情報保護評価サブワーキンググループ
第２回議事録

内閣官房社会保障改革担当室

内閣官房情報通信技術（ＩＴ）担当室

第２回情報保護評価サブワーキンググループ

日　時：平成 23 年 9 月 7 日（水）14:00～16:00
場　所：都道府県会館 4 階 402 会議室

【出席者】

宇賀　克也	東京大学大学院法学政治学研究科教授
大谷　和子	株式会社日本総合研究所法務部長
新保　史生	慶應義塾大学総合政策学部准教授
玉井　哲雄	東京大学大学院総合文化研究科教授
宮内　宏	弁護士
峰崎　直樹	内閣官房参与
中村　秀一	内閣官房社会保障改革担当室長
向井　治紀	内閣官房内閣審議官
奈良　俊哉	内閣官房副長官補付参事官
篠原　俊博	内閣官房社会保障改革担当室参事官
阿部　知明	内閣官房社会保障改革担当室参事官
古橋　浩史	内閣官房社会保障改革担当室参事官
井上　知義	内閣官房情報通信技術担当室参事官
中村　裕一郎	内閣官房社会保障改革担当室企画官
水町　雅子	内閣官房社会保障改革担当室参事官補佐
木本　裕司	内閣官房情報セキュリティセンター参事官
関本　貢	一般財団法人日本情報経済社会推進協会 プライバシーマーク推進センター副センター長
高取　敏夫	一般財団法人日本情報経済社会推進協会 情報マネジメント推進センター副センター長

【議事次第】

１．開　会

２．議　事

（１）政策評価の実施の枠組みについて

（２）諸外国の第三者機関が承認を行わない理由について

（３）情報保護評価に関する論点について

（４）政府機関における情報セキュリティ対策について

（５）一般財団法人日本情報経済社会推進協議会（JIPDEC）からのヒアリング

３．閉　会

【配布資料】

資料１　　：政策評価の実施の枠組み

資料２　　：諸外国の第三者機関が承認を行わない理由について

資料３　　：情報保護評価に関する論点

参考資料１：諸外国における PIA ガイドラインの記載内容

参考資料２：情報保護評価報告書の記載様式項目（案）

参考資料３：諸外国における PIA 質問票

参考資料４：諸外国における PIA 報告書

参考資料５：情報保護評価と関連既存制度との関係について

参考資料６：情報保護評価に関連する認定制度

参考資料７：政府統一基準群について

参考資料８：諸外国における PIA 要否等判断基準

参考資料９：情報保護評価の実施の仕組み（案）

説明資料１　　：政府におけるセキュリティ対策

説明資料２－１：プライバシーマーク制度について

説明資料２－２：SMS 適合性評価制度の概要

【議事内容】

（中村企画官）

定刻となりましたので、ただいまから「情報保護評価サブワーキンググループ」の第２回会合を開催したいと存じます。では、宇賀座長、本日の議事進行をよろしくお願いいたします。

（宇賀座長）

それでは、早速議論に入りたいと思います。本日は、まず「政策評価の実施の枠組みについて」、それから、前回ワーキンググループにおいて宿題となっておりました「諸外国の第三者機関が承認を行わない理由について」、事務局の方からお配りした資料の説明をしていただきます。続きまして、事務局から「情報保護評価に関する論点について」を御説明いただきます。情報保護評価に関する論点の各項目について順次委員の皆様方から御意見をいただき、可能な項目につきましては本サブワーキンググループとしての方向性をとりまとめることができればと考えております。

次に、情報保護評価ガイドラインの策定に当たりましては、情報保護評価に関連すると考えられる既存制度との関連性の整理が必要であることから、まず内閣官房の情報セキュリティセンターの木本参事官より「政府統一基準群について」を説明していただきます。

最後に、本日は一般財団法人日本情報経済社会推進協議会にお越しいただく予定です。限られた時間の中ではございますが、プライバシーマーク制度の現状についてお聞かせいただきたいと思います。

では、中村企画官の方から「政策評価の実施の枠組みについて」を御説明お願いします。

（中村企画官）

それでは、御説明いたします。資料１をごらんください。この資料は総務省の行政評価局作成の公開資料を基に事務局の方で作成をしたものでございます。

政策評価と申しますのは、行政機関がその所掌に係る政策について、必要性、効率性、有効性等の観点から自ら評価を行うというのが基本でありますけれども、各行政機関が行いました評価について総務省による点検が行われております。したがって、政策一般が対象であることとか、目的の方が効率的で質の高い行政ですとか、成果重視の行政の推進が掲げられているといった違いがございますけれども、情報保護評価と比較した場合、単純な比較はできませんが、細部を詰めていくに当たっては政策評価の手法が参考になる部分もあろうということで御紹介をするものであります。

実施主体につきまして、行政機関が自ら行うことが基本ではありますが、（２）のイのところにございますように、各行政機関が実施するとともに、総務省においても評価の役割分担がありまして、こちらの方では複数府省にわたる政策について政府全体としての統一性を確保し、または総合的な推進を図るという評価ですとか、各行政機関の政策評価の

客観的かつ厳格な実施を担保するための評価を実施することとされておりまして、この点で総務省が政策評価制度の所管省庁として、ほかの各行政機関と同列の立場もございますけれども、独自の立場から評価を行うものもあるということでございます。

次の２ページ目ですけれども、「２（１）各行政機関が行う政策評価について」のところでございます。これは事後評価の形が一般的でありますが、研究開発、公共事業、政府開発援助、規制の新設・改廃、租税特別措置のようなものについては事前評価を実施しなければならないとされております。

この中で特に規制の事前評価につきましては、諸外国で RIA という形で実施されてきているものを参考に行われているものでありまして、コスト、便益などの観点から影響の分析・公表を行うということで、外形、手法の面では私どもはこちらのサブワーキンググループで御検討をいただく情報保護評価にやや類似する部分もあるのではないかと考えております。

他方、「３　総務省が行う政策の評価について」に関してですけれども、先ほど２つの評価があると申しましたが、このうち政策評価の客観的かつ厳格な実施を担保するための評価の前段階に相当するものとして、各行政機関が行った評価について改善措置の必要性等を指摘することによって、政府全体としての評価の質の向上とそれを通じた政策の見直し、改善を目指すという「客観性担保評価活動」と言っているそうですけれども、こういうものを行っているということです。これが最初に申し上げました総務省が点検を行っているものに当たっておりまして、①～⑤のところで具体的な流れを記載しておりますが、必要に応じて審議会での調査審議も行いながら、最終的には総務省による評価の実施の必要性の認定を行って、本当にこの認定がされるとまさに総務省の評価の権限が発動されるということですけれども、こういった流れができているそうであります。

４ページでございますが、ただし、この点検作業自体が平成 22 年度から公共事業、規制、租税特別措置といった３分野に重点化されているほか、実際には各省の方で改善の指摘などを受け入れて評価のやり直しを行うなどの形で、必要性の認定が行われて総務省が評価をするというところまで至った事例はないそうでございます。

点検実施件数については４番のところに記載をいたしておりますが、22 年度において総務省が点検したのは 425 件あるということでございます。

５ページ以降は、具体的な政策評価の事例を点検結果表も含めて添付をしております。以上でございます。

（宇賀座長）

ありがとうございました。ただいま御説明のありました「政策評価の実施の枠組みについて」に関しまして御意見やご質問のある方は御発言ください。

（新保委員）

慶應大学の新保です。政策評価の実施につきまして、行政機関が行う政策の評価に関する法律に基づいて実施される政策評価の手法は、今後の PIA、情報保護評価において、具体的にどのような形で評価を実施するのか、その手法として非常に参考になるものと考えられますが、現在検討を行っている番号制度そのものにつきましても、将来的に、行政機関が行う政策評価に関する法律に基づく政策評価の対象になるか否かについて、現段階ではいかがでしょうか。

（水町補佐）
情報保護評価自体の政策評価という点ですか。

（新保委員）
はい。

（水町補佐）
政策評価法の条文が今、手元にないのですけれども、政策評価については各行政機関の方で基本計画等を策定して実施していくという流れになっておりまして、内閣官房が政策評価の義務づけ対象の行政機関に該当するかという問題がございます。また、第三者機関が設置されれば、その第三者機関が政策評価の義務づけ対象となった場合は、第三者機関の方で基本計画等を策定して政策評価を行っていくものと考えられます。

（宇賀座長）
ほかにいかがでしょうか。

（宮内委員）
１点質問させていただきたいのですけれども、評価の実施の必要性が認定されたものが３ページの一番下の⑤のところにございますが、このときに関係府省自ら実施するか、または総務省が代わってやることになっていますけれども、どちらがやるかについても何らかのクライテリアはあるのでしょうか。

（水町補佐）
こちらにつきましては先ほど御説明差し上げたとおり、まだ⑤の客観性担保評価が行われた実例がないという状況にございます。その中で総務省の方でこういったものについてガイドライン、告示、または内部的資料で基準等を定めている可能性があるものと思われます。

