をされているといういふような経済産業省としての対応について、今、言ったようなことはどれぐらいなされているのかということについてお伺いしたいのですが。

○相川課長補佐 クレジットの分野としては日本クレジット協会がございまして、そういった苦情の対応をさせていただいております。経済産業省全体というところでは、第2回のヒアリングで当省の情報経済課の方からとりまとめて、例えば経済産業省全体では18の団体を認定しているという情報とともに、御説明をさせていただいているところがございますけれども、そちらでは年1回は認定個人情報保護団体連絡会というものを実施してございまして、苦情の対応などもホームページに公表させていただいて、連携を図っているところでございます。

○長谷部座長 角委員、どうぞ。

○角委員 1つ教えていただきたいのですが、もしかしたら私が誤解しているかもしれないので、そのときはそうおっしゃっていただきたいのです。個人情報保護のガイドラインと割賦販売法における対応というのは、ガイドラインの方とはとにかく個人がOKと言わなければ、信用情報は外には出しませんよというスタンス。これに対して割賦販売法は、多重債務を防止するためには積極的に個人情報を取ってこいというか、必ずアクセスしなさいとか、与信を受ける側も自分の情報はちゃんと登録することに同意しなさいとか、しなさいとはそこまできついことは言っていませんが。そういうふうな、2つある意味で相反する目的を持っていると思いますが、そうするとその折り合いのつけ方というのはどうお考えでしょうか。

○相川課長補佐 確かに御指摘いただきましたとおり、まさに信用情報という、その方がどういふお買い物をしたのかという、かなり重要な情報である一方で、多

重債務問題ということで、先ほど御紹介させていただいた規定も平成 20 年の改正に基づいて規定が入ったものでございまして、ちょうど平成 21 年 12 月に大部分が施行されて、すべてが施行されたのが昨年 12 月 17 日で、かなり最近改められたという状況でございます。そういった相反する保護法益といったところがまさにあるので、それは本当に難しいところだなという認識をしております。

その中で、ではどうやっていくのかというところに関しましては、先ほど規定の中でも御紹介をいたしましたけれども、情報を見に行ってください、一方で情報をちゃんと登録してくださいという義務はどうしても多重債務問題への対応という観点で課さなければいけないので、そういった義務を課す一方で、ちゃんと同意をとらなければいけないということを、消費者にちゃんと説明しなければいけないというところがございますので、同じその法律の中で同意をとってちゃんとしてくださいという義務づけを併せて行っているところがございます。

あとは本当にちゃんと同意がとれているのかどうかとか、ちゃんとした書面でやっているのかどうかとか、その辺りは立入検査なりで監督をしていく。指定信用情報機関側にも情報がかなり蓄積をされることになりますので、そこに対しても我々の方で適宜立入検査なり、そういったある程度の権限を法律の中で与えられているところですので、それらを用いてしっかりとした監督をしていくというところかとは思いますが。

○長谷部座長 よろしゅうございますか。

○角委員 そういたしますと割賦販売法の関係ですけれども、同意をしてくれなかったら、クレジット業者は与信をするわけにはいかないわけですね。そういう対応に最終的にはなるのでしょうか。あなたが OK と言わなければ、残念ながら与信はできませんという対応でいいということでしょうか。個人情報に係る同意条項と契約条項の分離というのがよくわからなかったのですが、それにバッティングするのかわからないのか、教えていただければと思います。

○相川課長補佐 ガイドラインの方で 2 ページのところを御指摘いただいたのかと思いますけれども、確かに個人情報に係る同意条項と契約条項をちゃんと分けてくださいということを規定しております。こちら契約条項の中に同意条項が埋め込まれてしまうと、結局自分が何に対して同意をしているのか、例えばわっと細かい字でいっぱい書かれてしまうと、どこに本質的な同意があるのかというのがわからなくなってしまうので、そこはちゃんと分けた上で、これがちゃんと同意ですよ、あなたの情報を取得しますよというのをわかるような形で、その同意を取得してくださいという趣旨でございます。

○角委員 どうもありがとうございます。

(2) 我が国の情報セキュリティ戦略について（内閣官房情報セキュリティセン

ター)

○長谷部座長 ほかにはいかがでしょうか。よろしいようでしたら、そろそろ時間もほどほどでございますので、それでは、相川課長補佐、どうもありがとうございました。

それでは、続きまして内閣官房情報セキュリティセンターから、我が国の情報セキュリティ戦略につきまして、御説明をちょうだいできればと思います。内閣官房情報セキュリティセンターの高田参事官から、報告をお願い申し上げます。よろしくお願いいたします。

○高田参事官 内閣官房情報セキュリティセンター参事官の高田でございます。座って失礼させていただきます。

今日は情報セキュリティ戦略ということで、御説明の機会をいただきましてありがとうございます。私ども内閣官房情報セキュリティセンターは、後でまたちょっと資料の中でも出てまいりますけれども、政府全体の情報セキュリティ政策の企画立案、総合調整という立場で仕事をしております。具体的な個々の施策の執行自体は、基本的には関係各省庁さんにやっていただいております。政府全体として横串を通して対応する必要がある事項に関して、私どもの方から企画立案ということで積極的に発言をしたり、あるいは関係省庁さんの間で調整をとって、政府全体としての対応レベルを上げたりというようなことをミッションとしている職場でございます。

早速でございますけれども、資料に沿って御説明を申し上げたいと思います。まず、今日私ども情報セキュリティセンターがここにいる背景、どういう考え方か、何が起こっているのかという背景の情報となろうかということで資料の1ページ目、ちょっと古くて恐縮でございますが、総務省さんで行っていただいた調査を取り上げさせていただきます。

ごらんいただきますとおり、情報通信、IT利用に関する不安感がどういうところにあるのかというのを、いわゆる個人のレベルと事業者さん、企業さんのレベルとでそれぞれアンケート調査を行った結果が示されてございます。具体的にこの調査において選択肢として掲げられた項目は情報セキュリティ、プライバシー、マナーや社会秩序、商取引、知的財産権という項目で調査をされているわけでございます。いわゆる個人レベルで見ると情報セキュリティとプライバシーの問題というのはほとんど並ぶような形で、やはり最大の関心事になっている。それに比べるとマナー、商取引、知財というのは心配度としては少ないという調査結果が出てございます。他方、企業さんの場合はやはり事業活動を円滑に進めるという観点があるのではないかと思います。選択肢として掲げられている5項目、いずれも満遍なく心配事項として取り上げられているという現実があるかと思います。

そういう意味で、企業さんにおいても情報セキュリティの問題とプライバシーの問題は同じぐらいインパクトのある問題で、国民目線で見ても、あるいは事業者さんの目線で見ても、この情報セキュリティ問題とプライバシーという話というのは、大変大きな課題としてとらえられているという1つの例示になるのではないかと、思って、このデータを取り上げさせていただきました。

それでは、ざっくりと情報セキュリティとプライバシー、あるいはこの場でございますので、個人情報保護ともうちょっとかちつとした言い方でとらえた場合に、どういう関係にあるのかというのを、私どもの考え方でございますけれども、整理したものが資料の2ページ目でございます。

情報セキュリティ政策というのは、もともとICT、情報通信技術を安心安全に利用することによって利便性を高める、経済、社会の活力を高めていくというのが出発点になってございます。このために書かれてございます高度情報通信ネットワーク社会形成基本法、IT基本法と称してはございますけれども、こういう法律もつくりまして、総理大臣が本部長の下、IT本部というところで総合的な政策を推進していこうと決められたわけでございます。

そのIT基本法の22条でございます。ここで私どものミッションの根幹になります安全性及び信頼性の確保というのも、大事な政策領域であるということが明示的に規定をされている。それに並ぶ形で個人情報の保護、その他国民が安心して利用できるような必要な措置が講じられていなければいけない。ネットワークの安全性及び信頼性の確保、情報セキュリティの領域と個人情報保護その他という並べて書かれているのが、IT基本法22条であるという理解をしてございます。

具体的に情報セキュリティと個人情報保護はどう違うのかというのは、下半分の表のところ提示されております。俗に私どもは情報セキュリティと言うと3要素あります。C.I.A.という言い方をしてございます。CというのはConfidentiality「機密性の確保」、IはIntegrity「完全性の確保」、AはAvailability「可用性」です。情報の中身そのものではなくて、むしろそういう様態がきちんと確保され、いかなる情報であろうとちゃんと守られなければいけない情報はちゃんと守られているか、勝手に改ざんされていないか、使いたいときにちゃんと使えるか。この3つの要素で考えるというのが基本的な考え方でございます。

