

情報保護評価サブワーキンググループにおける「しきい値」議論の経緯

- 第 1 回(平成 23 年 8 月 8 日)
事務方より、海外では、PIA の要否の判断としてしきい値評価 (PTA) を実施している旨説明。
- 第 2 回(平成 23 年 9 月 7 日)
しきい値評価を簡易版の情報保護評価とすることについて議論。
- 第 3 回(平成 23 年 9 月 30 日)
事務方提示のしきい値評価の判断基準案について議論。しきい値評価による判断は不可欠であるが、このしきい値をどのように設定するかが検討課題との意見あり。また、しきい値評価書を公表することで定量的かつ形式的な確認が可能との意見あり。
- 第 4 回(平成 23 年 12 月 22 日)
しきい値評価の様式案 (重点項目評価書、全項目評価書の様式案も含む。) について議論。実際に行政機関が情報保護評価を実施する際に統一的、体系的に調査を実施することができるということで非常によい内容との意見あり。
- 第 5 回(平成 24 年 3 月 13 日)
しきい値評価の基準について引き続き議論。
- 第 6 回(平成 24 年 8 月 30 日)
しきい値評価(重大事故)基準について議論。重大事故の定義(101 人以上) は、引き続き検討すべきとの意見あり。

第1回 情報保護評価サブワーキンググループ（抜粋）

（水町補佐）

全体フローにつきましては、参考資料2の3ページ目以降をごらんいただければと思いますが、各国ともPIAが必要かどうかを最初に判断いたします。このPIAの要否の判断に当たりましてそれぞれ特徴がございますが、アメリカ、オーストラリア、ブリティッシュコロンビア州ではしきい値評価（PTA）を実施しております。このPTAは5～20問程度の簡単な質問票に答えることで、PTAの評価報告書を作成し、それによってPIAが必要かどうかを判断するという手順でございます。

イギリスですとPIAが必要かに当たってスクリーニング判断を実施いたします。こちらのスクリーニング判断を行うことでPIAが不要かどうか、更に必要な場合にはスモールスケールPIAで足りるのか、それともフルスケールPIAが必要なのかについて判断することとなっております。カナダでは、原則的には個人情報を取り扱うシステムかどうかでPIAが必要か判断するものの、そのほか10問程度の質問に答えることでPIAが必要かどうか判断されているようでございます。

第2回情報保護評価サブワーキンググループ（抜粋）

（中村企画官）

次に、第4の情報保護評価の実施の仕組みに関してですけれども、最初に申し上げましたように関係するシステムの数は非常に多数にわたるということでありまして、2つ目ですが、これらについてすべて第三者機関の承認が必要であるとした場合、実際のフィジビリティ的な面でコストなどを考えますと、やったはいいいけれども形式的な取り組みになってしまっていて有効な評価がなされないということになりかねません。そうなるとうしろ国民の信頼の確保からは望ましくないということで、情報保護評価の目的を達成し、実効性のある仕組みとするためには広く浅く一律な情報保護評価を実施するのではなくて、情報保護評価の必要性に応じたメリハリのある仕組みとしてはどうかということにしております。

その上で、メリハリのある仕組みとする前提としてそういう事前の評価を行う必要性の高さを判断して、それに応じた仕組みとしてはどうかということ、その必要性の判断の目安として最初に申し上げた目的を参考に、事前対応を行う必要性が高いかどうか、国民の信頼を獲得する必要性が特に高いかどうか、第三者機関による実効性を確保する必要性が特に高いかどうかといったことを、そこに記載しているような項目を参考に判断することといたしまして、次のページですけれども、そういったものを一定の質問に答えていくことによって導き出すような仕組みを考えていったらどうかと考えております。

特に（3）のすぐ上ですけれども、こういった必要性、しきい値評価ということで、英語が threshold analysis なのでそういう日本語訳にしておりますが、こういった評価を行うことで簡易版の情報保護評価も実施できるような形を考えてはどうかと思っております。こうすると仮にこういったしきい値評価を行っただけでもそれなりの情報保護評価はやっている形になるので、目的の面から見ますとこういうやり方がいいのではないかと考えました。

こういった必要性判断を行うといたしまして、以下記載しております内容については参考資料9の表でお示ししておりますので、そちらをごらんください。

具体的にはしきい値評価を行うことによって、割と数問でそんなにクリティカルな問題のあるシステムではないということがわかるような質問を用意して、そこでそういったものと判断できれば、基本的には情報保護評価の対象外というものがでてきてもいいのではないかと考えました。

その上で、こういったものは数問に答えるだけという前提であれば、国民の意見を聞いたりする必要も特段薄いのではないかと考えておりますが、論点といたしまして、完全に行政機関の裁量でいいのかどうかということで、第三者機関の一定の関与ですとか、結果の公開ぐらいはさせてもいいのではないかとといったようなこともあろうかと思

いますので、この点は御議論をいただければと思います。

質問票に全部答えた結果、必要性がそれほど高くない中程度のものと評価されたものについては本当のきちんとした情報保護評価までは行わないのだけれども、先ほど申しましたように、質問票に答えることによって一定の評価を行った形にしておりますので、できればそれで一定の信頼は得られるのではないかと考えてみたものです。ただ、これはやったらやりっ放しではなくて、しきい値の評価報告書については裁量によって国民の意見をなるべく聞くようにするですとか、サンプリングチェックの形で第三者機関が審査をするようなことを考えるとともに、この報告書自体については公開をしてチェックができるというような形にしてはどうかと考えました。

