情報セキュリティ政策会議　基本計画検討委員会
第８回会合議事要旨

１．日　時

平成 20 年 7 月 25 日（金）　16 時 00 分～ 19 時 30 分

２．場　所

砂防会館　会議室

３．出席者

【委　員】

筧　捷彦　委員　　早稲田大学理工学術院教授
木内　里美　委員　大成ロテック株式会社常勤監査役
重木　昭信　委員　株式会社ＮＴＴデータ代表取締役副社長執行役員
下村　正洋　委員　ＮＰＯ日本ネットワークセキュリティ協会事務局長
須藤　修　委員　　東京大学大学院情報学環・学際情報学府教授
高橋　伸子　委員　生活経済ジャーナリスト
富永　新　委員　　日本銀行金融機構局参事役・上席考査役
中尾　康二　委員　テレコム・アイザック推進会議委員（KDDI 株式会社情報セキュリティフェロー）
満塩　尚史　委員　環境省情報化統括責任者（ＣＩＯ）補佐官
（各府省情報化統括責任者(CIO)補佐官等連絡会議情報セキュリティワーキンググループリーダー）
三輪　信雄　委員　綜合警備保障株式会社参与
安冨　潔　委員　　慶應義塾大学大学院法務研究科（法科大学院）・法学部教授
和貝　享介　委員　監査法人トーマツ

（五十音順）

【政　府】

内閣官房情報セキュリティセンター
警察庁
総務省
経済産業省
防衛省

４．議事概要

⑴ 政府機関対策の現状に関する質疑

○　資料４－２にある左右の組織体制は表裏一体の関係にあるのか、ライバルなのか、両者間

のリンケージはどうなっているのかを伺いたい。右側の政府全体管理組織では、各省庁のシステム全体の最適化、このシステムとあのシステムを一本化したら良いというようなことまで含めて検討されているのか。

⇒ 右側の図は最適化に係る取組みということで、体制が各省の中に既に構築されている。左側の図は統一基準に基づき、セキュリティに関して我々はこうして欲しいというものを模式的に示したものである。基本的には各省はこれに沿って、例えば、多くは官房長クラスが就いている最高情報セキュリティ責任者を置き、セキュリティ委員会というものを設け、ポリシーを策定している。それぞれのシステム部門はそれに従い、責任者・管理者を置き、セキュリティ関係の作業をやっていただいているという理解である。また、最高情報セキュリティアドバイザーを置くことが望ましいとしており、現実をみると大半の省庁でそういった方を置いている。右側の業務・システムの最適化に係る組織・体制は、電子政府の評価委員会やＣＩＯ連絡会議、ＣＩＯ補佐官等連絡会議などの各種会議体を数年前から置きつつ、それぞれの役所の中で最適化の検討が進んでいる。最適化はそれぞれの府省で共通する業務、例えば、人事・給与というようなものについて全体で造るというものである。また、個別の省庁の中でも、特に大きなシステムについては最適化計画を策定し、それに従って運用経費・コストの削減などを目指していくということになっている。具体的には、個々の省庁の中に管理組織（PMO）、ＣＩＯを置き、そこにはＣＩＯ補佐官を置くということになっている。ここでは、それぞれのシステムについてある程度の予算要求をする際に、補佐官の方が予算要求調達仕様に関するチェックをかけるという仕組みがある。ＣＩＯ補佐官が集まる連絡会議では、年度の最適化計画実施状況の評価等についての意見交換などを行っている。

○　資料４－１の４頁について。政府統一基準があり、府省庁のポリシーがある。さらに、省庁対策基準があり、政府機関統一基準に準拠及び独自基準を付加するということが書かれている。また、個別マニュアル群についてはNISC が提供し、省庁実施手順が作られるとなっている。ポリシー、政府機関統一基準、個別マニュアル群はそれぞれの中で取捨選択するのではなく全てを使って、さらにはそれにプラスアルファされているのか。

⇒　政府機関統一基準には基本遵守事項と強化遵守事項があるが、基本遵守事項については、これは必ず全て取り込んでいただきたいというものである。強化遵守事項は、システムによって入っていないものがあるが、ポリシーとしては基本的に統一基準全体を準拠していただくことが前提であり、そこに各省庁の特殊性に応じて付加的な基準を加えてもかまわないことになっている。ポリシーの構成も統一基準をそのままコピーするのではなく、使いやすいように構成は変えていただいてもかまわないということになっている。基本はそのまま準拠していただくことになっている。

○　政府機関統一基準に示されている対策の水準は、各省庁の特性によってそれが落ちるということはないと理解してよいか。

⇒　水準を落とすことはない。別な形で実施するということはあるが、基本的にそのレベルは維持していただくことになる。

○　そのチェックは既にされているということでよいか。

⇒自己点検、監査の中で各省庁のポリシーが統一基準に準拠しているかということをチェックしていただいている。そのような形で準拠性を担保している。

○　もう一点、資料４－１の９頁の把握率について、何故文部科学省だけがこのように低いのか。

○　何故ここまで低いかについての理由は、今記憶していないが、こういう報告をいただいており、我々としては本年度中には全て把握をして欲しいということである。

○　把握できなければＰＤＣＡは回らないが。

⇒おっしゃられるとおりである。

○　先の委員が参照されていた資料４－２の２頁について、情報セキュリティ責任者、情報セキュリティアドバイザーは各省庁で明確に定義づけされているか。ＣＩＯ、ＣＩＯ補佐官は比較的耳にし、満塩委員がここに参加されるなどで理解している。ＣＩＯやＣＩＯ補佐官が、情報セキュリティ責任者や情報セキュリティアドバイザーを兼ねているかもしれないが、その方たちが認識をもって、明確な組織的位置づけで活動されているかといえば、必ずしもそうではないのではないかと思う。その辺りが明確になっていないということが、１００％達成されていないことの理由であれば、そういったことも提言できるのではないか。

⇒体制に関しては最高情報セキュリティ責任者を置くこと、と統一基準にあり、全ての省庁で置いているという結果をいただいている。どういった方が就いているかというリストがあり、多くはＣＩＯと同じ官房長、ないしはそれに相当する方である。自己点検において１００％そういう方を置いているという結果をいただいている。最高情報セキュリティアドバイザーは必要であれば置くということになっており、今記憶している限りでは１９府省庁中１８府省庁で最高情報セキュリティアドバイザーが既に任命されている。ＣＩＯ補佐官の兼任というところが多かったと記憶しているが、名目上置かれているだけなのか、具体的にどういった活動をしているかは各府省庁で異なってくると思われる。

○　資料４－１の８頁について、１００％実施すべきとする中で、このように実施されていないという状況のようだが、原因はどのようなものかについて別途分析されているのか。

⇒我々としてはいただいた報告の内容をみており、何故このようになっているかについて細かい分析まではできていない。ただ、ヒヤリングなどを行っていく中でセキュリティを統制していくことについて、教育ができていないなど、弱いところがあると感じているところである。

○　今のタイミングは、いろいろと議論していくという段階ではないのではないか。資料４－１にある取組みがなされていることは理解しており、政府機関総合対策として統一基準が策定され、各府省庁でいろいろな形の検討が行われてきたというのは分かる。情報資産において格付けという表現がされているが、資産を選び出してその重要度を分類、カテゴライゼーションすることはおそらくやられている又はやる方向であると認識している。情報システム資産と一般的な情報資産が混同されており、現状では資産分析、管理がまだ十分なされてい

ないと思っているが、正しいか。

○　情報セキュリティマネジメントということあればリスク分析の話しが必ず入る。日本ではそういったことをしっかりやるところと、基準と照らし合わせてギャップがどれくらいあるかギャップ分析を行い、リスク分析をスキップしてしまう手法もある。これまでやられてきた取組みでは、このリスク分析にはあまり重点が置かれていないという認識は正しいか。

⇒　どの程度リスク分析が行われているかの確認はしていない。当然ながらセキュリティポリシーを作っていくにあたって、リスク分析を行っていくということは前提である。例えば、最適化計画を作る際には業務分析を行い、その中で情報資産の格付けが行われていることは承知している。各省が持っている全てのシステムで、そのようなことをやった上でセキュリティ対策を講じているかということになると、全てについてはできてはいないだろうというのが当方の直感としてある。かなりやられていない部分があるのではないかと感じている。リスク分析、ギャップ分析について、やられているものもあるかもしれないが、多くのところは十分できてはいないのではないか。NISC からセキュリティポリシーを統一基準に基づいて作りなさいと言われ、それをそのまま写して、こういうことをやっていますというのがかなりの部分ではないかと感じている。ただし、正確にはどうなっているかは把握していない。

○　それは把握される予定はあるのか。

⇒　今の段階では、かなり難しいかとは思う。

○　２点ほど質問したい。１点目は資料４－１の７頁以降で、いろいろな項目について評価されているが、例えばこの中で、情報セキュリティ対策の教育、格付け取り扱い制限係る措置、情報システムの台帳整備、職員識別の徹底が挙げられているが、これ以外にも調査をされているのか。あるいはこの４つを代表特性として把握しようと、意図的に取り上げたのか。

○　２点目は、資料４－１の１５、１６頁で企画設計段階からセキュリティを取り込むことが大事であり、推進しているとある。これには全くそうあるべきであり、我が意を得たりという感だ。他方、資料４－２の２頁で、セキュリティポリシーを策定するのは左側の組織でやられ、それを実行するのは右側の体制でやられるのが一般的かと思われる。セキュリティポリシーを決めた、それを企画設計段階から組み込むための方策は、具体的にどのようなイメージで、この２つの組織でどのように行われていくことを想定しているか。

⇒資料４－１の８頁目に挙げている項目は、対策実施状況報告をいただいた上で、全体の平均が９３％程度ある中、それより比較的低い部分を取り出している。このあたりの改善が必要であるということで、政策会議に報告させていただいている。統一基準は四百数十項目あるが、その大半についてどの程度できているかということを一つずつ調査し、その結果については手元にある。その結果を全体分析する中で、この辺に弱点があるのではないかということで示しているのが資料４－１の８頁である。