それに比べますと、これは私の理解ですけれども、個人情報保護と個人情報ということ自体が、守るべき価値のあるものというアプローチであるわけですが、そこで法律上書かれてございますのは漏えい、滅失または毀損の防止ということで、やはり改ざん、漏えい、毀損と考え方は似ているだけけれども、言わば情報セキュリティの立場で言うと、両方扱うメディアとしてのいかなる情報であろうと守っていかなければならないのに対し、それ自体に守るべき価値があるものととらえるのが個人情報。そういうとらえ方の違いがあるのかなと理解してございます。

私どもは基本的に冒頭でも申し上げたとおり、情報セキュリティセンター自体で直接具体的な法律を所管して何か政策を執行するという体制はとってございません。政府機関については政府統一基準というガイドラインをつくって、その上で各省庁さんが自己の情報システムを守るための情報セキュリティポリシーというのを各省庁ごとに、要するにシステムの責任者ごとに定めていただいて、それに従って運用する。あるいは重要インフラに関しても重要インフラの行動計画ということで共通的なガイドラインを設けまして、その中で各重要インフラ事業者さんの所管各省庁さんの下で、場合によってはその事業関連法律の下あるいは各省庁さんの施策の中で対応していただくということで、基本的には法律そのものではなくてガイドラインによって横串を刺していくというのが、私どもがやっている考え方でございます。

当該分野に関しては一番下の柱でございますが、国際規格であるとか認証制度もございます。情報セキュリティ一般ですと I S O の規格に準じて定められました I S M S、情報セキュリティマネジメントガイドラインに基づく認証制度というのが運用されてございます。個人情報保護の観点から P マーク制度というものがそれぞれに運用されていると理解してございます。そういうことで国民の不安感の観点から、非常に情報セキュリティとプライバシーの保護と密接にしておりますし、制度的あるいは政策的枠組みというのともかなり近接する部分があるのではないかとということで、実は私どもセキュリティセンターとしても、消費者庁さんあるいは消費者委員会の皆さんとも密接に連携しながら、政策を進めていく必要があるということは日常考えているところでございます。

ページ進みまして、具体的にどういう考え方で情報セキュリティ政策をやっているのかというのが、スライド 3 枚目の資料でございます。少し経緯的な話を御説明申し上げた方がいいと思いますが、資料の下の方ですけれども、そもそも政府における情報セキュリティ対策はどうやって始まったのかというのを示したいということで用意した年表でございます。

2000 年ごろ、インターネットも大分普及してきて、政府からの情報提供手段としてインターネットの活用、ホームページの活用というのを非常に一般的にされるようになってきたわけですけれども、2000 年に複数の省庁のホームページが不正侵入されまして、改ざんされるという問題が立て続けに起こったことがございます。このころから正確な情報、きちんとした情報を伝える上で、政府機関もきちんとした情報セキュリティ対策をやっていかなければいけない。これが私どもの政策の発端でございます。この 2000 年 2 月に情報セキュリティ対策推進室というものが設置されて、これがいろいろ経緯ある中で 2005 年に現在の情報セキュリティセンター、現在の政策体系がつくられるに至った流れになってきている。

その後、私どもも基本的な政策に関して、政策のスタンスに関して第 1 次、第 2

次と書いてございます基本計画ということで、3～4年ぐらいのスコープで、まず大きな政策の枠組みをつくり、その上で各年度の年次計画をつくって、どういう政策を進めていくのかというのをやってきたところでございます。実は2009年に2回目の第2次情報セキュリティ基本計画というものをつくりましたが、その後、政権交代等もございまして、改めて2010年に国民を守る情報セキュリティ戦略、これが先ほど申し上げました政策の基本骨格をなす文書でございまして、これを2010年5月に策定いただきまして、現在の基本的な政策の指針となっているところでございます。

その指針で掲げられている重要な要素がスライドの上の部分でありまして、1つは情報セキュリティの問題を単に情報システムを守ってやっていくのではなくて、ナショナルセキュリティに準ずるものとして考えていかなければならないのではないかと。サイバー空間上の安全保障・危機管理と、少し大きくくりな立場で物を考えていかなければいけないということを強調したというのが1つの点です。

もう一つは、これは従前からあった考え方ですけれども、やはり国民生活、経済、社会を活性化する上で、積極的にITを使っていかなければいけない。その上で基盤となる情報システムのセキュリティをきっちりしていかなければいけない。両者合わせて情報セキュリティ先進国に我が国をしていきたいという考え方でやっております。

特に安全保障・危機管理という項目が、2010年の国民を守る情報セキュリティ戦略の中で新しい概念として取り込まれてきたわけです。この背景として前年2009年7月に実は韓国とアメリカで非常に規模の大きい、いわゆるサイバー攻撃という問題が発生しまして、特に韓国の場合はいわゆるオンラインバンキングなんかは停止するとか、かなりのシステムが破壊されるという、大きな被害が現実のものとして隣国で発生した。アメリカの場合は比較的上手に抑え込んだようでございますけれども、やはり個々のシステムを個別に何とかするというのを超えて、経済、社会の基盤を破壊するようなインパクトのあり得る攻撃というのは現実に起こり得るんだ。実はこういうサイバー攻撃自体も、もっと前に2007年のエストニア、2008年のグルジアなど、ヨーロッパあるいはもう少し西の方で経験はしてはいたんですが、韓国、アメリカと近隣でも起こる。これにきちんと対応していかなければいけないということで、新たな項目が入ったというのを御理解いただければよろしいかと思っております。

それをどういう体制でやっているかというのが、4枚目の情報セキュリティ政策の枠組みと推進体制ということで、先ほどもIT基本法の話で申し上げましたとおり、総理大臣を本部長とするIT戦略本部の下に、情報セキュリティ政策会議というものが設置されてございます。これは官房長官を議長に閣僚6名、有識者6名の合議体でございまして、ここで私どもの政策の基本線は決定いただく。官民連携とい

うのが情報セキュリティの場合、非常に重要ということで、行政だけの会議体ではなく、行政と有識者の方の合議体の形で政策の基本的な軸足を決定するという体制をとってございます。

私ども内閣官房情報セキュリティセンターは、この情報セキュリティ政策会議の事務局という機能も果たしていることになります。関係省庁さんや構成員で参加されている総務、経産、国家公安委員会、防衛の4大臣のほか重要インフラ、先ほども金融の話をちょっと申し上げましたけれども、金融システム防護ということで金融庁さんあるいは医療の場では非常に情報を扱いますので厚生労働省さん、あるいは交通システム、航空、鉄道、物流といった観点から国交省さんにも御協力いただきながら、政策を進めているということでございます。

5 ページ、現在の戦略の考え方ということで、ちょっと見づらくて恐縮ですが、国民を守る情報セキュリティ戦略の概要を昨年5月に今、御説明申し上げました政策会議で御決定いただいた中身でございます。概略は先ほど御説明したのですが、現状認識として大規模サイバー攻撃というのは現実の問題としてあり得る。他方で従来以上に、これは今後とも続くわけですが、情報通信技術への依存度というのは高まっている。しかも技術自体がどんどん変わっていく。先ほどのサイバー攻撃の話でもそうですが、国境をやすやすと越えていろいろな問題が起こってくる。グローバル化の進展。私たちの経済活動あるいは社会活動でも海外に出ていくという部分も含めて、グローバル化という問題がある中で、基本的な考え方のグリーンの2つの楕円ですけれども、サイバー空間における安全保障、危機管理の推進と確保ということと、経済社会基盤としての情報通信技術の利活用を促進するんだという、この2つの考え方で進めていきたいと思います。

具体的に何をやっているかということで6 ページをごらんいただいて、1 が申し上げた大規模サイバー攻撃事態への対処体制の整備ということ、もう一つは経済社会に対応した情報セキュリティ政策、経済社会基盤としてのセキュリティ政策を進めていくんだということで、2つの大きな柱があると御理解いただければと思います。安全保障、危機管理の観点からいろんな連携体制をつくるとか、実際に演習、訓練をやってみる、日ごろからの情報共有体制を強化する、こういう活動に着手したところでございます。

経済社会の基盤としての情報セキュリティ対策としては基盤の強化、国民目線に対応しなさいという御指示もございました。国民利用者保護の強化、国際連携、技術、制度という5つの柱が基盤としては掲げられている。その中の特に国民目線というところで、明示的に個人情報保護の推進というのも重要な政策の柱の要素の1つとして、掲げられているわけでございます。具体的にはプライバシー保護技術の適切な利用を促進しようではないか。技術的な対応ができる部分について、それを積極的に活用していきたい。それから、どういうレベルが望ましいか。これはまさ

に消費者庁さん、消費者委員会の所管事項になりますけれども、個人情報保護に係るガイドラインの見直しの問題あるいは国際連携の問題、こうした項目が具体的な政策項目として取り上げられるようになってございます。

7 ページ、情報セキュリティ 2010 というのは今、御説明申し上げた国民を守る情報セキュリティ戦略と、大きな戦略の中で今度は具体的に年度年度でどういう政策事業をやるかという、個々の実行予定の施策のロングリストと御理解いただくとわかりやすいかと思えます。その中で特に個人情報関連でどういう項目が取り上げられているかというのを、列挙したものでございます。