(略)

(玉井座長代理)

質問ですが、先ほどもちょっと触れましたけれども、5ページの「ガイドラインの記載事項」の⑤で記載様式の中に質問票があり、8ページにしきい値評価質問票がある。この関係ですけれども、多分しきい値評価質問票の方が簡略されたものであるとは思いますが、あるいはサブセットになっているのでしょうかけれども、しかし、今、事務局で想定されているのは、これを含んで同じようなレベルのものが5ページの方の質問票というイメージでしょうか。

(水町補佐)

しきい値評価の質問票について④の実施の仕組みの中に入れ込むか、または⑤のところでしきい値評価の質問票と統合評価の質問票双方を記載することを考えております。

(玉井座長代理)

つまりどこに書くということではなくて、質問の内容というか、形式というか、趣旨です。それはレベルが違う、あるいは詳細さが違うというけれども、同じような形式を想定しているのですか。

(水町補佐)

現在想定しておりますのは、本評価の場合は参考資料2のようなこういう形なのだけれども、しきい値評価につきましては参考資料8の方に諸外国におけるしきい値評価の質問票を設けておりますが、こういった形の簡略化したものをしきい値評価では用いようと思っております。構造としては変わらないかと思うのですけれども、かなり簡略化したものと考えております。

(玉井座長代理)

わかりました。

(宇賀座長)

ほかにいかがでしょうか。

(大谷委員)

「第3 1 (1) ガイドラインの汎用性」について、「ガイドライン作成に当たっては、一般的なシステム全般にも広く活用できるよう配慮する」ということについて、この点については余り汎用性がないものをつくることそのものがよろしくないと思うので勿論賛成なのですが、ただやはり「番号」に係る個人情報の特性というか、あるいは「番号」に係る個人情報を取り扱うシステムならではの、あるいは共通番号制度についての特別法に基づいて、どうしても一般的な個人情報の取扱いとは違ってクリアしなければいけない幾つかのポイントがあるかと思しますので、ガイドラインの全体の構成などは一般的に汎用性の高いものとしつつも、例えば質問票の項目ですとか、しきい値評価のためにする判断事項の切り分けとか、そういったところについてはどうしても汎用化が難しい面が多数出てくると思います。そういう意味で汎用性にこだわるばかりに共通番号制度の信頼性に関わるような重要なポイントが見えにくくなるようなことがないようにはしていく必要があると考えております。

例えば先ほども8ページ、玉井先生から御指摘があったところなのですが、しきい値評価の必要性の高さを測る基準など、諸外国の例を出していただいています。これらの項目は一般的なものとしては非常に納得性の高いものなのですが、共通番号制度ということで見えてまいりますと、余りにも抽象的過ぎて、これをそのまま参考にしづらい面が大きいと思います。そういう意味である部分かなり特殊なものにしていかざるを得ない面もあると思いますので、限られた期間でもあり、欲張らずにここの部分は進めていただくことの方が優先するのではないかと私は考えております。

第3回情報保護評価サブワーキンググループ（抜粋）

（中村企画官）

「2 情報保護評価の実施の仕組みについて」。この部分については、前回その情報保護評価を行う必要度に応じてメリハリを付けた仕組みということを提案させていただきましたけれども、これをもう少し詳細に考えてみたものを御提案しますので、御議論をお願いしたいと思います。

具体的には、必要性の判断の仕方ですけれども、しきい値評価と前回も申し上げましたが、これをやるということですが、参考資料2ということを実際にこんなやり方をしてはどうだろうかというものをお付けしております。簡単に御説明しますと、そもそも最初に概要という欄でチェックマークが付いておりますけれども、マイナンバーを取り扱うとか情報連携基盤を利用することを確認するかどうかといったことをまず確認した上で、幾つかの質問項目がありまして、こういったものを答えていくことによって、フローチャートの対象外、中程度の必要性、高度の必要性というものが判定されるといった仕組みを想定しています。

1つ目の質問は、対象者が行政機関などの職員のみかどうかということでありまして、こういった情報については、言わば被用者と使用者の関係の内部的な情報であって、その存在や利用方法も一般的には当事者たる職員にはよく知られているということであるので、必ずしも義務づけてまでさせる必要もないのではないかと考えたものです。

ただ、論点ということで2つほど掲げておりますのが、職員本人の被扶養者ですとか、遺族に関する情報というものも含まれていると思われまして、こういったものをどのように考えるべきかということですが、こういった情報についても、その存在や取扱いについて、ある程度は職員についてわかるということに関しては、本人の情報もそんなに次元が違うものではないと思われまして、そういうことから現に行政機関個人情報保護法においても、こういった被扶養者などの情報が含まれている場合でも事前通知などの対象外となっているということでもありますので、同じように考えてもよろしいのではないかと考えております。

もう一つの論点として、ここで特に行政機関を想定しているわけですが、国家公務員共済組合とか地方公務員共済組合といった職域で福利厚生関係の法人組織ができている場合をどう考えるべきかということですが、この加入者というのは共済組合自体の職員ということではないわけではありますが、実態的な関係から見ますと、その職域単位で設立をされて、その人たちが入っているということですが、あるいは特に公務員でありますので、実際に共済組合でどういう情報を持って取り扱われているのかは、本来の職員としての情報と同じように、今は知ることが期待できるというふうにも思いますので、職員の情報と同じように考えても差し支えないといった考え方もできる