⇒全体の企画段階でのセキュリティについては、資料４－２の２頁目左図で示す体制で、システム毎にシステムセキュリティ責任者、管理者を置くことになっている。右図では、個

別管理組織、電子政府推進担当課長等は、それぞれのシステムに携わる課長が就いているであろうと理解している。多くは、その方々がシステムセキュリティ責任者という位置づけになっているので、その意味では表裏一体であり、ポリシーを定めていれば当然調達の方でも反映される。ただ、各省の話では、統一基準の中では比較的細かい技術基準が書かれているが、何をすればよいかよく分からない、少し抽象度が高い記述だと、どのように反映してよいか悩むところがあるとは聞いている。

（2）政府機関情報セキュリティ対策における PDCA サイクルの実効性強化について

○　考えられる方向性として、「各省庁が自ら能動的に PDCA サイクルを回せる仕組みを構築」と示されているが、構築する主体がどこになるかについて明確にする必要がある。資料４－２の２頁の図において、それを推進するのは左側の最高情報セキュリティ責任者や最高情報セキュリティアドバイザーになるのかもしれないが、ＣＩＯの役割と比べると最高情報セキュリティ責任者の記述があまりない。包括的に表現したものかもしれないが、「各府省庁における情報セキュリティ対策に関する事務を統括」とあるのみである。仕組みを構築する際、あるいはその前かもしれないが、この最高情報セキュリティ責任者がその役割、その推進役になるのではないか。誰が主体なのかを明確にしておく必要がある。

○　考えられる方向性の２点目で、評価や第三者監査の導入の可能性について書いてある。監査を導入する際には、何と比較して指摘事項が出てくるのか、各省庁が考えるべきものとして基準やベストプラクティス、定量的な基準というものがある。それに照らして、どういうものが不足し、あるいは十分だということになるので、その評価の基準となるものが十分にできていなければならない。それは仕組みの構築の中に含まれているのかもしれないが、重要なことである。

○　３点目の考えられる方向性では、先ほど話で１９府省庁中１８府省庁で最高情報セキュリティアドバイザーという方がいるとのことだが、その方々を十分に活用しなければならないということが書かれているのだと思う。不足があれば、この方々が推進役になる、活躍する形で、その機能を明確にし、PDCA の仕組みを構築するということが必要ではないか。

○　「各府省庁が自ら能動的にＰＤＣＡを」との記述は、一読するともっともそうだが、よく考えれば気になる。各省庁が独り立ちし、立派に旅立って行ける状況になれば、「自主性に任せてきちんとやってもらおう」というのは正論だが、サッカーに喩えると、ジーコジャパンが選手の自主性に任せてオーストラリアに負けた、あのパターンに陥るような気がする。トルシエでもオシムでも良いが、監督・コーチが統制をとる意味で、NISC の役割もなお重要である。一定のレベルまで上がったところ、例えば PDCA が２回まわったところで、３回目からは各省庁で独自路線を歩みなさいという展開でなければ、各省庁がてんでバラバラな方向に行くリスクの方が大きいのではないか。

○　全体的に共通して感じるが、各省庁の分散管理が前提となっている。今の NISC の位置づけ

からすると、今以上にNISCがバランス機能を持つというのは難しいのだろうと思う。各省庁の分散管理型でやると、情報に絡むところは非常に効率が悪い。民間でもそうだが、情報に絡むところは、少なくとも全体を統括するような横断的な強い仕組みがなければ、効率が悪いままに行く。また、自己点検が主体となっているが、自己点検は意識づけとして最低限やってもらう必要があるものであるが、少なくともセキュリティに関しては客観的な監査をきちんとやらなければ、自己点検だけに期待できるものは少ない。分散管理では対応が恣意的になりがちであり、実効性にはばらつきがあるだろうし、もう少しガバナンスが効いた仕組み、最低限客観的な監査をPDCAとして回していかなければ難しいだろう。

○　これまでの委員の意見では、重要な点がいくつか入っている。議論している政府機関の対策の目的・目標は、各省庁が行っているいろいろなことを束ね、全体的に大きな一つのポリシーがあり、それに従った全体のＩＳＭＳのようなものを、PDCAを回して取ろうといった考えではないと思っている。その大きな理由は、各省庁はレベルがかなり違う、または要求条件がかなり違うのではないかと考えるからである。

○　ＩＳＭＳを取るとした場合、ＩＳＭＳは企業単位でも、企業の中の部署単位にも取ることもできる。私の会社でも、はじめは部署単位に取得したが、全社的に取得するためにそれを全体に広げた。そのために、いろいろな部署から委員を出し、委員会を作った。もし、“PDCAの実効性の強化”という言葉を使われるのであれば、誰がこれをやるかということが非常に重要である。これは横からあるいは上からといってよいか、NISCが外からいくら言ってもだめである。各省庁の中できちんと体制をとってやらなくてはならない。また、委員の方々が述べられるように、突然やれと言ってもなかなか難しい。

○　今年度までいろいろやられたわけであるが、正直なところ、企業がＩＳＭＳでやっているようなPDCA、マネジメントプロセスには乗っていない。どうすべきかは考えどころではあるが、監査をうまく使うというということが一つある。それは助言型の監査でもよいかもしれない。助言型では統一基準をベースとして、それがきちんとやられているかどうかを助言してもらう。または各省庁が各自達成できるレベルを明言書で明言し、それに合っているかを保証型で監査をするなど、いろいろとやり方はある。

○　教育しかり、いろいろな観点から各省庁で勝手にやりなさいと言うとかなり難しいので、可能ならばNISCがドライブする横断的な組織があり、そこへ各省庁の責任者或いは担当者が集まって情報共有を行う、ガイドラインを作っていくことが考えられる。先ほど統一基準の中に個別マニュアルがあるという説明があったが、個別マニュアルの一つ一つが、ガイドラインとしてうまくできあがっていけば、それを各省庁に持ち込み、具体的に自分たちで走ることができる。自分たちでいかに走れるようにするかが一つのポイントであるが、各省庁がやる気がない場合にはなかなか難しいのではないか。このような意味で、NISCがドライブするような横断的な組織というものがあり、また監査をうまく使い、早く立ち上げていくやり方が当面はよい。

○　いくつかコメントさせていただきたい。今のお話に繋がるところでは、歴史を若干しって

いる立場で申し上げると、政府機関統一基準ができる前、平成１３から平成１５年だったと記憶しているが、セキュリティポリシー策定ガイドラインというものを作って、まさに自主的に各府省庁でやっていたと認識している。正直、その時は全く進まなかったという感想がある。２、３年前に統一基準ができ、ようやく最低基準が出てきたと思っている。次の段階として、各省でのカスタマイズというか、自分自身でのPDCAということは理解できるが、少し抽象的な言い方になるが、評価方法であるとか、評価したものを見直す仕組みを作るといったところまで手を入れなければならない。そのような仕組みを入れたPDCAを作るというところまでは手伝わなければならないだろう。

○　資料４－２の２頁にある組織体で、セキュリティに関する体制は、上の方に横断的な組織がなく、各省でクローズしてしまっている。NISCへの調査報告はあるが、右側の業務・システムの最適化に係る組織で、政府全体管理組織とあるような情報共有であるとか、政府全体のセキュリティに関する絵図を描く委員会が必要ではないか。それは、情報セキュリティ政策会議も活用できると思われる。右側の体制で重要なＣＩＯ補佐官等連絡会議等、これは民間から来ている補佐官の情報共有会議である。これに相当する会議は是非作っていただきたい。

○　これまで何度もお話が出ているが、各省の中で実行部隊を設定、定義していただきたいと思っている。業務・システムの最適化に係る組織でこれがどこに相当するかというと、これは○○省全体管理組織（ＰMO）になる。実態上はいろいろな部局の情報管理を行っているところが担っている。各省ではＰMOという言葉は浸透しており、実際に業務を行う原課と呼ばれる組織が、ＰMOを認識してくれている。セキュリティに関してもやはり、ＰMO相当の認識は必要であり、実行部隊を明確に定義する必要がある。

○　そのＰMOは実際に各省で働いているか。

○　働いているか、いないかという言い方は難しいが、ある程度機能はしている。右側の組織体では、かなり細かいガイドラインを作っている。業務・システムの最適化の検討にあたっては、このように検討して下さいという標準形をかなり作っている。最低限それをするということだけでも、業務としては少し重いが、少なくともそこを通らないとシステムを作れない状況になっている。セキュリティに関しても、そのような仕組みが必要である。

○　最高情報セキュリティアドバイザーは、ほとんどの組織がＣＩＯ補佐官の兼務になっていると認識している。省庁によるがＣＩＯ補佐官は、大きいところでは３名、４名体制になっている。これも省庁によって異なるが、中にはＣＩＯ補佐官（セキュリティ担当）という業務で請け負っている方もいる。情報セキュリティアドバイザーはどんどん増やしていった方がよい。数字で申し上げると、現在ＣＩＯ補佐官は全省で、正式なメンバーとして４０名前後いる。それに加え、ほとんどがスタッフというものを付けるので、その２、３倍の民間人が業務・システムの最適化には関係している。セキュリティに関して、そこまであるのか各省の事情を全ては把握していないが、そこまではないと思っている。もう少し、最高情報セキュリティアドバイザーが何を行うか研究し、明示していくべき。それが先ほど申し上げた

会議体を通し、横串で繋がっていくのが重要である。また、ＣＩＯ補佐官も補佐官どうしのコミュニティができつつある。これはオフィシャルラインもそうだが、事実上補佐官どうしで連絡をとるということもある。そのような形でコミュニティというものもできてくると思うので、民間活用は重要なことだと思っている。