見ていただいているとおり、先ほどプライバシー保護技術の適切な利用促進、ガイドラインの見直しの話、国際フレームワークへの対応ということを申し上げましたけれども、それぞれごとにどの官庁がどういう対応を考えておられるのかということ、所管官庁さんごとに書かれているわけでございます。ガイドラインの見直しに関しては全省庁さんで進められているものと、特に総務省さんにおいては見直しをこの時点で準備をされているということだったんで、総務省さんに関しては電気通信事業における個人情報保護に関するガイドラインの見直しというのが特出しされていたり、あるいは国際的なフレームワークへの対応ということで、消費者庁さんで進められているOECDあるいはAPECの活動等々が書かれている。政策の構成としてはこんな形になってございます。

その中で私ども内閣官房としても、大きな制度的な問題に関して企画立案がミッションだということ、今日お配りしている資料でも「サイバー空間の安全性・信頼性向上のための課題等について」という資料がお手元に配付されてございます。これは国立情報学研究所の岡村先生を座長にお願いいたしまして、制度的な問題に関してどういう議論をしていかなければいけないのかという検討会を開催させていただきました。その中で特に個人情報保護に関連しそうな項目を、次のスライドの8 ページ目で3 つほど取り上げさせていただいております。中身自体は後ほどお時間があるときに、このレポートをごらんいただければと思います。

3 つと申し上げましたのは、1 つは事故が起こった場合に、被害の発生拡大を防止するための対策の実施を促す制度設計が必要ではないかという話でございます。これは私ども情報セキュリティの世界では、事故前提社会なのだ、事故をゼロにすることはできない。それをまずきちんと認識した上で、その中で何ができるかというのを考えていくようにしなければいけないのではないかと。そのときに1 つには技術的なソリューションということになるろうかと思えますけれども、暗号化技術を適切に利用することで被害の拡大防止ができるのではないかと。これを積極的に選択肢の1 つとして取り上げていくことができるのではないだろうかという問題意識を議論いただいた。これが1 つでございます。

2 つ目、クラウドコンピューティングにより海外にデータが移転する可能性があ

る。これに伴っていろんな問題が生じて来得るのではないかという問題提起でございます。エコポイントなんかでもそうですが、最近どんどんクラウドの活用、いろんな制約が高まっている中で、技術的に効率的に対応できる方法というのができてきている。他方でデータの居場所がどこにあるか必ずしもわからなかったりする。海外にある場合には海外の法制の影響を受けるかもしれないという、今まで経験しなかったリスクが起り得るということに関して、積極的に利用すること自体を云々するのではなくて、そういうリスクがあり得ることも念頭に置いて適切に評価を、リスクアセスメントなんかもしながら活用していく必要があるのではないか。そういう意識をこれからは持っていかなければいなくなるのではないか。新しいテクノロジーに伴う新しいリスク評価が必要になってくるのではないか。特に個人情報情報を扱う場合には、こうした観点も必要なのかなということで、この問題は取り上げられている。

プライバシーの問題というのも、こういうものはどちらかと言うと海外の経験の中で、いろんなアイデアが出てくるということに伴うものかとは思いますが、Privacy by Design と、システムをつくる段階からプライバシー保護をどうやっていくんだという考え方であるとか、あるいは自分自身が何をやっているかを第三者が追跡しないようにしてくれというのを主張する Do Not Track 原則、あるいは似たような観点だと思いますが、Right to be forgotten というような新しい、何を持って守るべきプライバシーとするのかというのも、これも社会的にいろんな論点が出てき得る。テクノロジーの問題だけではなくて、それは社会の需要の問題ということであろうかと思えます。

こうした問題に関しても将来を見据えて、情報セキュリティの立場からも私どもは取り組んでいかなければいけないのではないか。この辺が個人情報に関連する事項として先ほどの検討会の中でも御議論いただいた項目であり、現時点における考え方の整理というのが、この報告書の中にまとめられているという話でございます。

最初の事故前提社会、事故は起り得る。そのときに暗号化技術なんかは選択肢として使えるのではないかというのが最後のページ、事故前提社会における対策の推進というところの資料です。もうちょっと補足的に書かれています。最後これを簡単に御紹介して、説明を終わりにしたいと思います。

消費者庁さんでとりまとめられています、我が国における個人情報の漏えい事案というのは、幸い大きな目で見ると減少傾向と言えるのではないか。平成 17 年度は 1,556 件あったのが平成 21 年度は 490 件ということで、3分の1ぐらいに減ってきているというデータはあります。その漏えいがどうやって発生したのかの内訳が円グラフに書かれていまして、コンピュータウイルスに感染した結果、出てしまった、あるいは外部から不正アクセスを受けたのが、円になっていませんが、1%が不正アクセス群です。内部の人が勝手に持ち出してしまったというもの、情報処

理を外部委託する際に外部委託先の人が不正に利用してしまった、漏えいさせてしまったというのが9%、最後76%が情報が入っているPCとか、そういうものをなくしてしまったというのが76%ある。

これはなかなかゼロにするのは、現実問題として間違っなくしてしまったというのをなくするのは困難だ。なくしてしまったときに、きちんとした暗号化が図られていれば、それを仮に外部の人が入手しても使えるデータとして読めないわけですが、実際には残念ながらまだまだそういうリスクがあるのを認識した上で、きちんと暗号化をかけていたケースは3割にとどまっている。

一般的な個人情報保護のガイドラインの場合、こういう漏えい事案が発生した場合に何をしなければいけないかということで、本人への通知、一般に対する公表、主務大臣に対する報告というのを標準的なルールとして決められているわけですが、勿論積極的に二次被害を防止できるテクノロジーによる解決策というのがあるわけですが、これをうまく積極的に活用していくことができないかなというのは、私どもが現在ちょっと考えているところでございます。総務省さんが個人情報保護のガイドラインを去年の夏に変えられた際に、この部分も取り込んでいただいたケースというのがございます。

適切な技術的保護措置を講じられている場合には、こうしたいろんな対応というのを少し軽減していいのではないかという考え方を、ガイドラインに取り込むケースも出てきているということでございます。ここでも暗号と言っても簡単なパスワードで開けてしまうようなものはだめで、やはり高度な暗号化措置がちゃんと講じられてなければいけない。それから、復号鍵、暗号を解くための鍵の管理がきちんとされているかというような条件を加えた上で、これを積極的に役に立つ技術として個人情報保護ガイドラインの中に取り込んでいただいたというのが、総務省さんのガイドラインの中でも具体的な事例が出てくるようになっている。

このほかにも経済産業省さんも、ごく一般的な言い方で取組みがややされているという話は伺ってございまして、こうした活動も手段の1つとして活用していくということも、今後進めていきたいなと考えているのが現状でございます。

いずれにしても、情報セキュリティと個人情報の保護というのは非常に密接に関係すると私どもは理解してございます。先生方の御指導もいただきながら国民を守る上で、効果的な政策を推進していきたいと考えてございます。引き続き御指導よろしくお願ひいたします。

ありがとうございます。以上で終わります。

○長谷部座長 どうもありがとうございました。それでは、ただいまの御報告につきまして御意見、御質問等ございましたら、よろしくお願ひいたします。新保委員、お願ひします。

○新保委員 慶応大学の新保です。セキュリティ・インシデントへの対応について

の現状のNISCの役割についてお伺いしたいと思いますけれども、現状セキュリティ・インシデントが発生した場合に、各シーサート間の情報共有は積極的に行われていると、非常に我が国においてもそのレベルは高いと思われるわけでありませけれども、その一方で主務大臣の関与との関係において、セキュリティ・インシデントの関係において個人データの漏えいが例えば同時に発生をしているといった場合、各所の連携についてはこちらの資料におきましても、4ページの現在の連携体制というものがあるわけでありませますが、この点について現状においても個人情報保護法との関係におきましては、主務大臣の関与はあくまで各個人情報取扱い事業者の事業を所管する主務大臣が関与をするという形になっております。この場合にどの分野であるということがわからない場合も多いというのが現状としてあるわけでありませますが、この点につきましてそのようなセキュリティ・インシデントの関係において、個人データの漏えいが発生しているような事案で主務大臣の関与が必要な場合に、NISCはどのような役割を果たされているのでしょうか。

○高田参事官 情報の共有というのは、まさに何が問題だったかというのを共通の認識として意識して、それを踏まえて関係する主体が積極的な対応をとるという上で、最も大事な課題と考えています。現状で言うと、ごく率直に申し上げまして特に個人情報の漏えいが発生した案件という具体的なレベルで、どの程度まで情報共有ができていくかというのと、まだまだこれからの課題だというのが現実であろうかと思ひます。