かと思っておりますが、この点は御意見があれば伺いたいと思います。

2番目の質問は、情報連携基盤の接続のルールというものが恐らくできるだろうというところで、それを前提とした質問で、そういったものにとっていない特別な方式を取るのであれば、この後の質問がどうであろうと、全項目評価をやるべきではないかという考え方です。

その他、質問3で、大事故が過去にあったかというようなことを書いております。

質問4、質問5は人数の問題でありまして、質問4はその個人情報を取り扱う人たちがどれぐらいいるのか。質問5はそこで取り扱われる情報に関わる人の数はどれぐらいかということ聞きまして、御想像のとおりかと思えますけれども、数が多いほど必要度は高いという考え方を取っております。

最後に、これに基づいて、行政上の処分行為を行うのかといった質問を設けておりまして、これは言ってみれば御提案でございますので、全体として御意見をいただければ幸いです。

ちなみに5ページ以降、御参考ということで今の質問票を実際のシステムに当てはめてみたものであります。その当てはめの対処ですけれども、第1回の資料で1枚めくっていただきますと、そこからずっと付いているんですが、情報保護評価の対象となり得る機関とそのシステムを掲げさせていただいています。

2ページ以降に、実際に事務局のものがヒアリングを行って、そのシステムの詳細をとりまとめることができたものが56ほど並んでおりまして、こういった具体的なデータがあるものについて、一定の過程を置いてやってみましたところ、5ページのところに数字がありますように、対象外が7で、情報保護評価が重点項目は必要性が中程度というのが3で、必要性が高いものが46ということになりまして、かなりちゃんとした評価をやるというものが多結果になっているのです。

これは事情もございまして、あくまで事務局の方で取り急ぎ個別にヒアリングを行うことができた機関でございますので、当然、全国レベルの組織であるなどの理由で、もともと関係者の数が大きいようなシステムになっておりますので、恐らくこういう結果が出たのだらうと思えます。

現にこれもすべてを網羅できておりませんが、そのほかにもある程度の団体について、この別紙2という情報保護評価の対象となり得る機関の加入者数等ということで、詳細までは調べるに至らないんですけれども、この加入者などの数を一つの目安として、これもざっと調べられる範囲で調べていましたところ、先ほどの考え方でやってみた場合に、この対象人数というところで、かなり対象が重要度が高いというのではなくて、中程度というところに該当すると思われる例がかなり出てきておりますので、実際には割合的にすべての評価をきちんとやるというものが山のように出てくる基準ではないだらうと考えているところであります。

それでは、論点の資料3に戻っていただきまして、こういった形で必要性の判断をし

た後、その必要性に応じてどうやっていくかということについてですが、参考資料3の方も適宜ごらんいただきながら、お聞きいただければと思います。

10 ページで、対象外となったというものについては、対象外ということですので、情報保護評価はそれ以上は基本的にしないという考え方にしております。実際にこの質問票も言ってみれば、簡単に事実を答えるだけで弾き出されるものになっていますので、国民の意見を聞くとか第三者機関の審査をすとか、そういったことも特段必要はないのではないかと思います。ただ、そういうしきい値評価をやって対象外としたという、そのことについては公開をしたかどうかということもございますので、この点については御意見をいただければ幸いです。

次に、必要性が高くない中程度であると評価されたものについては、前回はしきい値評価をやると簡単に評価もできるというような形でつくるという御提案にしておりますけれども、ここはやや軌道修正をいたしまして、重点項目評価ということで、言わば簡易な評価というものをやることにしてはどうだろうかということでもあります。

この簡易な重点項目評価については、各機関はいわゆるパブリック・コメントなどの手法で広く国民の意見を求めることを自らの判断でやるというようにしてはどうか。また、第三者機関の方では、重点評価に対して、すべてではないけれども、何らかの手法でサンプリングを行って、幾つかのものは評価をすといったことにして、最後に重点項目評価とその前提となるしきい値評価をやったことこの公開は、すべて対象となったものをやるという案を考えていましたので、特にこの参考資料3で△と書いてあるところについては、御議論をいただければ幸いです。

最後に、必要性が高いとされたものにつきましては、当然自らがきちんとした情報保護評価をやって、第三者機関の審査もすべてやって公開もするということでもありますけれども、この国民の意見を聞くことに関して、一つの考え方としては、第三者機関が専門的な見地からチェックをするので、例えば必要性が高いものと同じように裁量でやればいいという考え方もあるかと思いますが、プライバシー保護のことを考える必要性が高いシステムなのであれば、全権国民の意見を聞いた方がいいとも考えられると思いますので、この点についても御議論をいただければ幸いです。

その他、細かい部分で前回から変更している部分もございますが、基本的な発想を変えてはおりませんので、質問等がありましたらお答えしたいと存じます。以上です。

(略)

(新保委員)

では、9ページの「(2) 必要性の判断」、しきい値評価について、まず1点ございます。しきい値評価を行うことは当然必要になってくると思いますので、各国におきましても、まずはしきい値評価を行って、本当に情報保護評価を実施すべきかどうかを判断

することは不可欠であります。しかし、このしきい値をどのように設定するかによって、具体的に対象になる、対象にならないシステムが出てくるわけでありませぬけれども、問題は対象外となった場合と必要性が高くないと判断されて、重点項目評価を行うという場合に、果たしてその評価、その判断が適切であったかどうかをどのように確認するのかという点にあるかと思ひます。