○　監査については当方が思っているイメージ、ニュアンスは若干異なっている。結果的には同じかもしれないが、内部監査レベルのものが欲しいということである。評価は重要であるが、それと共に今のフェーズでは指導・助言が重要である。外部評価になってしまうと、評価はするのだが、その後の指導・助言は自分で考えて下さいということになり、少しつらいかと思っている。基本的に必要なのは内部監査だと思っている。ただし、これも先ほど申し上げた実行部隊が機能し、それで外部評価があるということであれば機能するものと考えるので、全く否定するものではない。今は指導・助言というものが必要だと思っている。

⇒　一言みなさんに申し上げたいのは、各省の自主性に任せるということは、方向性として考えていない。表現を議論した結果“能動的に”としている。自主性に任せれば進まないことは理解している。セキュリティ対策を行わなければ困ったことになる、セキュリティのことを考えなければ、気になって寝られない、お酒を飲みたくてしょうがないが情報セキュリティをやらないと気になって飲んでもいられない、というふうになっていただきたいということである。これが“能動的”の意味である。自主性に任せるつもりは全くない。任せては全く進まないことは、平成１３年から１５年の間に証明されており、証明されていることを再びやる必要はない。任せるつもりは全くないということは申し上げておきたい。

⇒ 政府全体で一つの基準を全体にインストールし、それでよしとするかについては、各省庁のリクワイヤメント、デマンドがそれぞれ異なる。例えば一つの企業グループのように、それぞれ全く違う業務を行っていて、要求レベルが全然違うということが前提になっている。これまでは、最低限とるべき対策を統一基準とし、底上げ型にして、評価結果で改善勧告を行う牽制構造をもち、各省の中できちんと作ってねという構造を考えてきたところがある。これも結局はやりたくないということもあり、先の委員が述べたように、盛り上がらなければおざなりになってしまう。元気があれば何でもやれるはずであるが、元気がないのでやらない、ネガティブスパイラルの中に落ちてきている。その中でどうすればよいか、これを考えなければだめだということがある。これについて検討課題と考えられる方向性の１項目（政府機関情報セキュリティ対策におけるPDCAサイクルの実効性強化）、２項目（行政情報システムの最適化の取組みとの関係に係る検討）として挙げている。

⇒ デマンド側としては、3項目の事業継続性に係るものについては、各省庁関係なくやらなければならない。今地震が起これば、政府が潰れてしまう。今は何も対応できないと思っている。

⇒この中で説明責任というのは、一番役所が嫌う言葉であり、とにかく出したくない、見せたくない、都合が悪いものは棚の奥にしまっておこうという世界なので、この辺は牽制しなければならない。

⇒役人に対する幻想というものがあり、言われたことはきちんとやると１００回聞いているが、きちんとやらないので、きちんとやると言ってやらないものをどうすればよいかということを考えなければならない。この件に関しては、４年間やって相当腹立たしく、ストレスを感じる。各省庁の担当者を見るたびに怒りが湧き上がる状態であり、やれと言ってもやらない、不信の構造になっている。それはあまりよくないということで、少しは信じていただきたい、信じた上でやれという強制ではだめなので、自ら能動的にという表現になっていることはご理解いただきたい。

⇒　各委員及び補佐官から意見をいただいたが、“能動的に”というのは自主性に全く任せるということは想像していない。きちんと自ら考えることを行って欲しいということで、そのためにこういうことを考えてみてはどうかということである。NISC から言われたことを単にやるよりも、はるかに大変になってくるのは事実である。そこで考えられる方向性として想定しているのは、いくつかの企業で既に行われている情報セキュリティ報告書を出してはどうかということである。情報セキュリティ報告書は、その企業がどのようなリスクを抱えているのか、それに対してどのような対策をとるのか、その結果どうなのか、それをどのように改善していくのかというものである。

⇒先ほどリスク分析がどこまでやられているかという問いがあったが、ほとんどやられていないのではないかと危惧している。自分たちの役所でどのようなリスクがあると思って、どのようなことをやろうとするのかは、それぞれの役所で決めてもらいたいということである。どのようなシステムがあって、どのようなプライオリティの下で、それぞれの役所がセキュリティ対策を講じていくのかということを考えてもらいたい。端末一台が単独でその辺にころがっているものに対して、統一基準を全て満たしていくというのはナンセンスなのかもしれない。そうではなく、大きなシステムについては強化遵守事項も含めて、どのようにプライオリティ付けを行うのかを考えた上で、対策を講じていただく必要があると考えている。

⇒そのような報告書を自分たちで策定していくということになると、自分たちで何がリスクなのか、何をやらなければならないのかを考えていただく必要がある。それをどのように評価するかについては、先ほどお話があったが、どういうところを最低限評価しなければならないのかについてはNISC が示すつもりである。それ以外の部分をどのように評価するのかについて、それぞれの役所で競っていただくということもあるかと思う。最低限だけをやればよいというところもあるかもしれないし、このような観点で評価をして、このような対策を新たに加えていくということを考えていただくのも重要かと思う。報告書を作り、自らの責任で公表していただくということが一つ有り得るのではないかと思う。ただし、これを来年の初めにやれというのは、第１次基本計画の下で統一基準を導入した際の各省の状況を考えると、そこまでは難しいだろうと考える。我々としては、最終的に次期基本計画の期間が何年になるかは分からないが、２年目、３年目くらいに徐々に報告書を作っていくということを考えていきたい。そのために初年度、NISC と各省で協働しながら、どういったものを作

るかといったことを調整していきたい。

⇒その際の専門家の関与については、今あるようなＣＩＯ補佐官連絡会議を利用させてもらうことも考えられるし、あるいは別な組織をつくるなどあるが、個別の省庁が報告書を出すだけではなく、そういったところを通して、周りの専門家に揉んでいただき、意見交換をしながらレベルアップを図るというような仕組みも大事である。個別に報告書を出すというだけではなく、そのような牽制も必要かと思う。あるいは報告書を公表する際に、役人である最高情報セキュリティ責任者の方自らが発表していただくなどがある。これは役人の性として、上司に何か言わせようとすると、恥をかかせたくないので、きちんとやらないといけないということも働くのではないかとの期待もある。こういったことを考えてみることも、能動的という趣旨で、それぞれの役割の中でどのようなことをやるのかについても次期基本計画の中で考えていきたい。

○　PDCA の実効性強化に関しては、とてもよいことが書かれていると思っていたが、お話を伺っているうちに不安になってきた。能動的と書けばよいのか、それで実効性が確保できるのかということが心配である。ここにある「自らが目標とマイルストーンを立てて、自ら対策を推進している」のが大事だとあるが、その通りであると思う。評価をする際に、計画に対して評価するのではなく、目標を達成できたかどうかで評価をしてもらう必要がある。そのためには目標の設定が何よりも大事で、どうしてそのような目標を立てたのかを説明していただく必要がある。それはどのような現状を踏まえたものか、結局 PDCA に戻ってくるが、目標について各省庁を集めて説明責任を持たせて説明していただき、目標をオーソライズするような会議を設けて、その目標を達成できたかどうかで評価をするような具体的な仕組みを作っていただければ、実効性が担保できるのではないか。

○　“自ら能動的な”という私も捉え方を間違うような言葉は改めていただきたい。この文章から全て“自ら”という言葉は取ってしまったほうがよいというぐらいに思っている。その理由は、先ほど別の委員も述べられたが、私のイメージからすると各省庁は一つの企業グループの事業部としか見えない。つまり、どれか一つが無くなっても全体に影響を及ぼす。ある省が潰れたとする、機能不全に陥ったとすると、国家として動くのかといえば動かない。それは企業グループも同じである。企業においては、影響が弱いところに関しては自主性に任せるが、今の府省庁では、そのようなことは有り得ないだろうとしか思えない。個々でセキュリティ対策を決めるということは有り得ないだろう。全体を考え、その中で対策をとっていくしか有り得ない。それを任せていくというのはまずないだろう。過激な意見であるが、各府省庁が能動的に PDCA を回せる仕組みというのは有り得ない。PDA はよい、C は外に出せ、C だけをやる機能を作る、C はその C をやっているかどうかを、その中で PDCA を回すというような考えしかない。

○　第三者監査という意見がいろいろ出されてきたが、監査というものはセキュリティ度を保証するものではない。その幻想を抱かないようにしていただきたい。つまり保証するのは基準とか、標準とかそのようなものである。監査をやったからセキュリティがＯＫというわけ

ではない。それが全体の文脈の中で、誤解を及ぼすようなところがあるのではないかという危惧はある。それは改めていただきたい。

○　評価書の公表という話があったが、では公表して誰が読むのか、誰がみるのかといったときに、これは基本的に国民、一般の人だと思う。そういった方々が、それをどうやって評価するのかといえば、おそらく分からないだろう。今、企業のセキュリティ報告書が出されているが、それが一般の人々に分かるかといえば、分からない。では、同じようなものを作って効力があるのかといえば、それはないだろう。やはり、評価書或いは報告書を評価する仕組みがいる。そういったものを作らないとしようがない、そこは勇気をもって踏み出すべきである。

○　実態は想像以上にひどいということが、だんだん分かってきた。なんらかの形で強制力が働く仕組みを作らなければならないと思う。それは３つのステップ、即効性があるもの、短期のもの、中長期的なものを作っていく必要があるだろうと思う。中長期的にはガバナンス機能を持たせて、全体最適化であるとか、リスクのコントロールであるとかの仕組みを考えることだろうと思う。当面について、なんらかの形でそこに活動を引き起こすには何が一番有効かと考えていたが、実態を公表される、格付けされるというのが一番いやらしいようなので、一番いやらしいことをやる、見せていくことを繰り返しうるさく言うことによって次のステップに行けるのではないか。そこは敢えて避けずにやらなければ、次のステップに進めないのではないか。PDCA が循環するきっかけは、そのようなことをやらなければできないのではないか。即できることは、そういうところから始めることではないか。