（宇賀座長）

ほかにいかがでしょうか。政策評価法をつくるときに参考にしたのが環境影響評価法だったのです。環境影響評価の経験を踏まえると、報告書が非常に膨大で、しかも非常に専門的でわかりにくいという意見があったので、政策評価法の中では評価書を公表するときに要旨も併せて公表するという規定を入れてあります。その辺りは情報保護評価の参考になるかなと思います。

次に、引き続きまして中村企画官から「諸外国の第三者機関が承認を行わない理由について」を御説明お願いします。

（中村企画官）

資料２をごらんください。「諸外国の第三者機関が承認を行わない理由について」ですが、これは前回の本会合におきまして諸外国の事例では第三者機関は情報保護評価に対して承認を行っていないのが通例というか、ほとんどそのような仕組みになっていることを御紹介申し上げましたところ、なぜそのようなことになっているのだろうかという問題提起をいただきましたので、少し整理をしてみたものでございます。

事務局としての整理ですが、結論的には冒頭の３行でございます。諸外国の第三者機関は、オンブズマンなどの形で行政を監視するために行政の外部に立つ組織として設置されているため、行政機関の行為を承認することが権力分立などの観点から難しいということではないかと考えました。

まず１番目に御参考ということで、オンブズマン制度がどういうものかということなのですが、議会の代理人として行政を監視し、国民の権利利益を擁護するという機能を持つものでありまして、この意味でのオンブズマンは日本においては現在実例がないということでございます。

次に、諸外国のいわゆる個人情報関係の第三者機関の位置づけを調べてみますと、まずイギリスですが、これはいずれかの省庁の下にある機関ではなく、またイギリスは立憲君主制の形だと思いますが、女王の下の機関という形もとられていないということで、第三者機関はあらゆる面において政府から完全に独立をしているものとなっているということでございます。

次に、オーストラリアの場合ですが、こちらは内閣に置かれた政府機関ではあるけれども、独立して権限を行使することになっているそうです。

３番目、カナダ連邦ですけれども、こちらは最初に申し上げたオンブズマンということでまさに理解されておりまして、議会に仕えるもので、議会に直接責任を負う独立した機関であるということであります。

４つ目、アメリカですが、アメリカの場合は行政機関に対しては第三者機関は設置されていないということで、余り直接参考にはならないのかもしれません。

これを日本の場合と比較して考えてみますと、いわゆる社会保障・税番号大綱ですとか、これのもとになりました個人情報保護ワーキンググループにおきましては３条、８条とい

ったような議論がその後されておりますけれども、一連の議論の中であくまで行政機関ではあるということで議論がされてきたものと理解をいたしております。特にイギリスやカナダの事例ですと、第三者機関は行政機関には該当しないということで、行政権の個別具体的な作用に対して個別に介入することは権力分立の観点から望ましくないと考えられたのではないかと整理をしております。繰り返しになりますけれども、日本の場合はほかの行政機関からは独立した形をとるにしても、第三者機関自身も１つの行政機関ではあるという想定でございますので、そういったイギリスやカナダの場合のような制約はないと考えられるのではないかということでございます。

（宇賀座長）

ありがとうございました。ただいま御説明のありました「諸外国の第三者機関が承認を行わない理由について」に関しまして御意見や御質問のある方は御発言ください。

（新保委員）

諸外国の第三者機関が承認を行わない理由につきまして、本日の資料で非常にわかりやすく説明ただきましたけれども、これを踏まえて今後我が国の第三者機関を設置する作業工程について、これはあくまで意見として確認をさせていただきたいと思います。

まず、現在検討を行っている第三者機関はあくまで番号制度に係る第三者機関について検討を行っているわけです。番号制度に係る第三者機関につきましては、「番号」及び「番号」に係る個人情報を所管する。しかしながら、「番号」及び「番号」に係る個人情報の取扱いは既に意見が出ておりますとおり、個人情報一般との関わりにおいて必然的に他の個人情報の取扱い、とりわけインハウス情報と呼ばれるように企業の内部における情報の取扱いをはじめとして、個人情報一般の取扱いに係る問題と重複する部分がございます。そうしますと、必然的に個人情報の取扱い一般に係る第三者機関の設置は不可欠であるということが考えられるわけですが、今後の流れといたしましては、現在行っている検討はこの番号制度に係る第三者機関の設置ですが、将来的には個人情報の取扱い一般に係る第三者機関の設置の検討も行うことになると考えられます。各国の制度との比較について今回資料を御提示いただきましたけれども、その際に必然的にこの点について今後留意しなければならない点といたしましては、国際的に各国のコミッショナー、同様に個人情報、プライバシー保護への取り組みを行うことができる第三者機関として認められるか否かということが最終的な課題となるわけです。つまり順序としては番号制度という非常に狭い第三者機関、個人情報の取扱い一般という第三者機関、最終的には個人情報、プライバシー保護について、国内だけではなく、国際的にも認められたコミッショナー同様の組織が求められているわけでありますので、そのときに各国の制度はこのように現在承認という手続を第三者機関が行わないという形で設置されているわけでありますけれども、その理由も踏まえて今後最終的に国際的にも認められる第三者機関の設置を検討するに当たっては、

引き続きこの問題については検討を行わなければならないということについて確認をさせていただきと思います。

（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。

では、続きまして、中村企画官から「情報保護評価に関する論点」について御説明をお願いします。

（中村企画官）

資料３、それから、適宜参考資料１～９を使いながら御説明します。これは前回も情報保護評価に関する論点ということで議論をお願いいたしましたが、更にその議論を踏まえて深掘りをしたものですとか、更に新しい論点などをお示しして議論を深めていただきたいということでございまして、かなり内容が増えてきておりますけれども、前回と違っている点ですとか、たたき台的に整理いたしました点などを中心に御説明をいたしたいと思います。

最初に目次的にどのようなことが書いてあるかを示しておりますが、まずこちらのサブワーキンググループの検討の視点が書いてあって、その後「情報保護評価の目的」、その上で評価や保護の対象をどう考えるかということを書いております。次に、「情報保護評価ガイドラインに関する論点」として、記載事項ですとか、既存の関連制度との関係の整理といったことに触れております。それから、「情報保護評価の実施の仕組みに関する論点」ということで、これは前回にも少し問題提起をいたしましたけれども、システムの数も非常に多い中で実効性と信頼性を両立させてどういう仕組みでやるのがいいだろうかといった論点でございます。最後に、地方公共団体における情報保護評価はどうあるべきかというようなことで一応整理をいたしております。

検討の視点のところは前回の資料と余り大きな違いはございませんので、２ページをごらんください。こちらで情報保護評価制度の趣旨や目的につきまして、このように考えたらどうだろうかということで整理をさせていただいております。

１番の最初のところですけれども、番号制度はより公平・公正な社会、その他５つ書かかれているような姿の社会の実現を目指して導入されるものでありますが、一方でさまざまな個人情報に関わる国民の懸念が生じることもまた考えられるところであります。そこでこういった懸念を踏まえまして、国民の「番号」に係る個人情報が適切に取り扱われる安心・信頼できる制度の構築のためということで情報保護評価を実施するというのが総論的な趣旨ととらえております。

その上で、目的として３つ掲げております。

１つは、事後的な対応にとどまらない、積極的な事前対応を行うことでありまして、一度流出した情報は回収が困難であるなど、プライバシー侵害はその回復が容易でない側面

も多いことですとか、一旦システムを構築してしまって、後から問題があったということで大規模な仕様変更などが起きますと、財政支出の観点からも問題があるといったことで、事前対応が１つのポイントかと思っております。

続きまして、情報保有機関が国民のプライバシー保護にどのように取り組んでいるかについて情報保有機関自身が宣言し、国民の信頼を獲得することとしておりまして、これは個人情報の取扱いやそのシステムに対する透明性を確保しまして、国民に対してわかりやすい説明を行うことが国民に信頼していただける制度システムの構築に資するであろうということで、２～３ページ目にかけてそのようなことを記載しております。

３つ目ですが、第三者機関が確認を行うということで、今、申し上げた２つの点について厳格な実施を担保して、より実効的なものとするという、この３つで整理をしておりますので、御議論いただければと存じます。

次に、情報保護評価の評価・保護はどういったものを対象として考えるのかということなのですけれども、この点につきましては個人情報保護に関して既存の法令などがございますが、単にこれを守っていれば、遵守していればよいかどうかということではなくて、諸外国の例ですとか、今、説明しました目的を踏まえますと、プライバシー保護という観点からそれぞれの業務ですとか、システムの特性に応じて適切な取扱いがなされているのかどうかというところを評価するものであるべきではないかと考えております。

具体的には（１）のところに書いてありますけれども、個人情報保護法令を遵守するだけではなくて、更により一層の保護措置を追求するということで、これをわかりやすい言葉で言い換えると、法令遵守といった画一的な基準をクリアーするというものではなくて、いろいろな制約条件等はあるとは思いますけれども、システムごとのベストなものを追求しているかどうかという観点からの評価を行うべきではないかということで整理をしております。