特に私どもが重要インフラと申します場合、地方行政はまさに住民票、戸籍という個人情報のかたまりです。金融も重要インフラとして政策の対象としてとらえているわけです。現実ではこういう重要インフラ全体としても、各事業分野ごとの中でも情報共有の推進というのは政策としては推進しておるのですが、現実を言ひますと、まず事業者間で情報共有すること自体が容易ではない。これは潜在的に競合相手です。競争者ですから、事業者間で情報共有するのは容易な課題ではない。更にその上に情報システムを通した漏えいということですが、その当該事業分野だけでない領域で同じ障害、同じ経路を使って情報漏えいが発生するかもしれない。そういう意味で事業種別を超えた情報共有をさせたいと思ひているわけですけれども、なかなかハードルが高い。要するに他の事業分野は関係ないというのが、基本的には一般的な認識だという現実があるろうかと思ひます。

そういう意味では、まずは障害の発生を共有することが、まずは事業の健全な発展の上でとても役に立つのだというのを推進する上で、特に事業所管官庁さんには引き続き積極的に活動していただきたい。そのためのいろんなコミュニケーションを私どもはさせていただひている。それが1つ。

もう一つ、情報システムという汎用性の高いものを通した問題という意味で、単にそれが事業所間の観点だけでなく、分野を超えた共通する問題だという意識を高

める上で、NISC自身が積極的に活動するような努力はしたいと思っています。

具体的には各事業種別ごと、これは10業種で情報共有のための枠組みとして事業者別ごとにセプターという、大ざっぱに言うと同業者の集まりというイメージでとらえていただくといいと思うんですが、セプターの中での情報共有を図る。セプター皆さんで年1回総会をやりまして、随時幹事会ということで代表者の会合をやっています、業種を超えた各セプターからの代表者によるセプターカウンスル、あるいはその幹事会ということで、業種を超えた情報共有のための取組みを進める努力もしているところです。

ただ、なかなか簡単な課題ではなくて、個別のこういう事象に対してこういうところで情報をシェアできた結果、それに続く2度目、3度目の防止できましたよと御報告できるほど、今の時点で具体的な話ができる状態では、正直言ってないのではないかと思います。ここは引き続き努力していく、重要な政策課題を御指摘いただいたと理解しています。ありがとうございます。

(3) 日本における個人情報とデータプライバシーの乖離（産業技術総合研究所 高木浩光 主任研究員）

○長谷部座長 申し訳ありません。御意見、御質問はまだあるかと思いますが、ちょっと時間が押しているものですから、済みませんが、この論点については以上でおしまいにさせていただければと思います。高田参事官、どうもありがとうございました。

それでは、引き続きまして通信情報分野における個人情報保護につきまして、独立行政法人産業技術総合研究所からの御説明をちょうだいできればと存じます。それでは、独立行政法人産業技術総合研究所情報セキュリティ研究センターの高木主任研究員から、御説明をお願い申し上げます。

○高木主任研究員 産業技術総合研究所情報セキュリティ研究センターの高木浩光と申します。本日は「日本における個人情報とデータプライバシーの乖離」と題しまして、意見を述べさせていただきます。

少しお断りしたいのは、これは決して研究所でとりまとめた意見ではございませんで、一研究員としての意見であることを申し添えたいと思います。したがって、にもかかわらず、このような機会をいただきまして、意見を述べさせていただけることを大変感謝いたしております。

さて、この機会をいただきまして、こちらの専門調査会の過去の議事録に目を通させていただきました。第1回のところで長田委員と三宅委員から御発言のあった部分に関して、本日はお答えするという内容になっているかと思います。具体的には資料の2、3ページめくっていただいたところに書き並べておりますように、日

本の携帯電話のIDの問題を1つの例として取り上げて、日本だけで起きているデータプライバシーに関わる制度上の限界、問題点について私見を述べたいと考えております。

今日はまず最初にどういうことを言いたいのかということ、簡単に結論を述べた後、なぜそういうことになるのかという根拠を次々と挙げていって、最後にまとめたいと思っておりますが、最初にちょうど今まさに内閣官房で検討されている社会保障・税に関わる番号制度の設計の中で、ちょうど興味深い論点が出てきておりましたので、これを1つ議論の題材として話を始めたいと思います。

今、「要綱に盛り込むべき事項案」というものが出ておりますけれども、この中で「番号」に係る個人情報という用語が定義されており、この「番号」というのは社会保障と税に係る番号で、今、名前が公募されているかぎ括弧つきの「番号」という名称で言われておりますが、「番号」に係る個人情報とは、「番号」及び情報保有機関において、「番号」に紐づけられて保有され、情報連携基盤を通じた情報連携の対象となる社会保障及び税分野の個人情報という定義に文章となっております。

そうしますと「番号」それ自体も、個人情報に該当するのだろうかということに疑問に思いました。もし該当しないとしますと、実はこの番号制度では「番号」の告知要求の禁止規定を検討されているようでして、これは住民票コードの告知要求の禁止と同じように、間接罰でもって禁止するということが検討されているようですが、その際に今、検討されているという第三者機関が判断に関わるという案になっているところを、第三者機関の権限のところ「番号」に係る個人情報についてということが、必ず書かれているわけです。ということは、もし「番号」自体が該当しないのだとすると、「番号」の告知要求に関して第三者機関の権限がないということの意味してしまうので、恐らくはこの「番号」自体も権限に入れているはずだろうと思うわけです。

一方で「番号」自体が個人情報に該当するのだとなると、さまざまな疑問点がわいてまいります。例えば「番号」に数字を書き足しただけのものでも、同じ「番号」であるのかどうか。あるいは一般にある関数で「番号」を変換した変換後の番号も、やはり税と社会保障の「番号」と言えるのかどうか。これは技術論から言えばもとに戻せる、あるいは皆が共通で同じ変換を使って「番号」を使っていれば、これは言わば共通の裏「番号」ということになるので、これも同じように規制の対象にならなくてはならないはずである。しかし、逆に1個の「番号」単独で考えると、それはただの数字でしかないのに、これが法律の保護の対象になるのかなどなど、いろいろ疑問がわいてくるどころです。

すなわち、述べたいことは、「番号」自体を法で保護している原理というものは、一体何であるのか。住民票コードも含めて告知要求が禁止されておりますが、なぜ

なのかという論が欠けているのではないかと思うわけであります。

これを現在の個人情報保護法及び行政機関個人情報保護法における個人情報の定義と比べてみますと、御承知のとおり個人情報というのは、個人に関する情報であって、氏名、生年月日その他の記述等により特定の個人を識別することができるもの（他の情報と照合することができ、それにより特定の個人を識別することができることとなるものを含む）とあるわけですが、ここが「番号」と個人情報の関係に関わる肝の部分であると思いますが、では一般的な情報管理するためのデータベースについている識別子（データ管理用の番号）というのも、個人情報の「照合することができ、それにより」に当たる情報なのかどうかということが問題になるかと思えます。

そのときに果たしてこの照合する主体はだれであるのか、データ保有者による照合の可能性があるということを言わんとしているのか、それとも情報の提供先における照合の可能性を問題にしているのか、あるいは何者かだれかが照合できるのであれば、それで個人情報だということになるのか、逆に広い範囲での照合可能性がある場合に照合性があるということを意味しているのかといったところが、はっきりしていないと思えます。

なぜはっきりしていないと言えるかということが、日本における携帯電話のIDの事例でもって言えるのではないかと思うわけです。

時間も今日は少ないですので、日本の携帯電話の問題を簡単に紹介したいと思います。実は日本の携帯電話、ガラパゴス携帯などと呼ばれますけれども、スマートフォン以外の日本独自仕様で動いている携帯電話は、2008年3月末からすべてのキャリアにおいて、ウェブブラウザでどのサイトにアクセスした場合でも、共通の電話番号とは別のID、番号を自動的に本人の確認なく、送信しているという実態がございます。これが何のために必要とされたかは諸説ございますが、もともとは広告の不正クリック防止のために必要だったのではなどといった意見もあるところですが、こういう機能が2008年から使えることになったことによって、行動ターゲティング広告用にアクセス動向の追跡のために使われているという事実がございます。

もう一つ興味深いことは、お一人様1回限りということが、この番号があると実現できるという点も特徴です。例えばSNS事業者で悪質利用者の排斥のために、ブラックリスト化するためにも使われているようです。これは資料にはございませんが、モバイルコンテンツ審査運用監視機構で青少年の保護を主に目的として、「コミュニティサイト運営管理体制認定基準」といったものがつくられておりますが、この中に「事業者は会員及び非会員投稿者に対し、携帯端末を特定する個体識別番号等を取得しなければならない」という規定を当初から入れている。すなわち、これによってだれがアクセスしているか、だれというのは住所、氏名を特定している