○　非常に重要な指摘、少しラディカルな意見もあり、実行可能性という点でも考えなければならない。基本的にはNISC のチェック機能が極めて重要である。やはり指標を作成する権限はNISC がある程度持つと同時に、それを各府省庁と話し合って、実行可能なところにもっていかなければならない。やはり、ここに書かれているように創意工夫は必要であると思う。全く言われたとおりに、スレーブの状態でやれというのは、みなやる気をなくしてしまうので、NISC がチェック管理機能を持つけれども、同時に各府省庁の自発的な創意工夫を評価してあげられる体制、それをやらないところは低い評価を受けるというようなことも必要なのではないか。そういった点を含め、本日いただいた意見を事務局でまとめて、また繰り返し討論する機会があると思うので、第一のテーマについてはまとめさせていただきたい。

（３）行政情報システムの最適化の取組みとの関係に係る検討について

○　情報システムの最適化は重要である。政府の情報システムにどんなものがあるか知らないが、「標準的なシステムについては、各種の設定パラメータを標準仕様として示すことを検討すべき」とは、妙に細かい話のように感じる。実効性という意味では大事かもしれないが、より大きな話として、同種のシステムが多数存在するならば、共同・共有化して政府ＳａａＳのようなものを作り、それをサービスとして利用するなど、情報システムをリストラして

しまえば、各種の合理化効果が一挙に生まれ税金も安くなる。そうした効率化したシステムを誰かが責任を持って見るようにするのが最適な姿だろう。一挙にできないとしても、長期スパンとしてそのような道筋を匂わせる、すなわち、いきなり設定パラメータの話より、システムの共同利用などの方向を考えた方が、メリットが大きいと思う。

⇒ パラメータの標準使用という話は、米国政府が進めているスタンダード・コンフィギュレーション・システムというものがあり、政府内で軍も含めて１５７万台であったと思うが、その中で一般行政事務に使われるウィンドウズシステムについては、各省庁に技術仕様を決めさせるのではなく、標準的なパラメータセットとアプリケーションセットを決め、それに応じた導入をするというものである。どの省庁でも、個別にカスタマイズせずに、ＳＥ側も導入側も対応でき、マネジメントコストを下げる効果が高いということで始まっている。昨年は６万台、今年で４０万台ほど導入されていると記憶している。これから３年間程度で、全て導入されてるということで進められている。これは、ＴＣＯを強烈に下げるという効果があり、全ての省庁に張り付いているオペレータも他の省庁を同じようにみれるようになる。サーバは別であるが、これを行うことに関して米国政府も含め、非常に高い評価をしていることもあり、調達との関係で非常に難しいが、こういったことも考えていくべきではないかというコンテキストが一つある。もう一つは、官房５業務の共通化、今の委員が述べられた同じような業務は共有化しろというような話がある。これはここでの話ではなく、最適化での取り扱いとして行っている。これはＴＣＯを下げる、ＸＰであるとかＶｉｓｔａであるといった、各省庁がバラバラで入れているＰＣを統一的に設定してはどうかというものである。行政官が机の上でやる仕事で、必要なアプリケーションは決まっているだろうという米国政府の仮定があり、これは概ね当たってはいるが、日本にもそれがあるだろうということである。

○　最適化と一体となった取組みの必要性があるのか、ないのかといえば、これは是非お願いしたいと思っている。具体的な話として、資料４－２の２頁目の業務・システムの最適化は、こちらは総務省の行政管理局がやられており、左側のセキュリティに関してはNISC でやられている。共通システムのセキュリティはどうするかについては、担当部署としてはセキュリティを意識してやっていただいていると思うが、融合的に両者が結びついていないので、是非お願いしたい。

○　最適化の方では、要求仕様を固めるにあたって業務レイヤであるとか、アプリケーションレイヤ、データレイヤといった各層の標準化を進めている。ガイドラインでこのように検討して下さいというものは作っている。それは業界も含めて読める形で、何年か進めてきている。是非これに、セキュリティの機能をどのように検討するのかについて、入れていただければと思う。

○　今の最適化に関わるものは、共通業務系のものと年間運用費が一億円以上のものである。これらについては、必ず最適化を行うということになっているが、運用費が１億円以下のものが多々ある。そのような小規模システムの標準化という意味でも、先ほどお話があったク

ライアントＰＣのセキュリティ・コンフィギュレーションを、クライアントだけではなくもう少し広げたほうがよいのではないかと思っている。また、１億円以上というのは最適化の一つの判断基準であるが、なんらかの基準というものは必要であると思っている。基準を設けて、システム調達をするときに要件を決めるといったことは必要である。

○　第１次基本計画でやられているセキュアＶＭやＧＳＯＣをはじめとしたセキュリティ機能が、各府省庁共通になっていくのではないかと思われる。ＧＳＯＣはまさに共通になりつつあり、セキュアＶＭも今後なっていくのではと思っている。それに関する全体絵図はどこかに描いておいた方がよい。これは最適化に携わっていて悩むところでもあるが、最適化の全体絵図が明確でなくなってきている。資料４－２の９頁にあるＩＴ政策ロードマップの記述にある、「電子政府を強力に推進するための新たな「司令塔」機能も併せて強化する」ということが、最適化計画の全体絵図を描くことに関係するのではないかと思っており、セキュリティに関しても全体絵図を描き、ロードマップ等に入れ込むのがよい。現実論はお任せするが、全体絵図としてはどこかで抑えた方がよい。

○　資料４－２の９頁のＩＴ政策ロードマップについては、事前に事務局に説明はしていたが、これは次世代電子行政ワンストップサービスのグランドデザインを実行するための法改正であり、登録申請業務での添付資料は徹底的になくすというものである。できれば、政府府省庁間のシステムの疎結合で、データをＸＭＬベースで全てやり取りできる環境にし、例えば特許等の申請行為をした場合に、本人確認のために書類を持って来いといわれるようなことはやめよう、システムを連携させて本人確認させればいいだろうというものである。そのために紙の文書を使わないで全てを完結させるために今の法制をどうするかということをやっていただこうというものである。これを考えると、今ある最適化がかえって邪魔になる可能性がある。電子政府評価委員会でみせていただいている限り、この最適化は各省庁で統一的な最適化になっていない。各局の最適化になっており、部局間のデータのやりとりは不可能である。府省庁間のやりとりは更に不可能である。ましてや民間や自治体とのやり取りは全くできない。これは防がなければいけない、法制もいじらなければならない。最適化のコンセプトも変えていかなければならず、共通基盤を造る、ＳＯＡ的な発想で攻めていくということを明確に出した。その中で、セキュリティも守る体制を作っていただきたいということである。グランドデザインはＩＴ戦略本部で掲載されているので、各委員もダウンロードして読んでいただきたい。

○　最適化の取組みの内容は、実態的には個別最適にとどまっている。電子政府進める上での全体最適にはなっていない。そういった最適化の取組みと一体となって、セキュリティを進められては困ると思っている。セキュリティ対策は個別最適では水準が保てないので、最初から全体最適という概念で進めなければ意味がないのではないか。

○　「システム調達に際して、一定以上のセキュリティ要件を求めるシステムに係る基準」とあるが、セキュリティ要件の具体的な内容、姿がよく分からない。何を要件としたいのか。セキュリティの対象もそうであるが、外からの攻撃であるとか、内からの漏洩であるとか、

システムサービスの障害、障害対策であるとかといったものなのか。また、セキュアプログラミングのような概念をきちんと取り込めということなのか、なにか起こったときに追跡できるフォレンジックの仕組みを考えておけというのか。どのようなことを要件としてイメージされているのか、もしあれば教えていただきたい。

⇒　現行の統一基準ではいろいろな遵守事項が書いてあるが、それぞれに対してどのように実装すべきか、ものによっては必要に応じてであるとか、重要なシステムについてはと書いてあり、それがどのような場合にあたるのかというのは、各省の判断に任せているということが背景にある。基準としては網羅的に書かれているが、実際のシステム開発において、この機能を入れなければならないのかというのは現場の判断が入ってくる。セキュリティ・バイ・デザインのところで、この基準はどのようなことを求めているのか、どういう場合に入れればよいのかということをできるだけ細かく示したいとは思っている。これは全くの例であるが、個人情報を何万件以上扱うシステムがあった場合に、そこでは標準的にどういったことをやらなければならないのか、また電子申請で公的個人認証を求めたりする場合に、このようなものについてはＩＤ、パスワードだけで構わないなど、どこまで細かくできるかは分からないが、設計側でどこまでやればよいかということを示すことができないかということである。

⇒　何かあったときに責任を取りたくないということもあり、きつい方に全て倒すということが起こる。やり過ぎで、非常にコスト高なシステムをつくる。外形標準的にこれはここまでやる、これはやらなくてもよいということ示せるところは示しておかなければ、身動きがとれなくなってしまう。息苦しい空間になってしまい、ここまでやるのかと冷め冷めとして目で見てしまう。責任がかかってくると全てきつい方に倒す病にかかってしまっているので、外形標準的にスパッときって、少しものごとを考えるようにできればよいと考えている。

○　今の外形標準的に取り組むということは、まさしくそう在るべきで大賛成である。概念が混乱しているかもしれないと思うのは、「調達物品についてある程度の類型化とその基準化」とあるが、他方別のところで、「システム調達に際して、一定以上のセキュリティ要件を求めるシステムに係る基準」とある。調達物品に対してセキュリティポリシーを適用しようとしているのか、システムのセキュリティポリシーを決めようとしているのかは、はっきりさせておいたほうがよい。セキュリティポリシーというものは使い方も含めたシステムに対して適用されるべきであり、非常にコストがかかる場合はマニュアルコントロールも含めた解決を図るということをシステムのポリシーで定め、それぞれの機器でどうするのかは実装の問題であるので、一定の基準を定めるのは難しいのではないか。システムについてカテゴリーＡ，Ｂ，Ｃ，Ｄのような形で類型化を行う取組みをやっていただけたらありがたい。