例へば既にこの点について評価を行っているものとしては、住民基本台帳ネットワークに係る地方公共団体の評価が行われているわけでありませぬけれども、自治体が行っているこの評価の項目については、現在、既に行っているということだけでなく、今後実施するという項目についても OK が出ているという状況がございますので、例へば安全管理措置について、必ずしも現段階で完全に行われていると限られない場合であっても、今後実施することで対応は OK という評価になっているわけでありませぬ。

この点について、すべての項目を例へば第三者機関が確認することは不可能でありませぬ。また、主観的にその評価を行ったことについては、それを主観的に評価することも不適切ではありません。そうなりますと、先ほど自治体の取組みといたしまして、オンライン結合に係る場合に、審査会・審議会がその際に関与をするという仕組みの御紹介があったわけでありませぬけれども、例へばこのような仕組みと連動して、条令における個人情報保護審議会・審査会等の判断において、結果的にこのしきい値評価において、対象外または必要性が高くないと判断されたものについて、審議会が関与することも案として一つあるのではないかと思ひております。

これがまず 1 点目でありませぬけれども、ここで一度区切った方がよろしいですね。

(宇賀座長)

今、しきい値評価との関連で御意見をいただきました。こうした形で分類すること自身は妥当であるけれども、分類そのものが適切に行われているかどうかについて、何らかのチェックの仕組みが必要だろうという御意見です。

それについて、ほかの委員の方はいかがでしょうか。

(玉井座長代理)

ただ、今日の参考資料 2 で出ている案ですと、かなり機械的。例へば取り扱う人の数とか対象になる人の数、それ以前にこのナンバーシステムを扱うかどうか基本的なふるいになっていますけれども、多分意図としては主観的なものが入らないで、非常に単純と言へば、単純な基準でしきい値を決めようということなのではないかと思ひますが、どうでしょうか。

(水町補佐)

事務局といたしましては、玉井先生の御指摘のとおり、参考資料 2 のしきい値評価基

準については、簡単に評価できるような、質問に応えるところで迷わないような質問を当初案としております。

(宇賀座長)

ほかにかがでしょうか。10 ページに書いてありますしきい値評価報告書を公開すべきかということですが、これは公開するべきということですね。

(新保委員)

はい。しきい値評価については、これは定量的な形式的な確認が可能かと思いたいで、公開しても差し支えはないかと思いたいます。

(玉井座長代理)

今のしきい値評価に関連して、細かい話ですが、11 ページに、必要性が高くないものに関しては、サンプリングチェックを行うという案が載っております。私の理解は、サンプリングは評価報告書が出されて、そのうちの幾つかをサンプルして、第三者機関が評価をすると思いたいましたけれども、ここに書いてあることはしきい値で出たことと、後でそがないかを書いてあるということは、このサンプリングをするのは報告書が出てからではなくて、しきい値評価の段階でやるというふうにも読めるんですが、その辺は事務局の意図を伺いたいたいと思いたいます。

(水町補佐)

わかりにくい記述となっておりまして、申し訳ございません。サンプリングチェックにつきましては、重点項目評価を実施した後に、重点項目評価報告書を各機関の方で作成します。それを第三者機関の方で幾つかの報告書を選んで、サンプリングチェックするというふうにご考えております。

11 ページ目の「また」以下の段落につきましては、サンプリングチェックから外れたもの、第三者機関がチェックしない重点項目評価報告書につきましても、報告書が出たオンタイムでは第三者機関は審査をしないものの、そういったものについても何らかの問題か後で発生した際に、重点項目評価報告書を見ていくことで、問題の解決の糸口となるのではないかという記載としております。

(玉井座長代理)

そうしますと、ここに書いてある何らかの問題というのは、例えばどんなようなことが想定されているのですか。

(水町補佐)

例えば、漏洩事故等が起こったり、具体的な問題が発生した際に第三者機関が一般的な立入調査権限等に基づいて、調査を行っていくかと思えますけれども、その際に立入調査をして、すべてを網羅的に調査するという前に、まずこの重点項目評価を確認することで、機関のプライバシーに対する考え方やそのシステムがどうなっていて、どういうプライバシー保護の取扱いがなされているかを確認するために、この重点評価項目所が有効な手段になるのではないかという意図でございます。

(玉井座長代理)

意味がわかりました。

(宇賀座長)

ほかにいかがでしょうか。

(宮内委員)

この質問4と5につきましては、実は4が先にあって、その結果で5をやるかどうか決まっておりますが、実際にはこの2つの質問の内容は、マトリクス的に考えるべきではないかと私は思います。

特に今の人数が適当かどうかという論点は勿論あろうかと思えますけれども、例えば現在の枠組みでいくとしますと、対象人数が1,000人未満のときには、取扱職員が1万人以上かどうかで、対象外と全項目と分かれてしまうのは必ずしも適当ではないかもしれないと思うようなところがまずございまして、ここはマトリクスでもう少し分析していく必要があるかなと思っています。

ただ、現在はまだ全項目といっても、その全項目が何か、重点項目は何かというのは固まっていない状態ですので、そちらが固まった段階でもう一回マトリクスで見て、どういう内容が適当かをもう一回見直す必要があるのかなと考えております。

(宇賀座長)

ありがとうございました。ほかにいかがでしょうか。どうぞ。

(新保委員)

今の宮内委員の御指摘に全く同感でありまして、後ほどお話ししようと思っていた点ですけれども、このしきい値評価の参考資料2の項目については、これでそもそもよいかということについては、本日の検討会で結論は恐らく出ないと思われまますので、とりわけ各項目について、精査が必要と思う点だけ意見を述べさせていただきます。