４ページの（２）と書いてあるところの上に簡単にまとめておりますけれども、こういった観点からしますと、例えば行政機関個人情報保護法上も一定の事項を公表するとされておりますが、情報やシステムによってはそれよりももっと公表事項を増やすとか、第三者提供は一定の法律の要件の下で可能とされているところでありますけれども、こういったものをなるべく制限的に運用するような考え方をとっていますとか、そういったようなことを措置としてとっていただいて、それを評価していくといったことが考えられるのではないかと思っております。

続きまして５ページですが、「第３　情報保護評価ガイドラインに関する論点」でございます。

「ガイドラインの汎用性」につきましては、前回も完全に「番号」に特化したものとするのかどうかというような御議論がございましたので、少しこちらでも考えてみましたけれども、一応形としては「番号」に係る個人情報を取り扱うシステムということでつくりつつ、実際の内容の検討に当たっては、一般的なシステムで個人情報保護を考えたい場合

にも広く参考、活用できるような配慮をしていくということではどうだろうかと思っております。

次に、「ガイドラインの記載事項」でありますが、基本的な構成としては参考資料１として付けております諸外国の記載内容なども参考にして、情報保護評価とは何だとか、目的であるとか、実施の仕組みであるとか、報告書の記載様式、実際にはこれは質問形式の形をとっているのが通例でございますが、こういった記載事項を諸外国で定めているようですので、私どものガイドラインでもこういったものを決めていってはどうかということであります。

具体的に少し御議論いただきたい内容として報告書の記載事項がございまして、記載様式の項目をどのようなことにしたらよいだろうかということで、今、このペーパーでは考え方としては個人情報のフローをまず示して、そこから導き出されるプライバシーに与える影響について収集・使用・管理・提供・抹消といった各段階ごとに対策を記載していくといった考え方をとっております。

その考え方を基に参考資料２ということで、今、ここで細かい内容まで逐一御説明はしませんので、質問等があればお答えしたいと思いますが、「情報保護評価報告書の記載様式項目（案）」ということで、今、申し上げた考え方に沿って関係法令の規定ですとか、あるいは参考資料３として付いているんですけれども、諸外国における質問票の記載を参考に質問の一覧を考えてみたものでございますので、御意見を賜りたいと存じます。実際「コメント」というところで何を参考にしたのかを、略式な記述で恐縮ですけれども記載しております。

続きまして、資料３の方に戻っていただきまして、６ページ、「既存の関連制度との関係性について」でございます。情報保護評価ガイドラインの策定に当たっては、情報保護評価に関連すると考えられる既存制度との関係も整理しておいた方がよいだろうということで、今回関係の機関や団体の方においでいただいておりますけれども、少し議論をお願いしたいと考えております。

参考資料５をごらんください。この資料とここに書いてある内容を一部わかりやすく説明した参考資料６、７を付けておりますが、これは公開資料を基にして、こちらも事務局の方で作成したものであります。

情報保護評価はプライバシーへの影響を評価するということでありますけれども、評価の対象として個人情報保護対策や情報セキュリティ対策が含まれ得るということで、これらに関連する制度との関係を整理したいと考えました。

具体的な既存の制度としてはいわゆる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取り組み、プライバシーマーク制度、セキュリティ関連では政府統一基準群、ISMS 適合性評価制度、IT セキュリティ評価及び認証制度がございまして、これに関してそれぞれ簡単な検討を加えております。

まず、行政機関個人情報保護法に基づく取り組みですけれども、これは行政機関個人情

報保護法では個人情報ファイルを保有しようとするとき、一定の事項を総務大臣に行政機関が事前通知するとともに、保有後に個人情報ファイル簿という形で公表しなければならないとされております。ファイル簿の中でかなりのことが記載されていればそれでよいのかもしれないのですけれども、２ページですが、こちらの方は別紙２という形で実例も後ろの方に付けております。要はそのような個人情報を持っていますといったこと、言ってみれば結果としてこういう状況になっているということを静的な形で記述したものにとどまっておりまして、具体的な業務やシステムの中でそういった持っている情報がどういう考え方でどのように具体的に取り扱われるのかといったところまでの分析評価はされていないと考えておりますので、単純に個人情報ファイル簿の公表などを行っているからといって、それで情報保護評価の仕組みが無用になるものではないと考えております。

ただし、例えば事前通知を行うことと、情報保護評価で第三者機関に承認を求めることに関しては外形的には少し類似したようなところもございますし、その他基本的な目的などの記載事項の重複等も考えられますので、手続的な面から両制度間の調整を図る必要がないかという検討はあってもしかるべきではないかと考えております。

次に、「プライバシーマーク制度」でありますが、これは３ページになります。個人情報について適切な保護措置を講ずる体制を整備している事業者等を認定して、その旨を示すプライバシーマークを付与して、事業活動に関してプライバシーマークの使用を認める制度と理解をいたしております。この認定ですけれども、基本的には個人情報保護法の考え方が根っこにあって、若干の上乗せ等はあるにしても、こういった法令をきちんと守れる体制になっているかを認定するものと私どもは理解しておりまして、そういった意味から情報保護評価が個人情報保護法令遵守にとどまらないものであるとすれば、やや範囲が異なるのではないかといったことがあります。同時に、４ページの記載ですけれども、２つ目の○にありますように、プライバシーマーク制度は全社的な、事業者全体としての取り組みを認定対象としているのに対して、情報保護評価は個々のシステムを評価の対象とするものでありますので、こういった点で決定的な違いがあると理解しております。したがって、プライバシーマークを取得している事業者であっても、また別の取り組みとして情報保護評価を実施する必要はあると言えるのではないかとしております。

５ページでありますが、「セキュリティ関連の既存制度と情報保護評価」であります。

総論ですけれども、プライバシー保護にとってはセキュリティ対策は１つの手段に過ぎないのではないかということをまず最初に掲げておりまして、セキュリティ対策は外部からの攻撃などを想定するものだと思うのですけれども、通常無事に情報を取り扱っていてもプライバシーは問題になってくるわけで、１つそこは視点が違うのではないかと思っております。他方、セキュリティ対策についてプライバシー保護の観点から余り深く掘り下げていくような必要性も逆になくて、逐一セキュリティ関連の項目を評価していくまでの必要は必ずしもないのではないかと整理しております。

その上で、まず「政府統一基準群」でございますが、こちらは NISC、内閣官房情報セ

キュリティセンターという政府の一部門におきまして、政府機関が遵守すべき情報セキュリティに関する基準を定めておりまして、各政府機関におきましてはそれで定められた以上の情報セキュリティの確保を目的としてそれぞれ基本方針などを策定して、セキュリティ水準の向上に努めるものであると私どもとしては理解をいたしております。

「情報保護評価との相違点」といたしまして、やはり情報セキュリティ対策は情報を資産として見て、これが機密性、完全性、可用性といった観点からきちんと保全されるかどうかが関心事項であって、そうしますと例えば個人情報とかプライバシー情報でないような通常の統計データなどであっても、逆に言えばこういったことは大事なものでありますが、一方で、最初に総論のところでも申し上げたように、プライバシー保護という観点からはカバーし切れないものもあるだろうということであります。したがいまして、政府機関が統一基準群にのっとって対策を実践しているとしても、全く別の観点から情報保護評価を実施する必要はあると言えるのではないかとしております。

次に、ISMS 適合性評価でございますけれども、こちらはセキュリティ関連でプライバシーマーク制度と同様の取り組みと理解しておりまして、事業者としてのマネジメントの中でセキュリティがきちんとできる体制になっているかを見るものと理解しておりますので、こちらも少し違うだろうと考えております。

最後に、「IT セキュリティ評価及び認証制度」ですけれども、これはデジタル複合機、ミドルウエア、ネットワーク機器など、IT 関連製品ですとかシステムのセキュリティ機能について認証するものですが、これはあくまで製品として十分なセキュリティの性能を備えているかを見るものと理解をしておりますので、これも情報保護評価でやろうとしていることとは目的等が異なるのではないかという整理をいたしております。

こういった検討を踏まえまして、資料３の６ページにおきましては、全体としては今、申し上げたようなほかの取り組みをやっているとしても情報保護評価をやるべしということに立ちつつ、個人情報ファイル簿等について両制度間の調整を図るですとか、あるいはほかの仕組みにおきましても、場合によっては情報保護評価の特定項目の省略が可能な場合なども考えられるかと思いますので、こういった点を今後具体的に内容を詰めていく中では検討していってはどうかということでまとめております。

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、実際のフィージビリティー的な面でコストなどを考えますと、やったはいいけれども形式的な取り組みになってしまっ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。そうなるとむ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で、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して、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出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性も特段薄いのではないかと思っておりますが、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、結果の公開はさせてもいいのではないか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。

最後に、本当に必要性が高いですよと判断されたものについては、ここで書かれております措置は一応すべて行って、情報保護評価をしっかりやるし、第三者機関の承認は勿論しっかりやったものとして受けて公表もするということにしております。ただ、実は国民の意見を聞くことに関しましては、前回もパブリックコメントという形はどうだろうかと少し問題提起をさせていただいたところ、それが実効性、意義があるのかどうかというこ

とについては種々御議論がありましたので、今日この時点では各機関が裁量によってセキュリティ上の懸念がないようなものについてパブリックコメントのような形で国民の意見を聞くという考え方にしております。