⇒　既に書かれているものからの引用で「物品」と書かれているが、場合によっては先ほど端末等の物品もあるが、広くシステム全体として考えたいところである。

○　いろいろな標準的なセキュリティの要件を求めるためのシステムの基準というものを考えると思うが、おそらく省官庁の中にあるシステムは非常に重要なきついレベルを求めるもの

から、どうでもよいようなところまであると思う。全て同じ基準を適用するのではなく、一般的には、１０００システムあったとすればそのうち１００は重要なシステムなので、それについてはしっかりやりましょう、ここの部分についてはそうでもないので標準的なテンプレートで行きましょう、という差別化、クラシフィケーションがある。既に議論があったが、情報又はデータがどういった重要性があるのかについては、各省官庁は既にやっているので、その重要なデータを扱っているシステムは重要であるなどのクラシファイをするようなものも必要な気がする。全体的な流れは悪くないと思うが、その辺も含めた検討が必要である。

⇒　その辺も含めて考えていきたいと思っている。これまでもシステムの格付け、情報の格付けなどがあり、我々としてどこまでできるのかということは、是非この次期基本計画の中で考えていきたい。アメリカでは様々なシステムの格付けを行っているが、それが果たしてうまく回っているかなどを検証しながら、日本であればどういったものが在り得るのか、場合によってはかなり大きな外形標準になるかもしれない。それより更に一歩進めたものがあるのであればチャレンジしてみたい。そのようなことを考えたいと思っている。

（４）政府機関における機密性の高い情報の保護及び事業継続性確保に係る検討について

○　機密性の高い情報については、想像力をたくましくすればいろいろあると思うが、本当に機密性の高い情報はシステムに載せない方が良いかもしれない。このような言い訳の下に、穴が開いて漏れていくようであれば、好ましくない。そのことの傍証として申し上げると、ＩＴベンダーの金融系共同センターを立入調査する際、時々個別情報の存在を理由に「立入りは困る」と断って来るケースがある。システムをチェックする立場からは、個人の預金残高等など機密性の高い個別情報を見なくても調査はできる。機密性を盾に「自主的に運用するから任せてください」という閉鎖性は、弊害の方が多い可能性を感じる。

○　「国の根幹的活動にかかる業務については、事業継続性の観点から具体的なコンティンジェンシープランの作成を求めるべき」という論点をそのまま読めば、現状ＢＣＰが存在しないということであり、金融界では有り得ない。本当に「無い」ということであれば早急に作らねばならない。そうではなく、さすがに「有る」という前提で、政府機関の事業継続性確保のための施策に関して検討するならば、「ＢＣＰのテストや訓練を徹底してやる」ことが対策になる筋合いだ。テストもシステムでいう単体テストではなく、総合テストに当たるストリートワイド訓練のような、省庁だけではなく重要インフラも民間企業も含めたものを、シナリオブラインド型（予めシナリオを明示せず、次々に課題を与えて複雑化していくタイプの訓練）でやることが望ましい。金融界でも課題として取り組もうとしている段階であるが、このようなレベルを向こう３年以内くらいには目指していただきたい。

○　アメリカの金融の危機管理の担当官とパネルディスカッションを行ったが、今述べられたようなエクササイズを繰り返し繰り返し、民間と連携して行っている。ＢＣＰは必要になろうと思う。総務省が今年の６月くらいに各自治体に対して事業継続性確保のための指針を出

しているので、それも参考にするとよいと思う。

○　過去、金融の仕事をしたことがあるので、レベルとしてはかなり悲しいものがあると感じる。今どのレベルまでできているかとみてみると、防災計画に基づいたＢＣＰがオンゴーイングという認識である。ＩＴのテストだとかのレベルまでは行っていない。防災計画に基づくものであり、障害であるとか、もっと別の災害、火災だとかの話になるとまだまだだなと思っている。実行レベルでは作るしかなく、３年以内にはエクササイズをするところまでもっていくべきだとは思っている。その中で、バックアップの体制の政府横断的な検討というのは重要な視点である。ＢＣＰＧでフルサービスの確保はしなくてもよいのではないか。行政のサービスでも、情報提供が一番多いので、そのようなところは勘弁していただき、通信手段はもちろん確保するイメージだとは思う。その場合、バックアップ体制はかなりの縮小体制、縮小運転でいけると思う。今のところ各省で検討しているので、バックアップセンターをどうするかということも個別に検討している。関東大震災レベルを考えるとみな移らないといけない、ただし縮小できると考えると、もしかすると共通化もできるかもしれない。火災などを考えると、全てが一度に潰れるわけではないので、その点でも共通化は考えられる。バックアップ体制を政府横断的に検討していただけるのであれば、大変助かると現場をみていて思う。費用が高い低いの問題ではなく、費用の認識として日常使わないものであるので予算上の理解が難しい。できるだけ極力お金がかからない形で行っていくべきなので、横断的な検討は是非お願いしたい。

○　機密性の高い情報の保護に関する検討ということで、先の委員からそういったものはシステムに載せないほうがよいとの意見があったが、防衛省など、どうしても扱わざるを得ない省庁もあろうかとは思う。

○　載せない方がよいというのが趣旨ではなく、それを口実に自主性に任せることにはひっかかるというのが趣旨である。

○　その防衛省に関して、防衛省改革会議で興味深い報告書が出されている。不祥事の分析と改革の方向性ということで、我々が議論したことも書いてある。この辺は参考になるので、もし委員の方に配っても問題がないようであれば、配布していただきたい。結構よい報告書である。

○　官邸のホームページからも報告書はダウンロードできるようになっているので、容易にご覧になることができる。報道等では組織改編ばかりが注目を浴びているが、給油量の取り違え事案から始まり、情報流出であるとか、イージスであるとか、あたごなど、何故防衛省でこのようなことが起きるのか、起きるのは防衛省の風土あるいは組織文化に改革すべき点があるのではないか、改革すべき点があるからこそ文民統制の組織改革というようなことが述べられている。委員長が述べられているのは、そのような流れがこの場でも参考になるだろうということだと思う。

○　アカウンタビリティに関しても、何故これを国家安全保障として扱うかについてもきちんと説明を行うべきと書かれているようだが。

○　広報をどうすべきかということで、書かれている。我々防衛省職員に対しては、規則遵守の徹底、プロフェッショナリズムの確立、全体最適を目指した任務遂行優先型の業務運営ということが指摘されている。

○　事業継続性も全て絡んでくるので、結構よい報告書になっているのではないかと思う。

○　先ほど別の委員からご指摘があった点について、防衛省には機密性の高いシステムがいろいろとある。政府機関統一基準は、最低限守らねばならない基準だと考えるので、防衛省の全システムには訓令という形で、全て防衛省用語に書き直して適用している。更にその上を目指すため、独自の厳しいものを上乗せした運用になっている。

○　機密性の高い情報の保護に関しては、ある種自主運用するところも必要かとは思うが、日本の組織活動の多くが、情報閉鎖型の活動であるため、歯止めの問題がある。自主管理が拡大することには歯止めが必要である。カブ・ドット・コムのような公開型の活動を行っているのは非常に珍しい企業で、なかなかあのようにはいっていない。ある枠組の範囲内での自主性にとどめるべきであろうと思う。どのように歯止めをかけるかは非常に難しいと思うが。

○　コンティンジェンシープランは、リスクのある全ての業務に対して必要となるはずである。それは、影響度と発生確率をマッピングし、対応パターンを標準化しなければできない。これは軽い対応でよい、これはきっちりやらなければまずいということをリスク的にみてコンティンジェンシープランを作っていけば、それほど大変なことではないと感じている。全体像をつくる、標準化していくところは結構力がいるかとは思う。

　⇒　今委員が述べられたとおりで、各省庁がリスク分析なりリスクのプラオリタイズを行っていなければ、コンティンジェンシープランはできない。現状では、やっていないとは言わないが、リスク分析、アセスメントを自らの手でやっているところは少ない。その上でかつ、政府全体としてみたときにリスクシナリオの共有ができていないと、各省庁の中でプライオリティをつけてやれない。唯一できているのは、首都直下地震だけである。首都直下地震に対してのＢＣＰを作れというのは、中央防災の方からも出ていて、それに対して我々もお手伝いをしている。次のステップ、他のリスク、どれだけリスクシナリオがあるかについては、全体最適を行っているわけではないので、各省庁の中ではあるかもしれない。そのとき、全てが重要な機能だというようなことが起こってしまい、そこが一番難しいところであると思っている。どうしても作らなければならないものは別として、財政状況をみれば、各省庁が独立でバックアップ体制をつくれるわけがない。コスト最適化は各省庁毎にやっていてはできない。ここが、部分最適から全体最適への切替をなんとかしなければならないという問題意識である。ＢＣＰから切り込んでいけば、省庁最適ではなく全体最適へのステップがみえるかもしれないという意味でのチャレンジである。そのためには、リスクシナリオのシェア、リスクアセスメントを能動的にやるということがないと、全くできない。これが、鶏と卵の状態になっており、そこをどうほぐすかということが難しいと感じている。

○　政府全体の全体最適を求めるのか、ある省庁毎の自主独立性の範囲でしばらくやってもらうのかという判断は、最終的には政府全体最適を求めるということになるのかもしれないが、

各省庁毎にＰＤＣＡを回すということの関係をよく考えなければならない。

⇒　それについては、基本的に政府内のラフコンセンサスはあると思っている。一定の秩序回復が行われたリカバリーのフェーズにおけるバックアップと、何かが起きた後、例えば７２時間なりにレスポンスをするという、しのがなければならい期間のフェーズを分けて考えなければならない。レスポンスの部分は、今の政府ではほとんどが官邸主導で行われる。そこには、いろいろとプライオリティが付いており、それに応じたバックアップが考えられるというのが、まず第一段階である。首都直下地震では、リスクシナリオが共有でき、かつ各省庁の機能が官邸主導でどれだけ動いていくかということに対して必要なものは何なのか、人命の救助等、レスポンスの段階では何が起きるかは別として、起きたときの体制のドライブは比較的シェアされている。そのことに関しての横断的な判断というものはおそらくいるのだろう。最初のしのいだ後、ある意味で秩序回復ができた状況では各省もどうするかということを考える。危機管理においては、このように２つのフェーズの体制にならざるを得ない。

