参考資料２

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 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が、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○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とれども、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。全て申し上げませんけれども、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、規模から申し上げると表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が、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すが、

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いうのは、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でして、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（みっけた）」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います。
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てみますと、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ことで、特段の措置について検討を行っているわけであります。

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います。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すが、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うということです。

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けれども、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す。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す。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ところ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けれども、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いまして、細かいことですが、言い添えさせていただきました。