以下、こういう内容が資料３の 10 ページの前半まで書いてあります。

あとは多少記載を追加しているような事項もございますが、おおむね前回と同じようなことが書いてございまして、１つ付言をさせていただくとすれば、「４　報告書の公表について」というところの最後なのですけれども、ここで公表の仕方として情報保護評価報告書の一覧性を確保するということで、この報告書は任意で公開してもいいかとは思いますが、各機関にて公開するのではなく、第三者機関のウェブサイトなどで一括して公開することとしたらどうだろうかというような提案をさせていただいております。

説明は以上でございます。

（宇賀座長）

ありがとうございました。それでは、各項目についての議論に移りたいと思います。まず、「第１　本 SWG における検討の視点」及び「第２　情報保護評価の目的」について御意見のある方は挙手をお願いします。

（大谷委員）

大谷でございます。今、御説明をいただいた中で念のため確認をさせていただきたいのが、３ページのところです。情報保護評価の目的の③なんですけれども、第三者機関が確認を行うことで情報保護評価の厳格な実施を担保するという書き方をしていらっしゃいますが、この「確認」というのはいわゆる「承認」と全く同じなのか、ただ承認の中身が特に明確になっていないので、今のところはあえて「確認」という言葉を使っているのか、この点を教えていただけますか。

（水町補佐）

基本的には承認を考えております。承認にまで至らないシステムについても第三者機関の方で任意に点検等を行うことは可能かと思いますが、まだ詳細については検討ができておりませんので、ここでは「確認」という言葉を使わせていただいております。

（大谷委員）

わかりました。ありがとうございます。

（宇賀座長）

ほかにいかがでしょうか。

（新保委員）

３ページの「３　情報保護評価の評価対象・保護対象について」の「（１）個人情報保護法令遵守とプライバシー保護との差異」について、このような形で今回個人情報保護にとどまらず、プライバシーを保護することが重要であるという認識は間違いないといえます。。しかし、この件につきまして個人情報保護とプライバシー保護の違いは何かということと、今回の「番号」の取扱いに係る個人情報の取扱いについてなぜプライバシー保護が必要なのかということについて、今後更にさまざまな点で説明を求められる機会があるかと思いますので、確認をさせていただきたいと思います。

生存する個人に関する情報であって特定の個人を識別可能な情報を適正に取扱い保護することが個人情報保護の目的です。つまり個人情報保護制度は取り扱う情報の内容について特に色分けをせずに、個人情報の取扱いに係る手続を個人情報取扱事業者並びに行政機関、独立行政法人等に課しているわけであります。一方、現在検討を行っている情報保護評価制度の対象となる情報と保護対象については、社会保障の給付に係る情報や個人の所得に係る情報、税に係る情報など、個人の私生活上の事実に係る情報がこの情報には含まれますし、一般にこれらの情報は他人に知られることを欲しない情報であると考えられます。更に、行政機関が保有しているこれらの情報は未だ他人に知られていない情報であるといえます。この要件を踏まえて何をすべきかを考えることが必要なわけですが、これらの要件に該当する情報が「番号」を軸に利用されるということが今回の検討の対象となっているわけです。つまり「番号」を軸にこれらの情報が利用されることについて、プライバシー保護の観点からの取り組みが必要であるということを明確に確認しておきたいと思います。

最近ではいろいろなキャッチフレーズ的な用語でイメージとしてのプライバシー保護という議論がなされる傾向がございます。この点につきましては個人情報保護とプライバシー保護についてはそれぞれこのような違いがあって、今回の「番号」を軸に利用されるこれらの情報については特段の措置としてプライバシー保護の面も考えなければならないのだということを明確にしておきたいと思います。

（宇賀座長）

ありがとうございました。事務局の方から何かコメントはございますか。

（大谷委員）

今の関連でよろしいでしょうか。今、新保委員から御意見のあったことにつきまして、違う観点なのか同じ観点なのかよくわかってはいないのですが、プライバシー保護を対象とするということについて懸念している点などをお話ししたいと思います。

プライバシー保護を対象とすること自体は非常に賛同しておりまして、これまで諸制度の中でプライバシー保護を正面から議論することがなかなかできていない中で、こういっ

た情報保護評価という仕組みを通して、プライバシーについて各機関が真剣に考える機会を得るということはとても望ましいことだと思っております。そういう意味で大変賛成はしているのですが、先ほど新保委員もおっしゃったように、プライバシーという概念が個人情報保護とはまた違ったものであって、外延が明確になっていない概念ではないかと思っております。また、世の移り変わり、それから、何か特にプライバシーに対する侵害行為が重なったりしますと、消費者の心理などにも大きく影響があって、たちまちのうちにプライバシーに関する認識が急に高まったりというように変動するものでもありますので、やはりプライバシーについてベスト追求型の評価は試みるものの、やはり最低限の法令遵守といった基準はクリアーするような指標はミニマムで情報保護評価の中できれいにして、少なくともここはクリアーできているという宣言を各機関が行い、それに加えてプライバシーの観点から見たときに新たな配慮が必要かどうか、新たな問題点がこのシステムなり制度なりから生まれてこないかといったことをもう一度見るというように二層構造にしておくことが、見る方にとってもよりわかりやすく、また機関にとっても何について責任を持って判断しているのかということが明らかになりますので、それが望ましいのではないかと思っております。

新保委員ともしかしたら同じ意見なのかもしれないのですけれども、違っているところがありましたら十分に議論した上で、次のもう少し詳しい質問項目などに影響する点だと思いますので、この点は十分に明確にしていきたいと思います。以上です。

（宇賀座長）

ありがとうございました。事務局から何かコメントはありますか。

（中村企画官）

確かに御指摘のとおり、プライバシー保護はどういうことをすればそれが満たされたことになるのかといったものが、今、先生がおっしゃいましたように、国民や実施機関にとってもややわかりにくいことはあろうかと思います。ここで記載させていただいた際も、先ほど説明の中で申し上げましたけれども、単に画一的に法令の基準を遵守するというよりは、それぞれの特性に応じて努力をしてもらうということではないかというつもりで書いております。今後ガイドラインですとか、あるいは法令のレベルまで可能であればそういったものも含めて、どういった判断基準とか理解の基準のようなものを示していけるかは検討していきたいと思いますし、先生方の御指導もいただければと思っております。よろしくお願いいたします。

（宇賀座長）

一般法としての個人情報保護法制の基準は当然クリアーするということを前提として、更に特別法の番号法で規制を上乗せするという趣旨ですね。ですからそこをもう少し明確

に修文するといいのではないかと思います。ほかにいかがでしょうか。

（宮内委員）

今、ここで出ていますベスト追求型の評価ということで、この点については委員が言ったとおりだと本当に思うのですけれども、これに関しまして最近ちょっとインシデントがあったので御紹介します。DigiNotar という認証局と言われるところから数百枚の偽造 SSL 証明書が発行されたという事件がここ 10 日ほどいろいろ言われていると思っています。この DigiNotar につきましては、EV 証明書という信頼性の高い証明書の発行者として監査等も受けていたという事実がございます。実際そういう監査を受けて、ある程度の基準は守っていたのではないかと思われますけれども、実際にはセキュリティはぼろぼろだったということが最近だんだんわかってきている。

ここで非常に思うのは、単に基準を守るということだと、その基準を守るために一番安い方法をやろうとかいうことになりかねないということです。それに対してプライバシーを保護しようという立場に立ったときに、そういった基準を守ればプライバシーを守れるということではないと思いますので、各保有機関がプライバシーを守るためにベストなエフォートをしていくことが極めて重要だと思っております。

ですから、基準といいますか、この PIA の目標につきましてあくまで基準を守るというものではなくて、プライバシーを守るために各保有機関がしっかりと努力していくことが一番重要であるということは明記していきたいと思っています。

（宇賀座長）

ありがとうございました。今の点はこれに反映させてください。

（玉井座長代理）

玉井です。基準クリアー型だけではない、あるいは法令遵守だけではないという点は、ではそれをどうやって担保するかは難しいことには違いないけれども、結構重要な視点ではないかなと私は感じます。

というのは、結局これは一種のリスク分析で、それには考えられるさまざまなリスクを想像することが必要です。プライバシーというのは、例えば個々のシステムは大丈夫だけれども、名寄せしてしまうことでわかるということはよく言われますが、対象とするシステムを評価するときに、同時に関連するいろいろなことを想定するのは基本的な態度として重要で、勿論それはオープンエンデッドだからどこまでやればいいかということをクリアーにできないという問題点はありますけれども、基本的に事前に何かアセスしようという立場からすると、いろいろな場合の想像力を含めてリスクの可能性を可能な範囲で追求しようということを念頭に置いておくことが重要なのではないかと思います。