今、御指摘のあった数値でありますけれども、質問4の職員外部委託先第三者提供の人数の1万人以上であれば、情報保護評価全項目を実施するという一方で、対象人数が

例えば1,000人未満であれば対象外とするということについて、現行では個人情報保護法では5,000という数字があって、行政機関個人情報保護法では1,000という数字がありますので、この点の整合性が取れていないことから、どこでしきい値をまさに置くかということが問題になるわけであります。

1つ例を申し上げますと、今回の情報保護評価はプライバシーという観点からの評価を行うという観点からしますと、例えば1,000人未満の自治体で全住民が対象となる情報システムがある場合には、これは当然プライバシーへの影響があると考えられる場合もあるわけであります。ですから、必ずしも対象人数が1,000人未満であれば、対象外という一律にしきい値評価で区切ってよいかということについては、今後検討が必要と思われます。

第4回情報保護評価サブワーキンググループ（抜粋）

（中村企画官）

資料2から4という形で実際にどういう報告書に記載してもらおうかというものを示しております。

まず、資料2の しきい値評価のための事実報告書 ですが、これは情報保護評価の判断レベルを決定するための報告書ということで、3ページで流れを書いています。この流れにはまるように1ページ、2ページ目の様式をつくっています。

考え方としては、これまでに何らか取扱いに問題があったかどうかとか、その関係する職員など取り扱う人の規模、それからその情報としての対象の人数はどれぐらいかといった意味の規模、こういったものを判断基準として、一応機械的に、このしきい値評価のみで終わるもの、重点項目評価にいくもの、全項目評価にいくものというものを振り分けられるような形でつくっております。

詳細な質問項目としてどういうものを設けたということについては4ページと5ページに整理をしておりますが、説明は省略させていただきます。

（略）

（新保委員）

情報保護評価の報告書の記載事項について、全項目評価の資料4を参考に幾つか意見を述べさせていただきたいと思います。

今回、非常に細かく報告書の記載事項の案を策定していただきまして、実際に行政機関が情報保護評価を実施する際に統一的、体系的に調査を実施することができるということで、非常によい内容だと思います。けれども、全体についてというよりも、細かい点について、今後事務手続上このような報告書を作成するとき、従前の行政機関個人情報保護法に基づく個人情報ファイル簿の届出の項目などとの整合性を確保することも当然必要になってくると思いますので、この点についてまず1つ目に用語について「収集」、「取得」なのか、「保存」なのか「保有」なのかとか、原案ではまだ必ずしも平仄がとれていない部分があると思います。

第5回情報保護評価サブワーキンググループ（抜粋）

（新保委員）

検討事項につきましては、今回の資料3並びに添付資料のしきい値評価の評価書の記載についてであります。こちらにつきましては、しきい値評価のとりわけこのフローに基づくしきい値評価の実施の内容についてであります。1点目の引き続き検討を行うべきではないかと思っている点であります。今年度は諸外国の調査も含めてこの素案についての検討を継続していただけるということでもありますので、より細かく精緻なしきい値評価の基準等も最終的なとりまとめに向けて検討が必要ではないかと思っております。

この点につきまして、第3回の委員会議事録を御確認いただきますと、私の発言といたしまして、情報保護評価のしきい値評価について例えば対象人数が1,000人未満であっても対象外という形で一律にしきい値評価で区切ってしまってよいかということについて、今後検討が必要という意見を述べさせていただいた結果、原案としては質問項目での記載事項につきまして、「なお 社会保障・税分野の情報は概して機微性の高い情報であるため、情報の種類を判断基準とするのは困難であると考えられることから、情報の量のみを質問項目とした」という形で現在の案になっております。

つまり、しきい値評価においては特定の機微な個人情報を取り扱うか否かといった文字どおりのプライバシーに該当する情報を取り扱うかどうかということについては、しきい値評価の基準にはなっていないわけであり。その理由は、今、申し上げたとおりということでもありますけれども、そうしますと、今後の検討に当たって、この 基準についてかなり厳密にしきい値評価の基準を定めておくということやその解釈についても厳密にしておく必要があるのではないかと思っております。

具体的には、漏えい等に関する重大事故という形の基準がございますが、この重大な事故というものはどの範囲の事故を含むのかといったことについては、現在では余り明らかになっていない点であります。更に、重大な事故だけではなく、軽微な事故も含めて事故をどの範囲の事故を認識することができるのかということについて、現状、事故であっても認識していないという場合が多々あるわけであり。

例えば具体的に自治体における事例として、後ほど自治体の部分の論点も出てまいりますけれども、某システムインテグレーターが納入した図書館システムにおいて、そのシステムをかなりの図書館に同じシステムを納入した結果、委託先において本来その委託先のシステムインテグレーターが確認すべきシステムの個人情報の残存状況等について確認を怠った結果、結果的に納入先にも元の発注元の個人情報、貸出記録とかですが、そういったものが結果的にそのまま引き継がれて納入されてしまったという事案がございます。

これはシステムインテグレーターとしてはとんでもないことをしでかしたわけであ

りますけれども、こういった事案について納入先の自治体などがそれを個人情報の不正な保有であるとか漏えいであるとか、そういった問題として認識していないということが既に報道されているわけであります。

このように、認識していないという場合には、結果的に漏えい事故などを起こしていないということになってしまうわけですから、結果的に正直な組織のみが対象となってしまう、又はそのような漏えい等についてのきちんとした知見を有する組織のみがこの部分について確認するということになってしまいますので、そうしますと、逆にいうと何も対策がとられておらず、漏えいさえ認識していないような組織にはについては漏えいを発生させたことすら認識していないというおそれがあります。