わけではありませんが、同じ人物であるということを必ず特定しています。この認定基準は今、改正案がパブリックコメントにかけられているようですが、そちらの方では「規約違反投稿により退会処分された者が再入会することがないよう、努めなければならない」といった記述があって、個人を特定しないまま人を識別して、将来一切の出入りを禁ずるといようなことが行われるようになってきた。これはこの機能が3年前からすべての携帯電話で使えるようになったために、起きていることであると思うわけです。

実はこういった機能というのは、一般のインターネットのパソコンにはない機能でありまして、通常のパソコンのウェブブラウザでお一人様1回限りというのを実現しようとしても不可能です。これは技術的にできないのですが、それをやりたい事業者は多いようでして、携帯電話を活用することでお一人様1回限りを実現するような、例えばポイントカードの発行の際に1人1枚のみを実現するためにやっている事業者もあるようです。

実はこういった仕組みというのは欧米では決して許されない仕組みでありまして、この10年間ずっと議論になってきているところです。1999年にはインテルのPentiumⅢという、パソコンに内蔵されているCPUですけれども、このシリアル番号を認証などに使いましょうということインテル社が提案してところ、ボイコット運動になって、この機能は現在では使われていないというふうになっています。2002年にはマイクロソフトのWindows Media Playerに「一意のプレーヤーID」機能というのが追加された際にも、同様の問題があると指摘されて、マイクロソフト社は直ちにこの機能を無効にするという対応をとったということがありました。昨年にはWall Street JournalがiPhoneアプリの端末識別番号が無断送信されている事例が多々あることを報道しまして、大きな問題になりつつあるところであります。

一方、日本では携帯のIDが言わばインテルPentiumⅢのシリアル番号や、Windows Media Playerの「一意のプレーヤーID」あるいはiPhoneの識別番号に相当するものであるにもかかわらず、ずっと問題が解決されないまま10年経ってきているところです。

とは言え、全くだれも問題視しなかったかということ、そうでもないのでありまして、次のページに歴史的経緯を簡単にまとめてございますが、最初は99年にNTTドコモ社がiモードを開始した際には、公式サイトにだけIDを送るということをやっておりました。ところが、続いて現在のauに当たるところは、すべてのサイトに送信するというので、これは問題ではないかということが当時の郵政省の研究会で指摘され、2001年の総務省の「モバイルコンテンツビジネスの環境整備の方策に関する研究会」あるいは「ビジネスモデルに関する研究会」の報告書の中で、これが問題視されております。

ちょっと読み上げますと、「次世代移動体通信システムのビジネスモデルに関する研究会」の中で、当時まだ個人情報保護法は案の段階であったわけですが、この案の下では「ユーザーの個人情報を同意を得ずに、通信キャリアがコンテンツプロバイダ等に提供することは原則違法である。ユーザーIDは同法律案の個人情報に該当することから、ユーザーの同意なしにはコンテンツプロバイダ等に提供できない性格の情報である」と、明確にうたっていたわけですが。この研究会報告に対してはパブリックコメントで当時のジェイフォン東日本株式会社も、「ドコモやJ-フォンが公式サイトに限ってユーザーIDを提供しているのは、そのためである」というふうに述べており、また具体的な危険の指摘として次のようにあります。「コンテンツ提供者自身はユーザーIDを直接不当に利用するものではなくても、獲得したユーザーIDを他者に転売するなどして利益を稼ごうとするものは存在しうるし、社員管理の徹底がなされていない企業では、不心得な社員による情報の流失も十分想定される」など、当時は業界の中でも問題視されていたわけでありました。

ところが、この問題はこの研究会を最後にぱったりと全く表に、問題視されることがなくなっていまいまして、実は私、この問題について情報セキュリティの研究をしている立場から、海外の常識観との比較などしながら、これは問題がありますよということをずっと言い続けてきたのですが、総務省で2009年に「利用者視点を踏まえたICTサービスに係る諸問題に関する研究会第二次提言」ができて、昨年公表されているわけですが、ちょっとこの資料で書いてございますが、携帯のID、ここでは契約者固有IDと書いてございますが、「個人識別性を有しない」と結論づけています。すなわち、この携帯のIDを使って収集される個人に関する情報というのは、あくまでも個人に関する情報であるけれども、個人情報ではないということであるわけです。したがって、個人情報保護法の下での議論というものはできないということをして、この研究会は結論づけた上、それでも何かしらの配慮は求められるであろうとして、その行動ターゲティング広告事業者に対する自主的なガイドライン改正を求めるといようなことが行われたわけです。

その行動ターゲティング広告といいますのは次のページに簡単に整理しておりますが、個人を特定せずに識別した上で嗜好情報等を蓄積する。すなわち日々自動車のサイトを見ているような人は車を買おうとしているのではないかという推測が働きますので、そういう人向けに車の広告を表示するであるとか、薄毛を気にしているような検索をしている人は、多分かつらを買ってくれるのではないかということで、かつらの広告を出すといったことが行われているわけですが、どうやって個人の嗜好を蓄積するか、実現手段は多々あるんですけれども、「サイト内完結型」としましたのは大手ポータルサイトを運営している事業者であれば、自社内のアクセスの動向からおおむねどんな人であるかわかる。こういう利用の仕方はほぼ問題がないであろうと思います。それはすなわち本人がほぼそれをわかって使

うことになるからです。

それに対して「広告ネットワーク型」として書いてございますが、第三者 cookie を用いる方法とケータイ ID を用いる方法があります。この第三者 cookie を用いるというのは、一般の PC のウェブブラウザに搭載されている cookie 機能を使って、ここにランダムに発行した番号を記憶させて人を識別するわけですが、この方法での行動ターゲティング広告が欧米ではずっと問題視されており、特に近年も問題となっているわけです。先ほども N I S C の方からも御紹介がありましたが、「Do Not Track」というのが去年になって出てまいりました。これはどういうことかと言いますと、もともと米国では行動ターゲティングに対して嫌がる人たちも多いんですけども、一方で広告のビジネスも続けられるべきである。この両立をどうするかというときに、オプトアウトできるようになっていけばよいであろうという考え方でできていました。

しかしながら、このウェブブラウザ上でオプトアウトをどう実現するかですけれども、今までは広告事業者のサイトに行って、オプトアウトしますというボタンを押すとオプトアウトするのですが、オプトアウトした人かどうかの識別というのも cookie でします。そうするとブラウザの設定をリセットした場合とか、パソコンを買い替えたり、Windows を新しいものにした場合には、その設定が消えてしまいます。つまり、オプトアウトというのは 1 回したらずっと続くわけではなくて、ときどきもう一回オプトアウトしに行かないといけない。これはおかしいのではないかというのが米国です。ずっと問題にされてきた問題で、昨年出てきた「Do Not Track」というのは、ブラウザ自体に私はトラッキングしないでくださいということを意思表示できる機能をつけて、事業者側がそれに自主的に従うべきではないか。こういうことによって両立を図るということが行われてきているわけです。

一方、こういった議論というのは日本では全くなされていないわけでありまして。それは日本が世界標準となるウェブブラウザの開発等に関わっていないこともあるとは思いますが、しかし、一方では携帯電話のように日本だけで使われている独自のシステムもあるわけですし、これらがそういった海外の標準とは全く違う形で進化といいますか、退化していつていることがあると思うわけです。

こういうことを述べますと、「何もかもよくないということですか」といわれたりしますが、あらゆる番号を規制しようということを述べているわけではございません。このことを説明しようというのが次のページに図で示してあるところですが、実は番号にもさまざまな性質で分類することができるのではないかと。上の図ですと、左はサービスごとに別々の番号が付いている。右の図ではすべてのサービスで共通の番号が使われているということを図示したのですが、左は右に比べてプライバシーへの影響が小さいということが言えるかと思えます。

また、番号が時間的に変化することによっても、プライバシーの影響を軽減する

ことができるというのを下の図で表したのですけれども、さまざまな番号があります。空間的に広く共通で使われていて、かつ、長時間にわたって番号が変化しないというタイプのものにだけ問題がある。この赤く塗った部分が私としてはある種の問題がある番号だと思うのですが、日本のケータイIDはここに入るけれども、世界で使われている第三者 cookie というのは真ん中辺に位置していて、さほど問題ないものであろう。このように技術的に性質を分けて考えなければ、この問題をどのように政策的に扱ってプライバシー保護あるいは個人情報保護をしていけばよいかということは、結論が見えないままに議論していると、恐らくプライバシーをとるのか事業をとるのかという二項対立論になってしまって、恐らく日本では事業優先ということになってしまうだろうというのが、これまでの流れであろうと思うわけです。