（宇賀座長）
ありがとうございました。

（新保委員）
個人情報保護とプライバシー保護との関係について、今後どのような基準で対応が必要なのかという点についてです。
プライバシー保護の基準については､従来から定量的かつ統一的な基準はございません。そのため何をしなければならないのかということでありますけれども、この点について従来個人情報保護制度においても、個人情報保護法、それから各府省庁のガイドラインにおいて取り組みが行われてきた部分として、しなければならない事項とすることが望ましい事項という形で分けて議論がなされてきた部分があります。
つまりどういうことかといいますと、しなければならない事項については、これは法令遵守のために必須の事項といえる部分です。それから、国民の人権保障のために不可欠な事項。これはしなければならない事項として従来から明確な基準に基づいて取り組みが行われてきたといえます。一方、することが望ましい事項については、プライバシー保護のために実施することが望ましいということで適宜実施されてきた部分です。
この点について従来からの基準は前者の基準、しなければならないという基準については現行の法令、判例に基づく基準、これに基づいて実施することとなってきたわけです。一方、今回透明性の確保の観点から重要な点としては、後者についてどこまでやるのか、情報保護評価によってどこまでプライバシー保護のための取り組みを行うのかということが求められているわけです。そのときに後者の基準は、これを国民の権利利益の保護に資すると思われる事項を今後検討するということになっていくわけでありますが、ここで情報保護評価制度はあくまで評価をするために各行政機関が自ら評価を行うという仕組みであります。
そうしますと例えば前者の基準、しなければならない基準は現行の法令に基づく基準として、これは自明であります。一方、後者の基準につきましては、例えばプライバシー保護技術、プライバシー・エンハンシング・テクノロジーといいますけれども、その技術を用いることによって結果的に個人のプライバシーを保護することができるという仕組みがあるわけであります。それを利用するかどうかということについては、情報保護評価を実施することでプライバシー・エンハンシング・テクノロジーのようなプライバシー保護技術として何をどのように用いるかという判断材料にもなるということなのです。
ですから、プライバシー保護については一定の統一的な基準はございませんけれども、情報保護評価を実施することで最終的にどのようなプライバシー保護を行うのか、またはどのようなプライバシー保護技術を用いることで国民のプライバシーを保護することができるのかという判断の指標にもなるといえます。ですから、その指標を決めるという視点からプライバシー保護という問題を考えるだけではなく、情報保護評価を実施することで

どのようなプライバシー保護を実現するのかという視点からの検討も必要になってくると思います。

（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。
よろしければ、次に「第３　情報保護評価ガイドラインに関する論点」と「第４　情報保護評価の実施の仕組みに関する論点」及び「第５　地方公共団体における情報保護評価に関する論点」について併せて御意見をお伺いしたいと思います。

（玉井座長代理）
第３のガイドラインに関する論点のところですけれども、ガイドラインがどういう形をとるかということについて、今、ここでも記載事項の想定なども書いてありますが、後の方に出てくるしきい値との関係もあって、ガイドラインのところでも⑤の質問票という、チェックリスト的なイメージがかなり強いように見えます。それはそれで便利だし、しかもやりやすいし、効率的だと思います。しかし、ガイドラインという名前からすると、情報保護評価をどういうふうにやるかということをガイドするものだと考えられます。そうするともう少しポジティブなというか、建設的な部分も、単にチェックリストでこれをチェックしたらそれで終わりというのではない部分もあっていいのではないか。
問題は勿論評価をどうやるかですが、同時にそれはシステムをどういうふうに考えて構築するかということのガイドにもなっているはずだと思います。そういう意味でいうと、対象は事前評価の必要性が高く第三者機関に報告書を出して、承認を受けるものだけではないところにも広げられるのではないか。番号制度に直接ないし間接に関連するようなシステムをつくるところが、このガイドラインを読むと、プライバシーについてはこういうふうに考えなくてはいけないなということがガイドされるような、そういう趣旨の記載のスタイルというか、そういう部分もあってもいいのではないかなと思います。

（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。

（新保委員）
順に、まず５ページの御指摘があった「（２）ガイドラインの記載事項」についてです。こちらにつきましては既に諸外国における先行事例もございますので、それらを参考にどのような記載事項にするのかということで、記載事項の内容そのものについては先行事例を参考にするということで問題はないと思います。その一方で、諸外国と我が国の制度、システムについては大きく異なりますので、そうしますとガイドラインの記載事項として対象となるシステムの範囲をどのように定めるのかということについては十分な検討が必

要だと思います。例えば住基ネットを含めるのか、公的個人認証サービスなどを含めるのかといったような具合に、システムをどの範囲で対象にするのかということについては、そもそもこの情報保護評価制度そのものの対象となる情報システムでありますので、その点は明確にしておくことが必要ではないかと思います。

続いて、９ページの「必要性に応じた仕組み」のイの四角の「②行政機関又は関係機関の裁量により、パブリックコメント等で広く国民の意見を求めるかどうか判断する」ということについてであります。つまり情報保護評価の報告書についてはパブリックコメントを実施することで広く国民の意見を求めるということが原案となっておりますけれども、前回も申し上げた点でありますが、第三者機関が専門的、客観的な観点、視点から情報保護評価制度の内容を精査することができるのであれば、必ずしもパブリックコメント等によって国民の意見を求めることが必要ない場合もある。つまり私見としては、パブリックコメントの実施を義務づけることについては必要ないのではないかという意見であります。その理由は、情報保護評価報告書自体は行政手続法６章のパブコメが義務づけられる命令と行政手続法２条８号には該当しないということになりますので、そうすると義務づける場合には特別法、つまり番号法に基づく義務づけが必要になってくるわけであります。そうなりますとパブコメは義務づけなくても、既に現行制度において行政手続法に基づくパブリックコメントの実施の対象にもなる。ましてここでも裁量という形になっておりますので、義務づけを不要にしても事実上実施するかどうかは行政機関の裁量に委ねられているとも考えられますので、第三者機関が専門的、客観的な立場からきちんとした精査ができるのであれば、パブリックコメントを実施することを義務づけることは必ずしも必要ないのではないかと考えております。

10 ページの「２　第三者機関による承認について」、今までの部分は意見ですが、こちらについては質問となります。第三者機関の承認について、この法的位置づけはどのようになるのかお伺いしたいと思います。例えば行政手続法上の処分に当たるのかどうかという点であります。こちらで一度発言を区切って、質問として第三者機関の承認についてその法的位置づけについてお伺いしたいと思います。

（宇賀座長）

では、事務局の方からお答えいただけますか。

（水町補佐）

第三者機関の承認につきましては行政手続法上の処分行為に当たるものと考えております。ただし、行政手続法上の適用除外事由に該当する場合は処分に該当しても行手法上の手続規制はかからないと考えております。特に国の行政機関に対する処分行為は行手法上の適用除外でございますので、行政機関に対する承認行為については行手法の対象外、また独法や公法人につきましても適用除外事由がございますので、これに該当する場合は

適用除外になると考えております。

（新保委員）
そうしますと、行政機関に対することについては行政手続法上の処分には該当するけれども適用除外ということになるかと思いますけれども、そうなると第三者機関が今後行政機関が行う行為について承認を行うという手続を置くことになっているわけでありますが、行政機関が行政機関の行為を承認することについては特に問題はないでしょうか。

（水町補佐）
行政組織法上現在の仕組みでも例えば人事院が採用を承認する権限ですとか、財務大臣が予算等に関連する承認権限を有しておりますし、そういった点で現在も上級行政庁でなくても他の行政機関に対して承認権限を行使しているという法制がございますので、それと同様に第三者機関についても総括管理機関として承認権限を行使していくことは特段問題はないと考えております。

（中村企画官）
すみません、ちょっとよろしいですか。承認ということで実際に例えば法律上も番号制度の関連法の中で今後法案作業を進める中で書いていくとすると、そのときに改めてきちんとした整理はしていかなければいけないと思っておりますが、現時点の考え方としては今、お答えしたようなことになるということでございます。

（宇賀座長）
よろしいですか。

（宮内委員）
少し戻りまして６ページの「既存の関連制度との関係性について」でコメントしたいと思います。ここで御説明いただいたように、既存の制度での認証等をとったからといって、PIA を省くことはできない。これはおっしゃるとおりだと思います。ここで既存のものにつきまして、例えば特定項目省略とかいうことが行われる可能性があると。これもそのとおりだと思うのですが、このほかに既存の基準に対するリファーみたいな形がよく出てくるのではないかと思っています。例えば政府統一基準からは重要な情報システムに関しては 15408 のセキュリティーターゲットの評価をやるべしということが書かれていたり、そういった形で他の標準に対するリファーは結構出てくるのではないかと思うのです。そういう意味でこの間の関係はしっかり認識しておく必要があると思っています。これはある意味では目的と手段の関係になっているような規定があり得るのではないかという意味です。

それから、実際にレポートといいますか、報告書を書く場合にも、この部分はこの基準に従ってつくりますというような記載が結構諸外国のレポートの中にも出てくると思います。例えばセキュリティモジュールについては FIPS140 を使うとか、そういうふうな書き方で一応レポートとして出るケースもありますので、そういった意味でも既存の関連制度、関連の基準はいろいろな意味でこれにも関連すると思いますので、その辺りはしっかり見極めていきたいと思っています。