○　とりあえずの対応をどうするかという問題は、今のＡｓＩｓ（アズイズ）ベースで作られているとは思うが、将来的にシステムのつくりにおいて、各省庁でバックアップをつくるのは大変だから、政府全体で仕組みを統一していく必要があるということに踏み込むのであれば、各省庁毎にPDCA を回す仕組みだけでは足りなくて、全体最適を回す仕組みも同時に提言する必要がある。

⇒　ここでは、第一ステップとして、本当に乗り切らなければならないところに関して、どれだけやれるかということからだと思っている。実際に政府全体を横断的に検討するといった場合に、横断的に対応しなければならないときとは何なのかというと、リスク意識のシェアというところで合意できなければできない。地震以外はそのレベルすらできていない。ＡｓＩｓ（アズイズ）でやるには到底遅い可能性があるので、そこはまずやろうということである。その次の段階については、各省庁毎に共有できる形でリスクシナリオを作っているわけではないので、そこは難しいと考える。

○　おっしゃることはよく分かる。そこをやはり全体最適を求めて、政府統一的な仕組みまでやっていこうというのか、将来的な課題なので当面はコンティンジェンシープランを各省庁毎に作ってもらうという最低限のところでがまんするというのか、そのスタンスをはっきり書いた方がよい。

⇒　そう思う。その意味では実利をとるために最短でやるべきだと考える。実際にはできていない、コンティンジェンシープランは作ったがおそらく訓練はしていない、訓練の錬度も上がっていないだろうし、検証、横断的なテストもできていないだろう。全体最適をやるための枠組ということで各省庁とやるよりも、先に実利を取るほうがよい。地震はいつくるか分からない。

○　全く賛成である。コンティンジェンシープランを作ってもらい、年に一度くらいのリハーサルをやり、その実施結果を集めるということが最初の目標としては実効性が上がるのでは

ないかと思う。

○　この議論はもっともだと思う。脅威、リスクから発生するインパクトで、全体の省官庁にまたがるような、首都直下地震であるようなもののＢＣＰは早く確立しなければならない。各省庁の中で、この重要システムが止まったような場合にはどのようなプロセスで回らなければならないかというようなことも考えていただかなければならない。各府省庁の重要なシステム、情報のバックアップ体制について、バックアップのやり方や連携の取り方についてはお話があったが、バックアップシステムの全体での共有、各省庁の重要なシステムを一箇所に集めて体系的に管理する、何かあった場合にそこへのコントロールを統制するといったところまでは述べられていないということでよろしいか。

⇒　議論結果としてそうなるのであれば構わないと考える。１年半程前に報道等で政府統一バックアップセンターといった記事が出て大騒ぎになったが、事実ではなかった。議論の結果としてそういったものが必要であれば計画に書くが、それを前提として全てを集約すべきとはしていない。

（５）政府機関における人材の確保などに係る検討について

○　本日一番強く言いたいメッセージとして、この人材確保論はフレージングがずれている気がする。何故、外の人に任せようとするのか。それは、何かＩＴを他人事扱いしているからではないか。大事なことは「コアな人材は内部に育成する必要がある」という点である。組織の風土や業務を分かった上でＩＴ化やセキュリティを考える必要がある。アドバイザーは助っ人として必要としても、所詮助っ人だらけのチームはジャイアンツのように優勝できなくなる。外部専門家というのは大いに怪しくて、ここにも外部専門家の方々がいらっしゃるが、各々かなり異なる意見をお持ちである。外部専門家は何でもできる救世主であるといった幻想を信じてはいけない。語弊があるかもしれないが、学者っぽい人でも、評論家っぽい人でも駄目で、実行力のある実践家でなければならない。官庁には日本一優秀な人が集まっているはずなので、その方々が自分の省庁の中で育っていく仕組みを作ることが抜本的な対策である。前回申し上げたような、２・３年で回る人事ローテーションの見直しを含めて、中長期的でもよいので、考えねばならない。「外人部隊を雇ってくれば良い」という時代は卒業すべきであることを、強く主張しておきたい。

○　事前に事務局と話す機会があったが、そのようなアウトソーシングについて、ＣＩＯ補佐官が複数いて、統括ＣＩＯ補佐官になるような方をきちんと育てなければならないし、高い給料を払ってでも外から雇ってきて腰を落ち着けていただかなければならないということを申し上げた。業務毎のＣＩＯ補佐官は外部から採ってきてもよいが、それを統括して組織全体の最適化を図らなければならないような補佐官は必要ではないかということを、カナダの州政府の例を出しながら申し上げた。基本的には先の委員が述べられた内部養成の必要性は申し上げたい。

○　先の委員の意見に同意である。まさに当事者意識が足りていてないのではないか。この論点についての記述を読んで、初めから政府機関での育成をあきらめているのかという印象を受けた。しかし、時代ニーズはそういったところではなく、専門的な人材育成がやれる組織、制度の設計をきちんとやらなければならない。いつまでアウトソースを行うのか、果たして役割を果たせるのかというところが、大きな問題であると考える。それができないところに、本格的な電子政府は進まない一要因がある。全体のデザイナーが内部から出てこなければ進まない。そこをアウトソーシングに頼ってもできるわけがない。そろそろそういった育成と制度設計を行うべきである。タイミングとしてはすぐにはできないので、すぐに取り掛かれるところ、中長期でやることを仕分けしながら、このような展望もってやるべきだということは示すべきである。

○　必ずしも外部からもってくること自体は否定しなくてもいいのではないかと。内部育成では膨大な時間が掛かり、キャリアパスからしても難しいものがあるかもしれない。そういったことを考えると外部からもってきてもいいのではないか。ＣＩＯ補佐官がどのように評価されているかについて申し上げる立場ではないが、“補佐官”と付いているところに活躍の限界があるのではないかと思う。それは別として、最高情報セキュリティ“アドバイザー”も中途半端な位置づけになってしまう可能性がある。やはり最高情報セキュリティ責任者という形で入らないと、実効的な活躍ができないのではないか。外部からもってきてもよいとは思うが、ＣＩＯのような本当の責任者として入る仕組みが必要なのではないかと思う。

○　今のお話にあるように、長期的には内部育成は必要かと思っている。ここ１年少々の間で政府全体の任命制度も変わってくると思っている。長期的な話として、内閣人事局でしたか、そういったところも変わってくるのでどうなるか分からないと思っている。短期的な話にもう少しシフトすると、委員が述べられたようにＣＩＯ補佐官の任用には賛否両論がある。全省４０名程度の補佐官という民間人が入って、ＩＴに関する調達がかなり変わってきたのは事実である。進んでいる進んでいないについては個別にいろいろとあると思うが、全体としては進んできている。補佐官、アドバイザーについて、民間の活用は重要である。補佐官、アドバイザーの名前と権限についても重要であると思う。事例を申し上げると、最初のころはＣＩＯ補佐官をどのように活用すればよいか分からないということがあった。ホームページに掲載されているが、ＣＩＯ補佐官活用事例集というものがあり、各省でサンプルを集めて活用を更に考えてくださいというものがある。もう少し最高情報セキュリティアドバイザーの業務、役割の明確化、詳細化は必要である。

○　民間にセキュリティのアドバイスができる人が多数いるかというと、それほどいないのではないかと思っている。民間でも足りないのではないかというお話が、別の人材に関する委員会でもあった。それを考えると、外部人材を活用するということは短期的にはよいが、NISCでＩＴ人材、敢えて“ＩＴ人材”と言葉を分けて使わせていただくが、これを育てるようなことはできないか。これをセキュリティ専門家として各省に送り込むような仕組みがつくれないだろうか。ＳＩｅｒの方に聞くと分かるが、何百人のＳＩｅｒの方がいるなかで本当に

セキュリティができる方は数える程である。それを集めるというのがいいのか、それを若干育成するというのがよいのかは、私も明確ではないが、少し育成ということも考えた方がよいのではないかと思っている。

○　やはり、基本的にはきちんとした仕組みはつくらなければならないが、具体的なことを考えたときに民間も含めて活用するということがなければならない。大学の方では、情報セキュリティ大学院大学もできて頑張り始めているところではあるが、先ほどの話でＣＩＯ補佐官が４０名程度いらっしゃるという中で、そういった大学院レベルから出る人が年間３０名程度という規模でしかない。お役人になる方々の中でそういった意識をもった人々が入ってくるような施策、その後の育成ということは、大学との連携、大学の中の教育の仕組みも含めて汲んでおかないと、いつまでもこのままというわけにはいかない。

○　今の議論を伺っていて、人材に２種類あるものが混同されているように感じた。インターネットのプロトコルが分かるような専門家を外部からアドバイザーとして連れてくるというのは分かるが、情報セキュリティ管理者やＣＩＯは内部の人以外では有り得ない。本来は、社長ないしこれに準ずる経営陣がやらなければならない。議論がズレている気がする。

○　ＣＩＯになる方は両方できなければならない。

○　私のセンスでは、暗号化などに詳しいよりは健全な常識や経営感覚がある人がはるかに適任だと思う。

○　こういった方々の権限をはっきりするということだけに尽きると思う。それを明確にしなければいくら高給を上げようが、なにをしようがろくな働きはしないと思う。方向性に関する資料、ＣＩＯ、最高情報セキュリティ責任者、ＣＩＯ補佐官といったところに世の中の優秀な人材が就きたいと思うような魅力的な言葉が書かれていないので無理だと思う。