そうすると、ここについては発生させたか、いいえということになってしまう可能性がある。

特定個人情報を取扱う職員の数につきまして、原案では職員、外部委託先、第三者提供先など合計人数が1万人以上ということになっているわけでありますが、この点につきまして、人数に比例して漏えいのリスク、不正利用のリスクなど、つまり人が多くなれば悪いことをする人も多くなるだろうということの思想に立ってこの人数になっているわけでありますけれども、昨今の個人情報の不正利用、漏えい等の事案を見てみますと、必ずしも人数が多い、大規模な組織であるからといって漏えい事故又は不正利用が多発しているということではないという状況があるわけです。ですから、こういったことについてかんがみますと、この1万人という数字によって、一律にそこを切ってしまうと、少人数の規模の事業者であって大量の個人データを取扱っているような第三者提供先とか委託先も含めて考えても、結果的にこの人数で切ってしまうと漏れてしまうという部分もあるのではないかと。

よって、この基準については、そもそもこの基準を入れるかどうかということ、並びにこの基準も従業者なのか従業員なのかということによっても数字が変わってくるという論点がございます。

更に対象人数についても、現在では1,000人未満10万人以上という数字をそれぞれ挙げているわけでありますが、これについても、恐らく引き続き検討すべき事項かと思いますが、そのときにカウントの仕方についても、この点はまだ十分に詰めていない点であります。現行の行政機関個人情報保護法の本人の数が政令で定める数というものは1,000人に満たないものという形になっていますけれども、この点につきまして、現行の法解釈で大きく3つこのカウントの方法が分かれているわけです。

1つは、個人情報としてカウントする場合。どういうことかといいますと、生存する個人に関する情報であって、個人識別性があるもの。なお、行政機関について容易照合性がないので、識別できるものはすべて個人情報となります。よって、民間部門とは異なり容易照合性がないものも個人情報ということになりますと、非常に膨大な量の情報が個人情報としてカウントされる。

2番目は、保有個人情報という形にくくった場合には、行政職員が職務上作成し、又は取得した情報ということ。

3つ目は、個人情報ファイルに記録される個人情報、これを行政機関等個人情報保護法では記録情報と呼んでいるわけでありますけれども、恐らくここにいう対象人数は記録情報、行政機関等個人情報保護法にいう本人の数が1,000人に満たないという場合の記録情報に該当するものと想定されますが、そうしますと、1つ問題として個人情報ファイルの通知公表義務の対象外として1年以内に消去されることとなる記録情報のみを記録するものについては、個人情報ファイルには記録しない個人情報となりますので、作成、通知の義務が発生しません。

そうしますと、たとえ対象者数が10万を超える場合であって、個人のプライバシーに与える影響がある情報であっても、記録情報に該当しないということになりますと、自動的にこれは対象外になってしまうのではないかとということで、結果的に10万という数字を持って1年以内に消去されることとなる記録情報のみを記録する場合には、対象外になってといった可能性もあるということで、以上を踏まえまして、こちらのしきい値評価につきましては、今後、この個人情報保護検討ワーキンググループにおいても原案としてこの部分について御提案をいただくということにはなるとは思いますけれども、今、申し上げた点も含めて引き続きこの点については より精緻なしきい値評価を行う上での基準の設定、解釈については引き続き検討が必要な部分もある ということについて、確認させていただきたいと思っております。

(略)

(水町参事官補佐)

新保先生に御意見いただいたとおり、まだしきい値評価の方は固まっていない部分もございますので、来年度以降、より精緻化する方向で検討していきたいと思っております。

ただ、しきい値評価で重点項目評価又は全項目評価を実行しないでよいと判断されてしまいますと何も評価しないということになってしまいますので、プライバシーインパクトがあるものを重点項目評価又は全項目評価で捕捉できるようなしきい値にしたいと思っておりますので、例えば従業者又は従業員という点につきましては、従業者と考えていきたいと思っておりますし、対象人数についてもよりプライバシーインパクトがあるものがきちんととらえられるような方法でカウントしていきたいと考えております。

(宇賀座長)

ほかの委員の方、いかがでしょう。

宮内委員、どうぞ。

(宮内委員)

このしきい値評価の評価書というものは、一応公開することが前提となっているというものだということですが、マイナンバー法案の15条1項のところによりますと、この評価書を公示するに当たって次の各号に書かれる事項を評価したと書いてあるわけですが、これが1号から7号が書いてあって、これがフローチャートに入っていないということは、法案の趣旨からすると漏れてしまう可能性もあるのかなと思っているのです。

つまり、ここに書かれていることはフローチャートに何らかの形で影響するというのが本来ではないかと考えるのですが、そういう意味で、今のフローチャートは最終形ではないと思いますけれども、この1～7号はそれなりに判断が入ってくるという形で考え直した方がいいのかなと思います。

(水町参事官補佐)

15条1項の各号につきまして、15条自体が全項目評価を念頭に置いた条文となっております関係で、しきい値評価というよりは全項目評価の内容となっております。

ただ、先生がおっしゃられるように、しきい値評価と密接に関係してくる部分も書いてございまして、特に1～3号等はしきい値評価に密接に関係してくるものと思われませんが、全項目評価の中でこの1～3号につきましても、従業者の数を必要最小限度に絞っているかですとか、個人情報ファイルの取扱い状況を踏まえて、事故の再発防止策をどのようにとっているかということや全項目評価書の中で記載させることとしておりますので、しきい値評価と関係してくる部分につきましても、その対策をどうしているか、そのインパクトをどう軽減しているかということや全項目評価書で書かせるという想定のある条文となっております。