（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。

（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、これを含んでいてかつ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本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）
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のような形なのですけれども、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記載しておりますが、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、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ーしなければいけない幾つかのポイントがあるかと思いますので、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。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。いろいろと貴重な御意見をいただきましたが、時間の関係がございますので、次に内閣官房の情報セキュリティセンターの木本参事官から政府統一基準群について御説明をお願いします。続きまして、一般財団法人日本情報経済社会推進協会の関本プライバシーマーク推進センター副センター長にプライバシーマークについてお話しいただき、高取情報マネジメント推進センター副センター長に ISMS について御説明をお願いしたいと思います。
なお、先ほど議論しました関連制度との関係性については、説明後、更に御意見があれば御発言をお願いしたいと思います。それでは、木本参事官、お願いします。

（木本参事官）

NISC の参事官の木本でございます。お手元の説明資料１に基づいて御説明を申し上げます。

先ほど中村企画官から概略について御紹介いただきましたとおり、政府機関統一基準群は政府の運用している情報システム、情報一切について機密性、完全性、可用性の観点から各府省に情報セキュリティ対策を講じるものとなっております。

ここでいう運用というのは、政府が保有しているシステム、あるいは外部委託をする形で政府の業務を外部に委託する場合の両方含んでいるわけでありますけれども、また可用性、完全性についても求めているわけでございますので、先ほどの御説明をもう少し補足させていただきますと、外部からの攻撃だけではなくて、例えばヒューマンエラーであるとか、機械の故障、天災など、広くシステム障害一般について対策を求めているものでございます。したがいまして、後ほど高取副センター長から御説明いただく ISMS に基づく中央省庁向けの基準と御理解いただいてよろしいかと思います。

また、この統一基準を制定、改定を行っておりますのは IT 戦略本部長である総理大臣決定により設置された情報セキュリティ政策会議、この２枚目でいいますと右側のオレンジ色の部分でございますけれども、この会議体が統一基準群を制定、運用しております。私ども内閣官房情報セキュリティセンターはその事務局として内閣官房の安全保障、危機管理担当の副長官補の下に設置されております。

３ページを開いていただきまして、もともと統一基準群でございますけれども、発端は 2000 年に幾つかの省庁のホームページがサイバー攻撃を受けまして改ざんされたという事件が発生いたしました。また、ちょうど 2000 年というのは御記憶にあるのではないかと思いますけれども、Y2K、要するに 2000 年問題で情報システムが止まってしまうのではないかということで社会的に大きな問題になりました。こういうことを受けまして、政府の持っている情報システムについてセキュリティを評価していかなくてはいけない、横断的にそういう対策をとっていこうということで、当時内閣官房の中に情報セキュリティ対策推進室を設けまして、情報セキュリティポリシーのガイドライン、それから、重要インフラのサイバーテロ対策に係る特別行動計画を設置したのが最初でございます。その後、2005 年に現在の NISC ができまして、また情報セキュリティ政策会議が設置されるということで、統一基準も 2005 年に制定いたしまして、以降４回にわたりまして改定を重ねてまいりまして、直近で申し上げますと、今年の４月に改定をして、それまで統一基準という１本の基準だったものを、統一規範、統一管理基準、統一技術基準という３つの基準に分けたことから、今、統一基準群と呼んでおります。

時間もありませんので２ページほど飛ばしていただきまして、５ページ目のところでございますけれども、この統一基準でございますが、先ほどの議論でいうと私どものはあくまでも基準クリアー型のものでございまして、当初は各府省いろいろとセキュリティに穴が空いているものが結構あったものですから、最低限各府省の足並みをそろえようということで始めたのが統一基準でございます。ただし、各府省最低限の基準をクリアーした上

で、毎年毎年 PDCA を回していく中で徐々にそれを進化させていくという仕組みを取り入れております。そういう形でセキュリティ対策についても内容を向上させていこうという仕組みにしております。

６ページでございますが、私どもの統一基準は先ほど申し上げたように、各府省のすべての公務員、行政事務従事者と私どもは呼んでおりますが、きちんと理解しておくべき統一規範、お手元に白表紙で今日お配りさせていただいておりますけれども、これらについてはすべての職員が理解しなければいけないということでまとめておりまして、その下に組織マネジメントの観点から統一管理基準、情報システムのテクニカルな部分については統一技術基準という３つの構成に大きく分けて現在運用しております。これらに基づきまして各府省個別にそれぞれ事情がございますので、各府省はこれらに準拠する形での省庁ポリシーを策定する、これを運用してもらうというような構成になっております。

今、簡単に各省庁と申しておりますけれども、内閣官房が運用しているシステムでございますので、基本的に内閣に属する行政機関が対象になってまいります。ただし、政府全体という意味でいうと、立法府、司法府あるいは内閣に属さない会計検査院なども同じ政府の中ということでございますので、これらについて情報は共有するような形にさせていただいております。更に先ほどの参考資料５の９ページのところで独立行政法人については対象でないというふうにまとめておられましたけれども、正確には各府省が所管する独立行政法人については統一基準に準拠する形で各独立行政法人のセキュリティポリシーを制定して運用させるように指導するようにということを求めておりますので、間接的ではありますが、この統一基準に準拠するような形で独立行政法人も対象になっていると御理解いただければよろしいかと思います。

７ページにまいりまして、ではこの統一基準で何を定めているかということでございますが、統一規範については、今、お目を通していただいたような形でセキュリティ対策基本指針とか基本対策というコンセプトが書かれているものでございます。あとこの中に CIA でいうと、それぞれ機密性、完全性、可用性についてどういうふうなクライテリアになっているのか、これは各府省で統一しないと、ある府省では機密性の高いレベルになっていたものが、他の省庁に持っていった途端に違う扱いになってしまうと、統一の運用ができなくなってしまいますので、こういうものについては統一するというようなことを定めております。

統一基準の一つとしまして管理基準でございますけれども、これには組織と体制の整備とか、これは後ほど御説明いたしますけれども、各府省にそれぞれ最高情報セキュリティ責任者を置いて、その下で一貫したポリシーでマネジメントしてもらうというようなことが書いてあったり、そのほか契約のときにどういうことをやらなくてはいけないかというようなことが書かれております。

技術基準については、例えばプリミティブな方でいうと、省庁の PC にはアンチウイルスソフトを入れなさいとか、あるいは省庁の LAN についてはファイヤーウォールを設け

なさいというようなこと、また具体的にそういう技術についてはどういうふうなレベルのものを入れなくてはいけないのか、先ほどちょっとお話がありました SP 確認、セキュリティターゲットの話もこの中には含まれておりますけれども、そういうようなことが書かれています。

更にこの内容を具体化したものについては８ページでございますが、「NISC Web ページ」と書いておりますが、細かいガイドライン、指針のたぐいを制定しまして、各府省にこれを参考にして自省庁の基準をつくってもらっているところでございます。内容についてはこの Web ページですべて公表しておりますので、ごらんになっていただければ幸いでございます。

先ほど申し上げました組織体制でございますが、９ページを見ていただきますと、各府省ごとに最高情報セキュリティ責任者、基本的にはこれは組織マネジメントになってまいりますので、官房長級の方をそれぞれ職として充ててもらっています。ただし、そうしますと官房長は必ずしも情報システムについての専門家ではございませんので、それをサポートするために右側に最高情報セキュリティアドバイザー、これは主に民間の情報システムの専門家の方を非常勤の公務員として運用しているケースが多うございます。ただし、幾つかの非常に機密性の高い業務に当たっている、例えば警察庁とか防衛省などの場合はこのセキュリティアドバイザーについても内部の公務員を充てているという運用をしております。その下でそれぞれのシステムごとあるいはそれぞれの部局ごとにセキュリティの責任者を定めて、課室のレベルまで情報セキュリティに関するヒエラルキーを構築するというようなことを定めております。

10 ページでございますけれども、こういう体制で各府省の情報セキュリティについての運用を行っているわけでございますが、現在これらについて各府省では毎年１回情報セキュリティ報告書を作成するようにしております。これは私ども NISC の方からああしろこうしろと言うだけではなくて、各府省で自律的にセキュリティのレベルを高めていく、先ほど申し上げた PDCA を各府省のレベルで回していくために現在こういう報告書をつくって、これを公表するという仕組みを今年度から始めております。私ども NISC の方では各府省からセキュリティ報告書を提出してもらいまして、11 ページでございますけれども、政府全体としての情報セキュリティに関する年次報告をまとめるようにしております。この年次報告については１年間のセキュリティの事象について概観するということ、それから、政府自体がどういうことに取り組んできたかについて表示するとともに、各府省で起きたセキュリティの事故についてそれぞれコメントを行うことと、もう一つは各府省でセキュリティに関する取り組みで特に優れた内容について上げてもらいまして、それらをベストプラクティスという形で紹介する。そうしますと、他省庁で行っている優れた取り組みについて自省庁に取り込んでいくことで、お互いにセキュリティの水準を各府省間でどんどん上げていくというような仕組みを年次報告の中で取り入れております。