○　組織の中の人がセキュリティくらい自分で考えろというのは全くその通りだとは思うが、私が知る幾人かの情報セキュリティ責任者の方は、結構セキュリティは哲学的なところがあり、自分はこう考えるというところがある。例えば、繋がないことがセキュリティであるとか、データにしないことがセキュリティであるなどのように、固執するところがある。そういう方が、内部で終身雇用で雇われた場合には、そこのシステムが永遠に開かれないとか、責任問題で妙に守るだけであるとか、先ほど述べられたように強い方向に倒す節があるなど、弊害がある。そもそも論もあると思うが、実際にそのような現象があることを考えると民間からの登用であるとか、特に任期付きの登用はリフレッシュされてよい。開かれた情報をいかに活用していくかということとセキュリティの両方をバランスできる人材が必要である。それが内部の終身雇用で本当に実現できるのか疑問を感じる。

○　今のご意見には承服しかねる。そのような偏った担当がいることを是正するのがＣＩＯの役割であり、健全なＣＩＯを育成すればそのようなことは起こらないと思っている。中のことを十分理解し、マネジメントを行える内部から育てない限り良くはならないと思う。教育であるからものすごく時間がかかるので、１０年単位くらいのことで考えなければならない。それまでのステップアップをどのようにするかが今は大事で、当面は外部の人たちをこのよ

うな形で使っていくことを明示することが重要である。将来像を見据えて、１０年後はこうなるというようなことを示していかなければ、電子政府はできないだろう。

○　先の委員が述べられたように、権限などの規定を明確にしなければならない。各省庁のＣＩＯ補佐官の業務内容をみていてもバラバラであり、ある意味では共通項が少ないともいえる。ＣＩＯの契約、権限等を可視化してきちんとシステム化する必要がある。このあたりをまず、着手すべきかと思う。それによって、チェック項目に合わせて教育体系などもできてくると思う。先ほどGAOの話があったが、ＣＩＯに関する報告書が出ており、米国においてもＣＩＯの権限が違っていたりするが、その組織の改革の状況、ステージによって機能が違う。セキュリティを非常に重視するＣＩＯがいれば、戦略性が求められるＣＩＯ、経営能力が求められるＣＩＯ、それはステージが違うからであり、ステップ・ステップで違ってくる。任命の仕方も、政治任命もあればキャリアアップで行政官から上がる場合もある。また、外から長官が任命してもってくる場合もある。そのメリット、デメリットも書いてあるが、これも時期によって違ってくる。そのあたりを時系列でも考えなければならない。もう少しそれは議論をして、ＣＩＯを体系的に育てる、必要であれば外部から来ていただくということが必要であろう。

（６）予算面における合理性に基づく柔軟な運用に係る検討について

○　ここについては、コメントがあるようであれば後ほど事務局に寄せていただきたい。

（７）技術面の知見を蓄積・活用できる構造に係る検討、暗号の利用に係る検討について

○　前から今回の暗号などがそうであるが、技術検討、知見を貯めていただきたいという意見を出させていただいている。資料４－２の１８頁に電子政府における安全な暗号の利用ということで、暗号の移行指針が示されているが、これはそのまえの１７頁に示されているCRYPTRECの検討をベースに出されていると理解している。省庁、民間もそうであるが、暗号の議論になった場合に、CRYPTRECから出されている議論の結果を覆そうとはしない。それは一定程度、暗号の専門家がいろいろ検討して出された結果であるので、それにはタッチせずギブンなもとして理解し、議論している。CRYPTRECの検討の結果自身にいろいろな異議はあるのかもしれないが、一般的にはそれで済んでしまう。知見を貯めていただきたいというのは、専門家によりあらゆる方向性が検討されているので、ここを使いましょうということを知見として貯めていただきたいということである。

○　知見を貯めるために、米国のNISTのような組織を作れということではなく、既存の組織を使って検討はバーチャルでも構わないと思っている。そこで検討が十分され尽したということが分かるような形で標準化される、例えばNISCのホームページで、ある基準、標準はこうなっている、NISCがオーソライズされているということが分かればよい。既存の組織を使い

ながら、十分検討されているので一般社会では検討しなくてもよいというようなエビデンスが揃った知見のセットを揃えていくということをお願いしたい。

○　電子政府推奨暗号は今いくつか数が出ている。前から多少述べさせていただいているが、日本の中にこのようなリストがあり、あるサービス、アプリケーションで何を使うかを考える時に、鍵のサイズを変えるといった暗号の移行の指針は示されているが、どういうものを選ぶべきか、その方向性をつけるようなものがない。「よく分からないけど、もうＡＥＳでいいや」となる可能性が高く、推奨暗号として示されているが企業等で全く使われないものもが残念ながら多い。推奨暗号のリストが挙がっており、またブロック暗号だけではなくストリーム暗号もこれから日本でも出てくると思われ、それらについて政府機関ではこのように考えて指針を提言しているといった利用指針が欲しい。おそらくNISCだけでは難しいので、CRYPTRECなどの専門家と一緒に検討していただいた方がよいかと思う。暗号はコアな技術になるので、CRYPTRECは安全性の検証だけで１０年以上食べているので、これはそれらの専門家に任せる必要がある。

○　各委員からのご指摘に全く同意である。技術的な検討は外部からもってくればよい。儀津的な知見を蓄積・活用するといったときに、通信技術などに限らず、想定する脅威としてどのようものを考えるかといった知見も貯めていただく必要がある。いろいろな対策を全てうてたかの判断は、全て予見可能性に帰着する問題だと思う。どこでやるかという問題はあるが、予見する技術は重要であり、技術というか想定する脅威の知見を貯めるということをやる必要があるのではないか。

○　今の脅威の知見は、今どの辺が一番よく分かっているのだろうか。

○　金融機関ではFISCであるとか、また経産省などでも出されているかと思う。

○　ここに入れるべきかはわからないが、国策としての国産情報セキュリティ技術を育成する観点というものはここに入れなくてもよいのか。

⇒　それについては、この政府機関対策の部分ではないと思っている。一つ申し上げたいのは、CRYPTRECの方々と話をすると国産暗号の推進を入れて欲しいと言われる。経済産業省、防衛省の方もよくご存知であるかと思うが、WTO・TBTというルールの存在と国家安全保障のシステムにおける例外規定というものが厳然としてある。国際標準との関係でこれは言われている。政府調達において暗号技術を導入する場合は、一般的にWTO・TBTに準じた取り扱いをしなければならない。その際、国産暗号を推進するような利用ガイドラインについては書けない。広く認められた国際標準に示されている方式を公平に採用しなさいとなっている。いろいろな暗号方式を使いなさいということは、一般の情報システムに対しては書ける。また国家安全保障等の特定の目的によって国家が優先するシステムにおいては例外とする。国防調達などでは別途定めなさいとなっており、政府統一基準とは別の空間にある。ここで、特に暗号の利用指針について書くことはtouchy(タッチー)な問題がある。暗号に限らず他の点についてもそうなので、かなりぎりぎりの線で書いていくという努力を統一基準では行っている。そのようなポリシーとしての話は、横断的基盤の技術戦略のところで書く話である。

調達にも関わる統一基準などに書くことは注意深くやらなければならない。

○　基本的には技術の国産云々については、今のご説明の通りである。知見の蓄積、暗号の利用についてはNISCがネットワークのコアメンバーとなるということと、知見をかなり活用できるようにする。研究は研究で動いていただき、その運用やマネジメントはNISCがやるべき仕事である。それは対等な関係で議論を行い、役割に応じてネットワーク、バーチャルな関係で組織するのがよいかと思う。それで、CRYPTRECはCRYPTRECとしの役割を果たし、NISCはNISCの役割を果たすということだろうと思う。ネットワーク、バーチャル組織でNISCの広がりも確保できるということはできる。それによって視野の広さをもった上で、調達等々について様々な検討ができる体制をNISCが作るべきだろうと思う。

（８）地方公共団体、独立行政法人等に係る位置づけと取組みの検討について、その他

○　地方公共団体について経団連からのパブコメ意見を見ると、「地方公共団体間の対応レベルの差をなくすように業務プロセスの共通化を図るべき」と述べられている。一住民としてはセキュリティ不安を理由に引っ越すのは非現実的なので、統一した方が良いとも思う。一方、第２回の委員会でも質問したが、例えば、東京はセキュリティ対策を最優先するんだ、大阪はそこにはお金を掛けないんだとなった場合に、総務省などが取り締まれるものなのか。答えによっては、いくら議論しても無駄になるような気がする。指導できないのであれば、政府機関が背中を見せて、それを真似したい首長が追随することが限界になってしまうのではないか。それが疑問であり、総務省の方からご回答いただけると有難い。

⇒　事務局の方で代わりにお答えしたい。答えは難しいが、総務省の自治行政局の方で、情報セキュリティに関するガイドライン、委員長からご紹介があった現在パブリックコメント期間中のＢＣＰのガイドライン、そのでこぼこをなくすため、強制力はないがガイドラインが出ている。国もなにもしていないわけではなくて、なんとかしようとしている。これをやりなさいという命令権はなく、やはり地方自治の本旨というものがあり、対等な中央の政府、地方の政府ということになる。

○　電子自治体の推進に関する懇談会で委員長を務めている立場から申し上げると、事務局が述べられたように命令権は全くない。ただし、対応していただけませんかということで、そのセキュリティ政策に関しては、地方交付税、交付金で対応させていただくということはある。ただ、地方交付税、交付金は強制力はないので他のケースで使われる可能性もある。それは自治体の主権であるからやむをえない。その財政的な担保は極力させていただきますというのが、総務省の政策である。最終的判断は首長及び議会が決める。

○　その他の部分として、確認ではあるが、第１次提言では情報セキュリティに関わる統一法規であるとか、基本法、個別法の制定の方向はないという形でまとめられていたと思うが、ここにある考えられる方向性については、ある特定のこれから制定しようとする法律、それ

が情報セキュリティに関わるようなものであれば、統一基準との整合性、一貫性をどのように考えるか、その方向を検討をしなければならないというようなことをここでは言われているのか。