第6回情報保護評価サブワーキンググループ（抜粋）

（中村参事官）

まず、しきい値評価基準についてであります。現在、中間整理におきまして、しきい値の評価質問項目案が大きく5つありまして、情報提供ネットワークシステムの接続規定に則るかから始まって、あとは重大な事故を1年以内に発生させたか、取り扱う職員の数がどれぐらいか、対象人数はどれぐらいか、どれぐらいの個人情報を集録しているかということ。それから、特定個人情報は行政処分の対象として用いられるものなのかどうかといったことでございます。

このうち 重大な事故というものについて、どれぐらいのものを重大事故と扱うかを改めて考えてみた ものが「②重大な事故について」でございます。この重大事故という質問項目を設けた私どもとしての趣旨でありますけれども、総論の2つ目の〇に書いてありますように、何らかの重大な事故を発生させた場合は、それが報道などを通じて国民の皆様方にも知られるところとなり、その情報保有機関に対して国民の懸念の大きくなることが考えられますので、特定個人情報ファイルの取扱いについての透明性を増して、国民の信頼を確保するという目的からして、きちんと評価を実施していただく必要が高まるのではないかと考えたわけであります。

漏えい等の事故の実情を簡単に調べてみたのが(2)ですが、2ページや3ページに総務省がとりまとめております行政機関などの事故のデータも載せておりますけれども、大体緑で塗ってあるところが数が相対的に多いものであります。全て申し上げますけれども、案件の種類としては誤送付、誤送信や紛失というものが多くて、規模から申し上げますと表2なのですが、大部分が50人より少なく、5人以下でも4分の3とか8割、それぐらいになります。通り相場としては、ごく不注意で少ない人数の方の情報を何らか漏らしてしまったというものが大部分と受け止めております。

また、ちなみに民間も含めた例も4ページに出ておりますけれども、このような例を見ても不注意のたぐいが多いし、こちらは500人以下で切られておりますが、非常に大規模な流出の例は少ないことがうかがえるかと思っております。

こういったものを見ながら検討をいたしました。4ページの一番下から5ページにかけてですけれども、めり張りのある仕組みをそもそも考えていた中で、あえて全項目評価をやらせる基準ということで重大事故を考えたわけでございますので、こういった実状を踏まえてどういったものがプライバシーインパクトが高いと思うかということなのだろうと思っております。

具体的にこうした視点から考えましたのが5ページの真ん中の枠囲みでありまして、当該機関の職員以外の特定個人情報を含むものを漏えいしていたものであって、なおかつ、その 職員以外の情報の本人とされる者の数が101人以上と考えました。101人ということに関しては何か客観的な基準を申し上げるのも難しいところもございまして、

通常、一般国民の目から見て3けたのレベルになるような事件が起きるとするのは、単なる不注意とかそういうことを越えて、その機関に何らかの構造的な問題があると思われるてもおかしくはないレベルではないかということで設定をさせていただきました。

(略)

(玉井座長代理)

極めて単純な質問ですけれども、101人以上とした場合に前の方に件数のデータがありますが、何件ぐらいが該当するのですか。

(水町参事官補佐)

こちらに付けさせていただいている表は、一般の個人情報に係る表として、行政機関個人情報保護法における個人情報と独立行政法人等個人情報保護法における個人情報と、個人情報保護法に基づく個人情報、これらの表ですので、このうちどれが特定個人情報になるのかという割合が現時点では判明しておりませんので、何とも確定した回答は申し上げられません。

ただ、一般の個人情報であれば例えば3ページの表をごらんいただければ、行政機関であれば101人以上が平成22年度ですと3.8%、1001人以上が1.4%ですので、合計5.2%。独法であれば、2.5%プラス1.3%ですので、3.8%と考えられます。

(玉井座長代理)

わかりました。

(宇賀座長)

ほかは、いかがでしょうか。

(新保委員)

しきい値評価基準の重大事故については、以前から基準をどうするかということについて 事務局も相当悩まれて101人という数字をお考えになったと思いますけれども、引き続きどういう基準にするかは継続的に検討が必要な事項だと思います。なかなか101という数字についても今、3けたという御説明がありましたけれども、「3けた(みけた)」だと重大事故を「見つけた(みつけた)」みたいに、その根拠は3けたという根拠ですということになってしまうと、説得力の点ではどうしてこの数字なのかということについて、なかなか説明が難しい部分があるかと思えます。

この点につきまして、引き続き検討が必要と申し上げた理由は、例えば現在、諸外国におきましてもセキュリティーブリーチ・ノーティフィケーション、情報漏えいに当たっての通知についての義務づけが進んでおります。米国では現在46の州まで拡大して

おりまして、46 の州及び4 地域が既にセキュリティーブリーチ・ノーティフィケーションの法律を制定しております。EUにおきましても、EUの個人データ保護規則が現在、案として出ておりますけれども、こちらにつきましても同じく通知を24時間以内に行うことと併せて課徴金の額も定められております。