最後になりますが、セキュリティの監査でございます。統一基準の中でもセキュリティ

の監査をきちんと行いなさいということを定めております。12 ページでありますけれども、現時点では準拠性の監査を必ずやりなさいと、統一基準に準拠する形で各府省のセキュリティポリシーが運用されているかどうかについての準拠性の監査を求めるということです。可能であれば、これは「推奨」と書いてありますけれども、妥当性の監査についても行いなさいと、さらにそれぞれについては可能であれば外部監査を行うことを勧めておりますが、先ほど申し上げたように、秘匿性の高い情報を扱っている機関もあるものですから、最低限内部監査を行うこと。ただし、監査と実施の分離という観点からいうと、情報システム部門ではなくて各省庁の監査・監督を行っている部門がきちんと監査を行うことを求めております。

大変駆け足ではございますが、以上が私ども NISC で実施しておりますセキュリティ対策でございます。先ほど宮内先生の方からも関連の規定についてはよく連携していくようにと御示唆を頂戴いたしましたが、私どもも担当室と同様に内閣官房の中でございますので、今後ともきちんと連携して PIA の観点、情報セキュリティの観点について仕事をしていきたいと思っております。以上でございます。

（宇賀座長）

ありがとうございました。それでは、続きまして関本プライバシーマーク推進センター副センター長、お願いいたします。

（関本副センター長）

ただいま紹介いただきました日本情報経済社会推進協会の関本でございます。本日のサブワーキングは情報保護評価がメインテーマということでございますので、私どもが運営していますプライバシーマーク制度について評価といった観点がどのような形で組み込まれているかということを中心にお話をさせていただきたいと思って参りました。

資料でございますけれども、１ページをごらんいただきますと、まず最初にプライバシーマークの概要をお話をしたいと思います。私どもが今、運用しておりますこの制度は 1998 年、平成 10 年４月からスタートしております。御案内のとおり、当時は民間の事業者に関する法律も当然ございませんで、関連の省庁がガイドラインという形で指導していたような状況でございましたけれども、私どもがガイドラインの１つであります当時の通産省のガイドラインをベースにしてこの制度をスタートいたしました。現在では JIS になっております個人情報保護マネジメントシステム要求事項という JIS Q 15001 という規格番号の規格を基準として運用をいたしております。先ほどもお話がありましたけれども、私どもが認定する単位でございますが、法人を１つの単位として行っております。

１ページのところに図がございますけれども、事業者は JIS に基づいた要求事項がございますが、この要求事項に適合するような個人情報の取扱いをするための仕組みを構築をし、運用する。その構築、運用の状況を内部監査で評価をし、その結果を踏まえて改善を

する、あるいは外部の意見を踏まえて改善をする、そういったような活動を実際にやっていることが認定するための条件であります。そのような状況の事業者に対しまして、私どもが第三者の立場で個人情報の取扱いを行う仕組みの内容及びその運用状況を基準に基づいて評価をし、それに適合しているということで認定をするという制度でございます。現在、約１万 2,000 社の事業者を認定をいたしております。

２ページに移りますと、これは運用の体制でありますので細かい絵で恐縮ですけれども、私どもは JIPDEC と申しますが、JIPDEC が全体の運用管理をしております。そして、私どもの審査をする部分の仕事を指定審査機関というところにお願いをしています。これが現在のところ 18 機関ございまして、右に吹き出しで書いておりますけれども、このような機関が審査機関として私どもと一緒にやっていただいているということであります。ここに組織の性格を見ますと、一般社団法人ですとか、社団法人、財団法人、NPO 法人といったような非常に公的な色彩を持っているところ、あるいは業界団体がございます。これには制度スタートのときの経緯がございまして、先ほど申し上げましたように、制度のスタートした段階では法律がございませんでしたので、そこでそれぞれの業界団体は各省庁の定めていますガイドラインに適合するような形で業界ガイドラインをつくって、先駆的に業界団体の会員に対する指導を行っていたような立場でありました。したがいまして、そのような既に行われている、活動している団体の協力を得ながら適切性の評価をしようということでこのような形の体制を構築して今日に至っているところであります。

この図の中に例えば指定審査機関の中に審査会といったものがありますけれども、今、申し上げたとおり、関連の 18 機関は会員各社の申請を受けて審査するというのが大原則になっておりますので、それだと身内の者が身内の者を審査しているのではないかというような指摘がございます。したがいまして、審査会といった外部の有識者の方々にお集まりいただいて、審査員が審査した結果をもう一度そこで評価することで客観性を保っている、そのような役割を持たせた審査会を設置する、それが義務として指定審査機関としての指定を行っています。

次に、最初に申し上げましたように、事業者の立場あるいは審査する立場で情報保護の評価という意味からどのような活動を行っているのかということで、３ページでは構築する事業者の立場から少し中心の部分を紹介したいと思います。

まず、事業者でございますけれども、個人情報を当然取り扱ってはいるんですが、その個人情報が我が社に何があるかということをまず明確にすることと、それをどのような業務で使っているのかということ、個人情報と業務を結び付けて特定をします。すなわちそれぞれの会社ではあるアプリケーションが動いているわけですけれども、それはまさに個人情報を取り扱う仕組みがそれぞれのアプリケーションで動いているということです。これは１つのシステムととらえてもいいと思うんですけれども、そのシステムが幾つも企業の中には存在している。そのシステム、言い方を変えますと業務と言ってもいいと思うんですが、業務の流れを明確に分析をします。そして、その流れの中で個人情報がどのよう

に推移していくか、どのような取扱いをされているかを分析をするわけです。その分析結果を踏まえてみますと、そこで要求されている、あるいは JIS や法律で要求されていることを阻害するような活動がこの状態で起こり得ないのかどうかという評価をするわけです。その１つとして例えばよくリスクと申しますけれども、法律的に言いますと同意のない取得が果たして今の仕組みで行い得る可能性がないのか、あるいは同意のない提供、目的外利用が起こらないのかという観点から、そのリスクが発生する可能性をここで評価をするわけです。そして、それが発生したときにどのような影響が我が社に及ぶのか、あるいは情報の本人に及ぶのかを評価し、その結果を踏まえてそれを最小化する、リスクが顕在化することを防止する対応策を検討するわけです。したがいまして、ここでの対応策はセキュリティ上の対応策だけではなくて、今、申し上げた法律上のいわゆるコンプライアンス上のリスクに対する対応策も同時に検討して､その影響を最小限に抑えるような選択をし、決定をし、実装をするわけです。そのような状況でそれぞれの事業者が個人情報の取扱いをその実装した仕組みの下で動かしていく。そのことによっていろいろな個人情報を取り巻くリスクから守っていくということで事業者は仕組みをつくっているということでございます。

４ページにまいりますと、今、申し上げたとおり、個人情報の取扱いに関するリスクを評価し、その防止策として仕組みをつくっているわけですけれども、更にその運用段階を見ますと、下段の方でございますが、実際は内部監査によって運用状況をチェックするというような仕組みを組み込む必要がございます。まずは適合性の監査と運用監査ということで、我が社が定めました個人情報保護のための仕組みが JIS に要求されている事項に適合しているかどうかを自らが評価をする。更には各業務部門が取り扱っている個人情報が我が社が定めたルールに従って行われているかを実際に評価する、そういった適合性評価と運用の評価を行うということが１つです。

更にはそのために監査で使用するチェックリストとしましては、影響評価がされたリスク分析結果を反映したチェックリストをもとにして、その結果が実際にマネジメントシステムに反映しているかどうかという評価をまずはします。そして、経済的な理由等でリスク対策が打てないということも当然ございます。そのようなものに対しては日常の点検などで重点的に監視しているかどうかも評価をする｡そのようなチェックリストをつくって、実際に監査をするわけであります。

３番目に書いてあります監査の運用体制です。これは先ほどもお話が出ていましたが、内部監査でございますので信頼性はなかなか難しいところではございますけれども、その組織において他の業務に関わりのない監査の権限を与えているかどうかが重要になりますので、そのような観点でも確保して監査を実施することを求めることになっています。

このように個人情報保護のためのマネジメントシステムは環境変化などにより新しいリスクが当然発生するわけですけれども、そのような新しいリスクによる影響に十分対応できているかといったことも踏まえて評価をする活動として内部監査を位置づけています。

５ページに移っていただきたいと思います。ここではプライバシーマーク制度に基づいて審査の立場からどのようなことをやっているかということでございます。

左側にございますのは、先ほど申し上げた事業者が自ら個人情報の取扱いのための仕組みをつくったということでありますけれども、それに対して第三者の機関としての審査員が行う作業です。まずは事業者における個人情報の取扱いに係る個人情報保護という観点で見た上でのリスクをどのようにして評価をしているかという観点で見る部分がございます。これは当該事業者におけるすべての業務とその業務で取り扱う個人情報が漏れなく認識され、特定されるというのは先ほど申し上げたとおりですけれども、その取扱いにおける影響が評価されているかということをまずチェックすることになります。そして、その業務ごとに業務手順、業務フローと言ったりしますけれども、それにおける個人情報の取扱いに関してリスクが漏れなく洗い出されていることが非常に大前提でございますので、そのリスクの洗い出し漏れがないかをまた評価します。そのようなリスクが顕在化した場合の本人及び当該事業者への影響の大きさが分析されているかということも評価をすることになります。そして、評価した結果の影響を最小限に抑えるための仕組みとして次に評価をするわけです。リスクの顕在化を防止することが当然必要になるわけですけれども、その対策が検討されて、合理的な対策を選択し、決定されているかを評価をします。次ですけれども、当該組織が定めたマネジメントシステムがそのとおりに組織の中で運用されているかということを現場にお伺いをして評価をするという段階、このような３つの段階で事業者の個人情報の取扱いを評価をしているということであります。