⇒　その通りである。ここに挙げている、文書管理法制や電子政府推進法（仮称）はどちらもNISCでやっているものではない。実行部隊としての事務局は影響力行使するしかないということがひとつと、もうひとつは統一基準の運用があるので、そこの整合性確保に努めたいということである。

○　ということは、今後できてくるいろいろな法律については、いつも常に統一基準との整合性をウォッチし、制度的に口を出して情報セキュリティを守るといった仕組みを出そうという方向なのか。

⇒　それはなんとも言えないところである。文書管理法制は明確で、政府の中で取り扱われている文書の形になっている情報について、最終的にライフサイクルをどうマネージするかということと、機密性管理をどうしていくかと情報公開法との関係など明確な領域の中にあるので、統一基準では情報格付けとの関係が最も大きい。また、アベイラビリティとの関係がある。電子政府推進法（仮称）は、まだどのくらい関係してくるか分からないため、法案ができるてくるフェーズ毎の活動はなんともいえない。今、喫緊で分かっている法案はこの２つである。

○　情報セキュリティは“情報”とついてはいるが、いろいろな法律はセキュリティの範囲が広く、法律について考えると必ずどこか情報セキュリティに係ってくる可能性がある。政府として統一的に、法律が情報セキュリティへ係ることに対して、口を出す制度であるとか、仕組み、規則などが何か必要な気がする。今特定のものが２つ挙げられているが、今後そういった法律が顔を出してくる際に、それを個別に検討を加える方向でよいのかどうか、統一的に何かが絡めておく必要があるのではないか。そのような提言はしておく必要はないか。

⇒　間違えていたら指摘いただきたいが、内閣が出していく法案に関しては全省協議というものに掛かっていて、各省庁の間で法案のレビューが掛かる。内閣官房情報セキュリティセンターにおいても、定義的には全ての法案に関して協議が掛かることになる。それは全てかどうかについては難しいところはあるが、実行上は関係しているところに対して notify(ノーティファイ)が掛かって、みていく構造になっている。必要なところを我々がみたときに、どのように影響力を行使したり、事実として直していってくださいということをどのようにやっていくかは、センターのキャパシティの中で行っているとしか言い様がない。もしこれをセンターのキャパシティ以上にやろうとすると、もう一つ上のレベルで、全体として何をするのかといった基本法のようなものであったり、ある一つの目標を高く掲げるようなルール設定がある中でやらなければならない。手続きに関して法律が運用される場合には、我々も口を出せる機会は多い。情報の保護のような概念的なものについては、これに関しては法律として個人情報保護法があり、これは政府にも個別の保護法があり、大きな法律として民間に網が掛けているが、実行上は情報セキュリティと表裏の部分もあり、ＩＴのことも考えま

しょうよということで、実行上のところでは、実際に社会に落ちていくところで影響力を行使していける。しかし、情報セキュリティをみんな考えようという概念的な大きな話になると、もう少し大きいルール、稲垣先生が言われていた情報セキュリティ基本法、なんでもかんでも一回、情報セキュリティを考えろということで、第一東京弁護士会も試案を出されていた。そのような形でぶつけるしか難しいのではないか。何故、電子行政推進法（仮称）のような考えが横断的にできて、いろいろなことが言えるかといえば、根っこにＩＴ基本法があるので、そこからいくつかの形で出てきたという歴史の中で、言えているという部分がある。我々はＩＴ基本法２５条に拠っているところであるが、それ以上のディテールまで入るところまでになったら、本当の意味でルール設定を改めて考えるとそれはできるだろうと考える。

○　ということであれば、情報セキュリティ基本法というようなものの必要性も議論の中に入れていかなければならないのではないか。

⇒　それは、センターのキャパシティを超えるようなところで影響力を及ぼそうとするならばそうだと思う。これも間違っていれば指摘していただきたい。内閣官房は総合調整権能とうものを与えられているので、どこの省庁でも結果はどうなるか分からないが、一応口を出せば話は聞いてくれるくらいの定期券は持っている。そこで実行上の調整を掛ける能力はあるということで、キャパシティと言っている。これを超えるとなると、総合調整権能を超えて明確に国家目標の中で何かをやるということが明確に謳われ、それに対しての実施体制へのコミットメントが政府内にできあがるということである。これが本当に今のNISCを中心とした総合調整という、内閣官房の中での設置要件の中で泳いでいる我々以上に何か必要かということである。これをまず考えなければ踏み出せない。これまでやってきた中での理解では、そこまでなくても、今のところ結構スピーディーに対応できる体制を内閣官房はもっていると考える。ＩＴ基本法と行政組織法に書いてある内閣官房の総合調整権能で泳ぎきれるのではないかというのが私の予感で、それ以上のところに対して基本法的なものを作る法益が何か明確に定義できるかというと、七転八倒しない限りできないのではないかという気はしている。個人的な意見ではあるが。

○　先のお話で、文書管理法制がきちんとできているということが述べられたと理解したので、これには反論しなければならないということで意見を述べたい。資料４－２の９頁目にある公文書管理のあり方に関する有識者会議中間報告との関連で、この考えられる方向性は書かれたかと思う。この有識者会議の委員を務めているが、この有識者会合も事務局は内閣官房であり、今のご説明によれば、内部調整でやっていただくので、こことの整合性、一貫性はとれると解釈してよいのか、あるいは有識者会合の中でしっかり話し合っておかなければならないのかを大変気にしている。文書管理がきちんとできていないので、各府省が独自のルールで作成、保存、廃棄等を行っているのできちんとしましょうということを話し合い、前半はこれで中間報告を出した。ここにあるようにＩＴに関しては、ほとんど踏み込んではいない。後半の、８月１日から始まる議論の中で入ってくるので、こちらの方がヒヤリングに

来ていただき、これをどうしましょうということをこちらの委員会とやるのかということも少し気にしており、ご回答があればお願いしたい。

⇒　先ほどの説明の中での趣旨は、議論をする枠組はできているということであって、文書管理がきちんとできているとは全く思っていない。現実問題として内閣官房であるNISCと公文書管理のあり方に関する有識者会議の事務局との間で既に話は始めている。影響力行使の枠組がきちんと動き始めている。それに関しては、協力体制ができるかもしれないので、有識者会合の皆様にはしっかりとした議論をしておいていただきたいというのが、補佐官としてお願いしたいことである。実ジョイントにはなっていないということは伝えておきたい。

○　現場で統一基準を導入する際に、文書管理との整合性がという話が必ず出てくるので、是非整合性をとっていただきたい。

○　外部組織に委託した場合に、請負先にセキュリティポリシーを守らせる仕組みが必要ではないかと書かれているが、これに関してはどのようなレベルか。ポリシーを守らせるということで、民間でも請負先の方を部屋に囲って、そこで自分のところのＰＣを使わせるパターンまである。そういったレベルのものなのか。若しくは、調達の契約内容としてセキュリティに対する管理体制であるとか、管理方法を提示してもらい、事故発生時に報告する義務を設けるだとか、事故発生時の監査権を明示しておくだとか、そういった法契約上の権利関係が主なものになる場合もある。現実論としては後者くらいかと思うが、別なイメージがあれば教えていただきたい。

⇒　基本的には後者の仕組みである。既に統一基準の中で、外部委託においてポリシーを守らせるということは求めている。あとはそれをどのレベルまでやるのか、相手にセキュリティ監査、保証型監査制度など、どういったことをその中でやればよいのか、小さなシステムは別にしても、ある程度大きなシステムを外に出し、国が運用していると思われる場合には、省のポリシーと同じレベルでやっていることを説明できるような仕組みを作っていくことだと思っている。

○　１０年程前、総務省で自治体の文書管理のＩＴ化の議論をした。多くの自治体では文書管理課があって、そこで首長印や課長印まとめて押すなどして、公文書としての効力を持たせている。これをデジタル化するときに公文書の原本性をどう保証するか、やはりこれは時刻認証、何時何分何秒に作成されたか、誰が作成したかの第三者的な認証が必要になってくる。デジタルは改ざんが容易である。それに改定が入った場合に、誰がいつどこで、どういった権限に基づいて改定したかということに第三者的な証明が必要である。そういうことを議論して、１０年程前なので、いずれそうなるだろうということであった。歴史的文書ではなく、実際に効力のある公文書をやるのであれば、そこを考えていただきたいということは、公文書管理のあり方に関する有識者会議でもどんどん言っていただきたい。電子行政推進法（仮称）について言えば、そこまで考えなければならないということは、官房と私の方では話をしている。これはNISCの協力が不可欠であろうと認識している。

○　この公文書管理のあり方に関する有識者会議は、委員構成として歴史的文書に関心がある

方と、私のように現用文書、これから作成する文書にやや関心が高い委員の二つに分かれている。前半は歴史的文書についての話が中心となっていたが、後半はＩＴの方で巻き返したいと思うので、こちらも応援をお願いしたい。

○　独立行政法人に関して、消費者庁論議で国民生活センターと各省、いろいろなところとの接続が話題になっており、国民生活センターは政府に準じた対策というのができるのではないかと考える。地方公共団体については、専門人材をどうするかという話になってくるのではないか。国の問題でも、任用に係る基準等々、つまり安いと来ないのではないかというお話があったと思うが、地方でも短期公務員の任用のあり方に関する研究会が、つい最近立ち上がったので、こちらで必要だということを言っていただければ、そういう制度をつくるということが総務省でもやり易くなるので、地方公共団体でも専門人材を確保してきちんとやるようにと書き込んでいっていただきたい。

○　今述べられた最後の点は、各委員異論はないと思うので、是非そういった文章を作らせていただければと思う。

○　各省庁から今日参加していただいている方で、是非言っておきたいということがあればご発言をお願いしたい。

○ 先ほどCRYPTRECに関するお話があったが、調達との関係でのTBTについては我々も認識し、その辺りは見直しを行っている。産業振興は産業振興で切り離すことができる仕組みを考えている。

⑸ 今後のスケジュール説明

○　事務局から、今後のスケジュールについて説明がなされた。

－ 以　上 －