この基準については次第に基準が明確になりつつある部分でありますけれども、ここで私から意見としては、今の動向としてどういう傾向にあるかといいますと、基準は情報の質と量という観点から判断を行う傾向がございます。質ということについては細かくいろいろな例がありますけれども、例えば非常に早い段階からノーティフィケーションを導入したカリフォルニアの事例などを見ますと、カリフォルニアでは暗号化されたデータは除外されている。日本では実は暗号化されたデータであっても、経済産業分野における個人情報保護ガイドラインを始めといたしまして、各省庁の個人情報保護ガイドラインにおいても、解釈上、暗号化されたデータであっても個人情報であると解釈しています。厳密には個人データまたは個人情報に当たるということで、たとえ暗号化されていても我が国の場合には総務省などの処分事例を見ていただいてもおわかりのとおり、個人データの漏えいに当たるという判断になっております。

一方、諸外国においてはこのように暗号化されたデータについては除外をするという、質の面から例えば除外をしている例とか、その一方でマイナンバー法の大綱におきましても一番最後の行には「情報の機微性に応じた特段の措置」ということで、医療分野について現在、医療情報の取扱いについては法制を番号法と併せて整備するという、特段の措置について検討を行っているわけでありまして。

そうしますと、私の提案といたしましては機微性と見読性、こういった観点から必ずしもそのデータが漏えいした場合に機微性が低いのではないか、見読性がないのではないかということも、これは今後、検討の対象に含めて考える事項ということになるかと思えます。ただし、今回はあくまで情報保護評価のしきい値評価基準における重大事故という判断基準になっているわけでありまして、この点について対象情報が個人情報と特定個人情報では事情が違ふということなのです。

つまり、今回のカウントをするに当たっても個人情報、厳密には個人情報保護法にいう個人データ、行政機関等個人情報保護法にいう保有個人情報、これらについては氏名とIDなどの非常にシンプルな情報で、たとえIDが1万件漏えいしてもそれほど大きな影響はないわけですが、その一方でセンシティブ性が非常に高い情報もある。個人情報については、非常に幅が広いという面があります。

一方、特定個人情報、つまり、マイナンバー法案にいう特定個人情報については社会保障、税分野における情報となりますので、その多くは機微性が高く幅が非常に狭い情報になるわけでありまして。ですから、前の個人情報が1件漏えいするのと後者の特定個人情報が1件漏えいするのではプライバシーインパクトは全く異なるということなのです。

ですから、この点からいたしまして、件数のカウントについても、個人情報と特定個

人情報では事情が違うということについても当然、考慮が必要になってくるかと思いません。この点については、諸外国の動向と情報の質と量についての、あくまでこれは基準といっても1件ずつ厳密にこれは個人情報か、特定個人情報かを区別するということまでは必要はないと思います。たとえ1件でもシビアな情報の漏えいではないかという場合には、それも含めるということも何らかの基準として加えることはできないかと思っております。

ただし、最終的な課題としては現行の法制度の範囲内では、私が申し上げた基準、情報の質と量については現行の個人情報保護法では全くこの点については基準はございません。併せてマイナンバー法案も含めて、現行の法制度においてこの判断をする基準はないわけであります。ですから、最終的にはこの点も含めてこういったことについては個人情報保護法本体の改正によらなければ適切に判断することはできないと考えております。

(宇賀座長)

ありがとうございました。

資料5につきまして、ほかにいかがでしょうか。

(水町参事官補佐)

ちょっと補足させていただければと思います。

新保先生がおっしゃられたとおり、特定個人情報については税、社会保障分野の情報であるということと、特定個人情報であるからにはマイナンバーが入っているということ。これらのことから、特定個人情報は、全て機微性の高い情報であると考えております。また、暗号化された情報であれば、仮に漏えいしてしまった場合でも、たしかに平文が漏れるよりは、という点もございますので、検討させていただければと思います。

101人というのは、確かになかなか基準として出すのは難しいところもございますが、勿論、そういった機微性の高い特定個人情報が1件であっても漏えいするのは大変な問題であると思います。ですので、現行の行政機関個人情報保護法等でも、またマイナンバー法でもそういった事案があれば、総務大臣なり委員会に知らせて、施行状況調査でこういう事案がどの程度あったというのを一般に公表しているところです。1件でも非常に重大な問題であることを認識しております。

ただ、ここにおいて 101人としたのは100人以下のものが重要ではないという趣旨ではなくて、しきい値評価では、重大事故に該当すると、ほかのしきい値評価の質問項目を満たすか満たさないかを問わず、重大事故に該当してしまえば必ず全項目評価を実施するものですので、これを起こしたという1点だけをもって全項目評価を実施するほどの必要性があるインパクトが強いものという意味で101人にしておりますので、その点だけ補足させていただきました。

(宇賀座長)

宮内委員、どうぞ。

(宮内委員)

今、言及されました暗号化をどうするかという問題はありますけれども、確かに経済産業分野におけるガイドラインにおいても暗号化されていても個人情報であるとされていますが、ガイドラインの中身につきましては高度な暗号化がされている情報の漏えいについては扱いをいささか違えているという面もございますので、この辺りも御参考にされたらよろしいのではないかと思います。

以上です。

(宇賀座長)

ありがとうございました。

ほかにいかがでしょうか。

大谷委員、どうぞ。

(大谷委員)

非常に細かな話なのですが、過去1年間の特定個人情報を含むものの漏えい事案ということになりますと、最初の個人情報保護評価のときにはだれも特定個人情報はまだ扱っていない段階ですので、経過措置的に情報保護評価の重大事故基準は最初の段階では何か読み替えをしていかなければいけないだろうと思ひまして、細かいことですが、言い添えさせていただきました。