５ページの下に書いてありますけれども、したがいまして、プライバシーマークによる認定時における審査は事業者が自ら定めました、あるいは定めるまでの過程で個人情報保護に対する問題点の影響をどのように評価をしているかの評価の適切性をここで確認するという行為だと考えております。

６ページ以降は参考資料程度でございます。

６ページは、私どもが事業者の皆さんから申請をいただいて認定するまでの流れということでありますので、参考までにごらんいただけたらと思います。

７ページは、JIS Q 15001 の全体の構成でございます。ここではマネジメントシステム規格としての構成ができ上がっていることを御理解いただければと思います。

ちょっと１つ申し遅れましたけれども、７ページのところで左側の少し茶色っぽいところがございますが、そこに 3.3.2 という JIS の項番がございます。ここでは「法令、国が定める指針その他の規範」というところがございますけれども、事業者はそれぞれの分野におけるガイドラインを法令や JIS 以外に適合しなければいけないことがここで明らかになっているわけですが、そのようなガイドラインについてもその適合性を評価しているということを最後につけ加えさせていただきたいと思います。以上でございます。ありがとうございました。

（宇賀座長）

ありがとうございました。それでは、高取情報マネジメント推進センター副センター長、お願いいたします。

（高取副センター長）

ただいま御紹介いただきました日本情報経済社会推進協会情報マネジメント推進センターの高取でございます。どうぞよろしくお願いします。

今、お手元にあります説明資料２－２をごらんになっていただいて、最初のスライド、番号でいいますと２でございます。私どもが ISMS 適合性評価制度の運用を始めたのが 2002 年４月からでございます。先ほどのプライバシーマーク制度が 1998 年ですから、その４年後と御理解いただければと思います。

まず、私どもは、情報セキュリティマネジメントシステムについての基準が非常に重要である。それはなぜかというと、制度そのものは国際的に整合がとれなければいけない。ですから、情報セキュリティマネジメントに対する第三者認証制度そのものが、認証あるいは認定という制度のスキームをきちんと国際的な整合性を図る。そのことによって日本における情報セキュリティ全体の向上を目指していく。先ほど内閣官房の情報セキュリティセンターの木本参事官からお話がありましたように、行政機関の情報セキュリティ対策そのものをまさにこの制度を用いてつくり込むことも可能であるということをつけ加えさせていただきます。

３番のスライドにあります適合性評価制度における適合基準が非常に重要でございまして、先ほど申しました認定認証制度という制度そのものを国際的な基準に適合させていく必要がある。その左側にあります認定機関、これは私どもの JIPDEC の情報マネジメント推進センターがこの役割でございます。それから、認証機関は審査をする機関でございますけれども、審査登録機関あるいは認証機関と呼ばれているもので、今、私ども JIPDEC が認定している認証機関は 26 機関ございます。そして、その認証機関が実際に審査をして、認証、ここに書いてある certification と言われていますけれども、ここがまさに認証取得する組織あるいは事業者でもいいですけれども、それに相当します。

それに適合させる基準はこちらの右側にあります ISO/IEC 17011 とか 27006 とか。最終的には ISMS を構築するためには ISO/IEC 27001 という情報セキュリティマネジメントシステムの要求事項に適合させるという意味でございます。

27001 の構造といいますか、構成が４枚目のスライドの「ISO/IEC 27001 の構成」、「ISMS における PDCA モデル」がスライド番号の５にあります。今回お配りされている参考資料６の別紙を見ていただけると、スライドの４と５を一緒にした図があると思います。私はこの別紙を見ていなかったのですけれども、別紙の方が非常によくできているので、私自身、実は全体、PDCA を回して ISMS の確立というプロセスはどうなのだというものを御説明しようと思ってスライドの４と５をつくったのですけれども、こちらの別紙の方を見

ていただくと、まさにここに書いてあるとおり、ISMS を確立し、導入・運用、監視・レビュー、維持・改善していこうという PDCA サイクルを回す。

その中の ISMS の確立の部分がこの下にある図のようなそれぞれのプロセスがある。その中で特に重要なのは、この規格は組織そのものの事業活動全般及び直面するリスクを考慮の下で、ここにありますような文書化した ISMS を確立して、導入・運用、監視・レビュー、維持及び改善するという仕組みでございます。確立する中で、特にリスクアセスメントについて、リスクを特定して、リスク分析し、評価するということはこのプロセスの中にあります。例えば IT のそれぞれの環境が違ってくれば当然リスクも変わるだろう。そういうような要因をきちんと何回もこのプロセスの中で回していく。

そうすることによって最終的にどういったリスク対策をとるかというのがあるかと思います。それが右下にありますように選択する管理策。これが ISO/IEC 27001 の付属書Ａに書かれておりまして、すべてのセキュリティ対策が一応 133 というセキュリティ対策を網羅的に選択するようになっております。中身はここにありますように、１情報セキュリティ基本方針～11 の法令順守に至るまで対策が網羅されている。ベストプラクティスということでございます。

ですから、ここの中で特に言いたいのは、いわゆるベスト追求型の評価をするためにはやはりこういうような仕組みが必要である。その仕組みが 27001 という国際的な標準である。ということは、グローバルに見たときに、フレームワークそのものは世界共通である。ただし、そこに取り込むセキュリティ対策は、先ほどの組織が、自分たちがベストプラクティスを選んでいく。ですから、仕組みは先ほど言いました基準をクリアーすればいいというベースライン的なところではない。そういう意味では仕組みそのものがそれぞれ違うと御理解いただければよろしいかと思います。

最後になりますけれども、今、申しました私どものスライドの７が 2011 年５月現在、今は９月ですけれども、大体 3,800 の認証取得の事業者がございます。

もう一方では８ページのスライド、これは各国あるいは地域ごとの ISMS の認証登録の発行数です。これはグローバルに見たときに各国がどのように認証取得されているかという認証登録の発行の枚数です。日本が 3,840 で、この数字を見ていただくと、ある意味では日本が ISMS に関しては約５割以上、50％以上の認証登録を発行しているという状況がわかるかと思います。

最後の参考なのですけれども、各種ユーザーズガイドをつくっております。いわゆる ISMS を構築するためにはどういうところに着眼すればいいのか、あるいは業種によっても違うだろうと。今回スライドの９を見ていただきますと、例えば医療機関あるいはクレジット産業、それから、法規適合性をするためのユーザーズガイド、そういう視点で各ユーザーズガイドを私どもはウェブで公開しております。これは無償で御提供申し上げておりますので、是非参考にしていただければと思います。勿論政府機関における ISMS のユーザーズガイドも先ほど御説明していただいた内容にほぼ近いものでつくりつつあるとい

うのもつけ加えておきます。以上です。

（宇賀座長）
ありがとうございました。予定の時間は過ぎているのですが、ただいまの御説明に関しまして、もし何か御質問とか御意見がありましたら、１、２お受けしたいと思いますが、いかがでしょうか。
よろしいですか。それでは、本日の議事はこれで終了しました。最後に、参与から一言お願いしたいと思います。

（峰崎参与）
今日はやや時間が押していたかなと感じますが、大変短時間でございましたけれども、ありがとうございました。政府におけるセキュリティ対策について説明されたのは、内閣官房情報セキュリティセンターなのですが、政府におけるセキュリティ対策については、実は初めて私も目にいたしまして、我々も紺屋の白ばかまではありませんが、十分対応していなかったなと感じております。
本日、どうしてもお話ししたいことといたしましては、新内閣が発足いたしまして担当大臣が与謝野大臣から古川大臣に代わりました。社会保障・税一体改革、更に番号制度を含めて古川大臣の下で我々もこれまでどおりしっかりとやってくれということですので、今日のサブワーキンググループの皆様方も含めて、今、ちょうど大綱のパブリックコメントを恐らく整理している最中だと思いますが、またいろいろと皆さん方に御報告をしながらしっかりとした法案作業に向けて頑張っていきたいと思っております。本日はどうもありがとうございました。

（宇賀座長）
ありがとうございました。本日御議論いただきました内容につきましては、事務局の方で必要な修正を加えた上で、次回更に各論点について検討していきたいと思います。それから、今日は時間の制約がございましたので、言い足りないことがあったということがありましたら、御意見を事務局の方に出していただいても結構です。それでは、次回の御案内をお願いします。

（中村企画官）
次回第３回のサブワーキンググループ会合につきましては９月 30 日、金曜日の午後２時からということで予定をしております。場所等の詳細につきましてはまだ未定でございますので、改めて御連絡をさせていただきます。以上でございます。

（宇賀座長）

本日は長時間にわたりまして活発に御議論をいただきましてどうもありがとうございました。以上をもちまして、第２回の「情報保護評価サブワーキンググループ」を閉会といたします。

以上