類似の話題としましては次のページでございますが、ネットだけではございませんで、ICタグ、RFIDの問題も同様です。日本では小学生のランドセルにICタグを付ける実験等が多々行われておりましたけれども、2003年ごろにはこのICタグに対するボイコット運動などが欧米で起こり、プライバシー上の問題がある。すなわち町中を歩いているだけでもあちこちに観測機が設置されていれば、どの番号の人がどこを歩いているかということが記録できてしまうわけですが、これが当時経済産業省がICタグに関するプライバシー保護ガイドラインというものをつくろうとしていました。その中間報告というものが出たときに拝見したのですが、驚いたことに、「ICタグの中に個人情報を書き込まなければ、何ら問題がないことは言うまでもない」という記述がありまして、私としては大変驚いて、それはおかしいのではないかと。番号があるだけで人の追跡ができるという問題に気づいていないのではないかと。このことを、経済産業省に直接意見をしに行きましたところ、幸いにもプライバシー保護ガイドラインというものの中に、そういった記述が盛り込まれることになりました。

こういったことを踏まえて最後に意見を述べたいのですが、日本ではどうしてもこういったIDに係るプライバシーの問題を、行政として何かやってほしいということを行ったときに、個人情報保護法における個人情報に該当するか否かの判断がまず入って、該当しないとなってしまう。該当しないとなった時点で何もできないということが、ずっと繰り返されてきたように思います。

そういう中で、ときどき単発で心ある担当官の方に直接話に行くと、偶然にもICタグのプライバシー保護ガイドラインみたいなものがつくられることはあっても、これが継続して改定されているかというのと改定もされておらず、この問題に関する取組みがばらばらに行われていて、継続して行われていない。総務省の携帯電話のIDの問題に関しても2001年には問題視されていたのに、いつの間にか放置され、2008年にはよりひどい状態になった。これはデータプライバシーと言うべき

かも知れませんが、データのプライバシーの問題を継続的に、総合的に取り組んでいく機関、部局が日本の中になかったことが、このような結果を招き、欧米諸国との違いが生じているのではないかと思うわけです。

したがって、今日いわゆる番号制度の中で第三者機関がつくられるとされているところですが、これもまた個人情報保護法の改正なしに進むのであれば、結局は番号法における番号だけ特別に扱って、なぜその番号が特別に扱われなければならないものかという理由を明確にしないまま、とにかくその法律に基づいて第三者機関は税と社会保障の番号に関しては監督するようになってしまって、それ以外のケータイIDであるとかICタグの問題などに関して、第三者機関が何ら権限を持たないということにもなりかねないという問題意識を持っているわけでありまして。そういう意味ではこちらの消費者委員会の中でも、継続的にこういった問題を扱っていただくのもよろしいと思いますので、是非御検討いただきたいと思っております。

長くなりましたが、私からは以上でございます。

○長谷部座長 どうも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きまして御意見、御質問がありましたらよろしくお願ひいたします。新保委員、お願ひいたします。

○新保委員 慶応大学の新保です。

非常に興味深いIDをめぐる御報告をいただきまして、ありがとうございます。この問題につきまして高木さんがいつもおっしゃられている、いわゆる国民総ケータイ番号制という問題が、非常に大きな問題としてあるということかと思っておりますけれども、この問題につきましては、いわゆるガラパゴス携帯と呼ばれる我が国特有の携帯電話の事情に起因するものなのか、とりわけスマートフォンを除くいわゆるガラケー特有の問題と考えられるのか、それとも携帯電話一般の問題として考えられるのか。この点についてどちらかということをお答えいただいた上で、現行の個人情報保護法との関係においては、6ページのケータイID問題は個人情報保護法で解決できるかというパワーポイントの資料を御提示いただいておりますけれども、この点と併せまして現行の個人情報保護法で解決できるのかという問題について、御意見をいただければと思います。

○高木主任研究員 まず最初の御質問ですが、日本の携帯電話、ガラパゴス携帯のみ特有の問題とほぼ言えると思っております。これは具体的にはウェブサイトアクセスするときのヘッダーと言いますが、そこに番号が付いて送られるのですけれども、こういった機能を持っている携帯電話が最初に現れたのがドコモのiモードであった。そしてauのEZwebにも付いていまして、実はこれは外国企業による開発でありまして、一部ごくわずか外国でもこの機能があるものもあるようですが、調べてみますとほとんど使われていないということと、プライバシーの問題があるという指摘が、大きくはないけれども、若干あるようであります。したがって、これは

日本固有の問題である。

I P Aの方から伺いましたけれども、韓国のK I S AとI P Aが定期的に会合を持っているということで、ケータイI Dのようなものが韓国にあるかと聞くと、ないという回答があったそうです。

第二の点ですけれども、まず総務省の利用者視点第二次提言の中では、個人識別性を有しないとなっているわけですから、この結論が正しいとすれば個人情報保護法では解決できないことになるのではないのでしょうか。ただ、この結論が実は間違っているのではないかと言うことも可能だとは思いますが。

それは、そもそも民間の場合ですと「容易に照合をすることができ」というところですが、この照合はだれによってするものなのかということで、ケータイI Dを送出するのは携帯電話事業者ですが、携帯電話事業者自身はこのケータイI Dと契約者の間の対応表を持っています。これはちょうど先日の京都大学の入試不正事件で容疑者が特定されたのは、ケータイI Dを使って契約者情報を調べたと言われておりますけれども、照合可能な電話事業者がケータイI Dを他者に渡すことは容易照合性がある、つまりキャリアにとって個人情報なのではないかという見方もできるかと思えます。

ただ、渡した相手にとってはただの番号でしかないとすると、実質的に相手にとって個人情報でないものを、自分では個人情報だからと言って番号のみを渡すということを問題視するのは、何か本末転倒な感じもします。

逆に受信した側が照合可能かどうかという観点でいくと、多くのウェブサイトはその人の個人情報を持っておりませんので、ほとんど照合できないということになってOKとなってしまいますが、そうすると、そうやって集められた、言ってみれば匿名の番号といえますか、住所氏名のない番号、しかし、だれかの番号に紐づけて蓄積されたプライベートな情報の売買等が合法だということになってしまいますと、どんどん蓄積されていったものが、いずれどこかで個人情報とマッチングされるということが十分にあり得るわけで、そういう性質の情報だと思います。したがって、単に番号がやりとりされるその場だけを見て、それが容易照合性があるかということで議論しても、本質を突いた議論にはならないだろうと思います。つまりシステム全体としてこういうふうに使われている共通の番号であるということが、リスクが大きいことを意味するのですから、そういった番号単独ではなく、番号の使われ方全体を見た上で判断するというのが、理想的な規制の在り方だと思います。

お答えになっておりますでしょうか。

○長谷部座長 三宅委員、お願いいたします。

○三宅委員 最後の京都大学の不正入試、あれが一番わかりやすかったですが、12ページの日本のプライバシー保護についての私見の最後のところで、個人情報保護法の抜本的改正というのがあります。今日のお話のポイントの1つは、個人情報の

定義が個人情報保護法には容易に識別という「容易」というのが入っていて、行政機関個人情報保護法には「容易」というのは入っていない。なぜそのところに絞りがあるのかというのは、立法の当時の議論では初めて個人情報保護法を導入するから、行政機関はとにかく徹底的に調べて個人が識別できるかどうかのところで判断するけれども、新しく制度を導入するに当たっての一般法では「容易」というところで個人情報の概念を狭めにして、個人情報保護の規制をやりましょうという話だったように記憶していますが、今日のお話を聞くと容易というところによって、個人情報として本来は保護させるべきものが保護されない、法の対象の外になっている可能性があるという議論だと思います。

私はたしか病院での治験の情報、新薬を投与しての治験情報についても、たしか厚生省のガイドラインをつくる時に、治験情報を製薬会社に渡すときに、当該薬を使われた患者さんの個人情報をカットして出さないで治験情報だけが行く。これは個人情報でないのではないかという議論があったときに、そうは言っても大学病院としては個人情報として保管しているから、個人情報保護としてのガイドラインをつくりましょうという方向づけになったように思います。恐らくそういう個人情報の保護についての個人情報の定義のところはケータイIDだけではなく、ほかにも多分問題があるように思いましたので、その点は1つあると思いますが、このところで個人情報保護法の抜本的改正というのがございますが、ほかに何か、この条項はこういうふうに変えるというような、具体的な御提案などがあつたら、今日は時間が多分ないと思うので、書面等でもしお出しただければありがたいなということで、ここは発言を抑えておきたいと思います。

○長谷部座長 これはちょっと難しいお願いかもしれません。もしお考えがございましたら、別の形で御提案をいただければと思います。よろしくお願ひします。

○高木主任研究員 承知しました。

○長谷部座長 白井委員、お願いいたします。

○白井委員 最初に書かれている税と社会保障についての「番号」、いわゆる共通番号と言われているものについて、高木さんはどうお考えですか。いろいろ書かれているのですが、これは個人情報だとお考えですか。そこをお伺ひしたい。

○高木主任研究員 個人情報であるとして何らかの規制をかけるという方法と、個人情報ではないけれども、特別にこういう理由があるから規制をかけるのだという方法があるかと思います。

私は後者をするべきだと思いますが、そのためにはそのための理論づけがないのではないか。住民基本台帳法の住民票コードの告知要求の禁止は、淡々と規定が並んでいますけれども、なぜそのように設計されたのかという情報を見つけたことがない。ただ、私が理解しているのは、これはこういった番号を国がすべての国民あるいは住民につけたとしますと、これが唯一無二の番号となりますから、先ほど言

いましたようなお一人様1回限りのようなものが、どんな事業者でもできるようになる。だれなのかを知りたいわけではなくても、会員登録の際に例えば住民票コードを入れてくださいというようなことが行われるようになって、それがやがてはブラックリスト化になるということが予測されるからこそ、そういうことが起きないように告知要求の禁止を設けたのだと思います。

それと同じように、税と社会保障の番号も告知要求の禁止を設けるべきだと思いますし、実際に今のワーキンググループでもそういう案が書かれておりますが、ただ、なぜそういう規定を入れたいいけないのかという、今、私が述べたような唯一無二として保証されている番号がすべての国民に配られることによって、ほかに類のない目的外の利用方法が生まれる。これはスライド3枚目の最後のところに書いて、先ほど飛ばしてしまいましたが、今までできなかったことがあらゆる事業者あるいは個人にとってもできるようになる目的外の活用方法が生まれるので、それを問題視してだと思えます。それをちゃんと理論立てた上で、制度を設計していくべきではないかと思えます。

○白井委員 先ほど三宅さんがおっしゃった他の情報と容易に照合できる、という点です。法律にはだれが照合するか書いていないですから、だれでもいい、だれかができればいいとも解釈できるわけです。そうすると、もともと共通番号というのは国がつくるわけですから、照合はできるわけです。そうすると、ぼくは明らかに個人情報だと考えていたのですが、そうでもないのですか。そうはお考えにならないのですか。

○高木主任研究員 そうですね。たしかこれも国際的にも議論のポイントになっていたかと思えます。番号のみでパーソナルデータと言えるのかどうか。おおむねそういう見解が多いと思えます。それは結局日本の個人情報という定義で、今までやってきたところとは言葉がちょっとなじまないような気がしますので、それで最初のタイトルに戻るわけですが、日本ではその個人情報なるものと、データプライバシーなるものが、概念が乖離してしまっているのではないかと思うわけですし、勿論それをこれからはそういった番号も個人情報だというふうに考え方を切り替えるのであれば、それはそれでいいと思えますが、そうするとこれまで問題となってきたケータイIDを、総務省が個人識別性はないと決めているようなこととの矛盾が生じてしまいます。その辺りの矛盾を一体どのように解決していくのかという疑問がわくかと思えます。

○白井委員 もう一つだけ、これは高木さんにお伺いするのはどうかと思えますが、高木さんは先ほど第三者機関が番号のみを特別に扱うことになるであろうとおっしゃったと思えます。この第三者機関はまだ性格がはっきりしないのでよくわかりませんが、本当に番号のみを扱うのか、あるいはもっと個人情報を広げて扱うこともあるのではないか。ここにワーキンググループのメンバーの方もおられるので、

そこはどうかというのを、高木さんよりもメンバーの方の方がわかりやすいかなと思ってお聞きしました。

○長谷部座長 高木さんは必ずしも番号だけということをおっしゃっていたのは必ずしもないと思うのですけれども、番号に係る個人情報ということですので、関連する個人情報は第三者委員会の権限にはいるという想定で議論が進んでいる。

○臼井委員 番号に直接関わらなくても、扱うのですか。

○長谷部座長 番号に係る個人情報です。ちょっとこの点はお話すると長くなってまいりますので。

○高木主任研究員 多分、御質問の趣旨というのは、番号に係る個人情報のみ第三者機関で扱うのであるから、結局プライバシーコミッショナー会議などで議論されているようなICタグのプライバシーの問題であるとか、ケータイIDのようなものに代表されるIDの問題、行動ターゲティング広告の問題等については、日本の第三者機関では扱わないのだということになるのではないかという御質問だと思うのですが。

○臼井委員 そういう意味もあります。

○長谷部座長 そういう御趣旨だとしたら、私の方からいいですか。それは係る個人情報ということでございますから、当面はそこから出発するという想定されているのだらうと思っております。ただ、未来永劫そのままという話で想定されているわけでもないだらうと思えます。

ほかにはいかがですか。三木委員、お願いします。

○三木委員 ありがとうございます。お話をお聞きしていて、以前からある個人情報保護なのかプライバシーの保護なのかという大元の議論を、もう一回考えなければいけないのかなということを改めて認識したのと、番号の在り方はどういうふうに使われるのかによって、既存の在り方を考えた方がいいということが御指摘の御主旨だったと思いますが、それはむしろ規制の在り方というよりも、社会像みたいなものと非常に関わってくる、結構大きなテーマだと私自身は認識をしています。つまり、番号を守ればいいのかというよりも、どういう社会に番号を使ってっていくのかということだと認識をしました。

それでちょっとお聞きしたかったのが、そもそも高木さんがお考えになっている番号規制というものは、どういうことをイメージしてお考えになっておっしゃっているのかというのを、お聞きできればと思います。

○高木主任研究員 例えばまさにおっしゃるどういう社会をデザインしていくのかという観点で言えば、韓国の事例が参考になるかと思います。韓国では住民登録番号があるわけですし、住民登録番号はかなりさまざまところで使われている。インターネットの掲示板で書き込むに際しても、ユーザー登録時に住民登録番号を記入することがマストである、必要であるというふうにインターネットが発展して

きて、日本とはかなり雰囲気の違い文化になってきている。これはどちらを選択するかというのはまさに国民が判断することですが、非常に難しいことですので、全く自由にしていけば結果的にそういうふうになっていくかもしれないわけです。

そのときに住民票コードがあのように告知要求の禁止の規定が設けられたことで、どうにか住民基本台帳法改正が通ったという以前の事例を見ると、あの時点ではそういった国民番号のようなものを目的外で人の識別のために使うことは、許さないという文化なのだろうと思いますので、それに合わせた施策をとっていかないといけないと思うところ、ケータイIDの問題というのは、結果的に同じような、先ほど新保委員からあった国民携帯総背番号制のような状態が進行してしまっているということかと思えます。

一方でプライバシーの保護なのか個人情報保護なのかということで、1つ興味深い事例を最後に使わなかった資料のところを書いてございますけれども、簡単に紹介したいと思います、ちょっと驚くべきことを最近体験しました。

図書館の個人情報が流出した際に貸出履歴が漏えいしたという事件において、「漏えいした内容は住所、氏名、生年月日等であった」という発表がなされていて、借りていた本の名前も漏れたはずなのに、何でそれを公表しないのだというのをその図書館から聞いたところ、「住所、氏名等が個人情報だから」という回答だったことに愕然としました。個人情報保護法では「個人に関する情報であって、特定の個人が識別されるもの」というわけで、その個人に関するあらゆる情報を対象としているわけけれども、ただし、それだとあらゆるデータになってしまうので、特定の個人が識別されるものに限定したのだと思いますが、そういった個人情報保護法あるいは個人情報保護条例のようなやり方をしてきたがゆえに、結果として、何やら「住所氏名保護法」のような状態になっていて、本来の守るべき属性データのことに関して皆忘れてしまっている。そういうふうに世の中が今、来ているのではないか。

この下のスライドにもございますが、プライバシーに関する認定制度をやっているところの解説を見ても、「個人情報とは個人の氏名、生年月日、住所などの個人を特定する情報のこと」という、完全に誤った解説を載せている事例があるというぐらい、日本の個人情報保護法制というのはおかしな方向に世間としてはとられている。本末転倒になっていると思います。

○長谷部座長 申し訳ありません。まだまだ御意見、御質問はあるかと思いますが、相当時間が押しているものですから、この論点につきましては以上でお願いいたします。高木さん、どうも御説明ありがとうございました。

それでは、続きまして消費者から見た個人情報保護の状況につきまして、全国消費者団体連絡会からの御説明をちょうだいでできればと存じます。それでは、全国消費者団体連絡会の阿南事務局長から御説明をお願いいただければと存じます。よろ

しくお願いを申し上げます。

(4) 消費者から見た個人情報保護の状況について (全国消費者団体連絡会)

○阿南事務局長 ありがとうございます。時間がないようですので大急ぎでお話したいと思います。私は全国消費者団体連絡会の事務局長を務めております。消団連のこれまでの取組みの紹介と、3つほど提案をさせていただきたいと思います。

個人情報保護については、私の前の前の事務局長が、個人情報保護法を制定するときから、活発な参加、運動を進めてきたわけですが、この間は私の方も余りこの問題に関与せずに、ほかのことばかりやっているという状態でした、この調査会の今日のお話の問題意識に合うのかどうかちょっと心配なところがありますが、よろしくお願ひしたいと思います。

まず消費者から見た個人情報保護の状況ですが、たしかこの調査会のヒアリングの中で国民生活センターからも、今の相談状況などについてお話があったと認識しておりますけれども、私は保護の取組みが進んでいると言われておりますが、消費者から見ますと余りそのように実感できないところもあるのではないかと考えていますし、また、新しい技術などによって結構危険な状況も生まれているのだけれども、消費者がなかなかそれに気づいていないのではないかと考えています。ですから、状況としては体制の強化が必要とされていて、個人情報保護法を新しい時代に合わせて改正していく必要があるのではないかと考えております。

次のページで、まず全国消団連の紹介を少しだけさせていただきたいと思います。私どもの全国消団連は1956年に結成されました。以来、消費者の権利を確立し、守るために運動を展開してきております。現在、全国45の消費者組織が会員として参加をされております。それぞれがそれぞれの問題意識に基づいて、消費者の権利のための活動を推進をされておりますけれども、現在は総力を挙げて大震災の被災地の支援などに取り組んでいる状況です。

個人情報保護については、最初から取り組んできたと申し上げましたけれども、次のページからその紹介をしております。法律制定までに私どもは8つの意見、そしてアピールを出してきております。最初が2001年5月に出了した個人情報保護法案に関するアピールで、ここから運動が始まりました。内容についてはお読みいただきたいと思います。

次のページは、これは2002年1月に出了した修正要望、その後、緊急アピールなどについて紹介しています。さまざまなアピールを出しながら法律の制定に関わってきました。

5ページは法律が制定されたときのアピールです。アピール中で私たちは問題点と、今後強化していくべき課題について述べておりますが、こうした点については

さまざまな改善が行われてきたと私たちは思っております。

7 ページは国民生活審議会に出した意見で、これは基本方針の検証、評価、監視のときに出した意見だったと思います。利用目的ですとか、取扱い事業者の件、そして分野、過剰反応などについて意見を出しております。

次に、具体的な提案に入りたいと思いますが、個人情報保護法の改正が必要だと考えますが、3 点に意見を述べました。

まず1 点目は個人情報の取得元ですが、本人の開示の対象とすべきではなかろうかと思えます。自分の情報がどのように流通しているのか知ることができることが必要ですし、自分の情報に誤りがあった場合には訂正ですとか、利用中止を必要な範囲で行えることが重要だと思います。不適正な取得を是正していくこともできますし、違法な第三者提供というものを明確にして、これも是正していくという観点からも重要です。

2 点目ですが、法律と技術の専門家を十分に配置した第三者機関の設置が必要だということです。まず行政機関の個人情報保護制度についての第三者機関ですけれども、各省庁からの独立性が担保されている組織が、苦情の受け付けですとか各省庁の制度運用の監督を行っていく必要があるのではないかと。先ほども話に出ておりましたが、社会保障・税に関わる番号制度の検討において、第三者機関の設置が検討されていますので、その他の行政機関の個人情報保護についても、その機関が監督などを行うようにするのが効率的ではないかと思えます。

公的機関以外の民間機関における個人情報、プライバシー保護についても、これまでは主務大臣制でありますけれども、そうではなくて第三者機関で一元化して苦情を受け付けて、各事業者を監督した方がいいのではないかと思えます。国民生活センターの報告にもありますように、消費者契約の相談に付随して、個人情報の適切な取扱いが表面化する事例も非常に多くありますので、この第三者機関がその問題のある事例を把握して、積極的に個人情報の取扱いの是正を図れるようにすることが必要ではないかと思えます。

最後になりますけれども、新しいサービスへの対応が必要です。先ほどもありましたが、行動ターゲティング広告、そしてストリートビューの問題もあります。IT 技術の進化によって新しいサービスが提供されるようになってきています。確かに消費者にとって有益なサービスであるという面もあるわけですが、個人情報に限らず、プライバシーが侵される懸念が持たれておりますので、それぞれのサービスが個人情報を始め、プライバシーの保護をどのように担保しているか、各事業主体が積極的に開示をして、消費者の不安を取り除くということで、それらのサービス提供が社会的に支持されることになると思えますので、これは事業者にとってもいいわけですね。こうした事業者に積極的な説明を求めて、個人情報、プライバシー保護上に問題のあるケースについては是正を促すといったことも、第三者機関が担っ

ていくということにすればいいのではないかと考えております。

以上でございます。

○長谷部座長 時間に御配慮をいただきまして、どうもありがとうございます。

それでは、ただいまの御説明につきまして御質問、御意見がございましたら、いかがでございましょうか。三宅委員、お願いします。

○三宅委員 強い第三者機関ということで、そこで個人情報の保護に当たるべきだということですが、1点だけ御感想ですが、お伺いしたいのは、この専門委員会は消費者から見てどんなイメージで持たれているのでしょうか。つまり、1つの第三者機関で足りるのか、この個人情報全般を扱う第三者機関を番号制を扱う第三者機関とを別にするのか迷うところがありまして、頼りないから要らないと言われるのか、消費者の個人情報のためには必要だから要するというような受け取り方なのか、どちらのイメージが強いのかなという感想で結構です。

○阿南事務局長 大変期待をしております。第三者機関をここがつくってくれると、そういう提言を出してくれるように期待をしております。

○長谷部座長 臼井委員、お願いいたします。

○臼井委員 先ほどの三宅さんの関連ですが、阿南さんのイメージでは今、第三者機関というのは社会保障と税に関わるのところだけをターゲット、対象にしていますね。しかし、そうではなくてもっと幅広くあらゆる個人情報に関するところまで対象にした第三者機関にした方がいいのではないかという御意見ですか。

○阿南事務局長 はい、そうです。

○臼井委員 そうすると、今、三宅さんたちがやっておられるものとは違うわけですね。

○阿南事務局長 違うのですか。

○臼井委員 当面は税と社会保障ということになっていきますけれども、その先どういうふうになるかわかりません。しかし、これは阿南さんにお答えいただくことではないですね。

○長谷部座長 ほかにはいかがでございましょうか。三木委員、お願いいたします。

○三木委員 第三者機関に関わる部分ですけれども、今、個人情報に関わる苦情も消費者相談の窓口によくが行っているという現状があると思いますが、第三者機関というのはそうした消費者相談の窓口に行っているものも、今後はいわゆる第三者機関で苦情を受け付けて処理をしていくというものをイメージされているのでしょうか。

○阿南事務局長 今、各地の消費者センターにさまざまな相談が寄せられてきますが、そことの連動をうまくして、それを分析できるような仕組みを第三者機関の中につくればいいのではないかと思います。

○三木委員 そうしたら、第三者機関は個別の救済をするというよりは、もうちょ

っと大きなことをするものとしてイメージされているということですか。

○阿南事務局長 そう思っています。

○三宅委員 ありがとうございます。

○長谷部座長 申し訳ありません。私の司会が不手際で随分時間を超過しておりますので、この辺りにさせていただければと思います。阿南事務局長、どうもありがとうございました。

それでは、最後に原事務局長から次回の日程等について。その前に三宅委員、どうぞ。

○三宅委員 すみません、ちょっとお願いがあって先ほど言えなかったのですが、内閣官房の情報セキュリティセンターの方に、資料がもしまとまるようであれば出していただきたいと思ひまして、資料2-1の2ページで総論的には情報セキュリティ対策と個人情報保護対策はこういうものだというのは比較できますが、個人情報保護法とその他の日本におけるさまざまな法律において情報セキュリティがどうなっているかという、情報ごとの比較表をできたらいただきたいと思ひます。お考えとしてお伺いしておきたいので、宿題としてお願いしたいと思ひます。

○長谷部座長 宿題ができるかどうか、いかがでしょうか。

○高田参事官 御説明の中でもお話しましたとおり、情報セキュリティ、いわゆる法律レベルでのものはございませんけれども、こういう考え方だというものを整理して、お眼鏡にかなうかどうかあれですが、宿題として持ち帰らせていただくということで、よろしくお願ひいたします。

○長谷部座長 それでは、よろしくお願ひを申し上げます。

それでは、原事務局長の方から次回の日程等についてお願ひいたします。

《 3 . 閉 会 》

○原事務局長 御審議に御協力いただきましてありがとうございました。

次回ですが、参考資料1として今後のスケジュールをお付けしておりますが、次回の第6回は5月20日金曜日の10時からで予定をしております。連休が明けてからは月1回のペースでお願いをしたいということと、3月に予定をしておりました専門調査会を中止いたしましたので、これに代わる会議を6月にどこかで日程調整をして入れていきたいと思ひておりますので、決まりましたら改めて御案内をしたいと思ひます。

事務局からは以上です。

○長谷部座長 それでは、本日はこれにて閉会とさせていただきます。お忙しいところどうもありがとうございました。

以上