情報セキュリティ政策会議　基本計画検討委員会
第10回会合議事要旨

１．日　時

平成20年９月４日（木）　16時00分～ 19時30分

２．場　所

内閣府本府　地下１階講堂

３．出席者

【委　員】

井川　陽次郎　委員　　読売新聞東京本社論説委員
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
関　正樹　委員　　関彰商事株式会社代表取締役社長
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
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）
深谷　聖治　委員　　東日本旅客鉄道株式会社総合企画本部システム企画部長
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）
宮地　充子　委員　　北陸先端科学技術大学院大学情報科学研究科教授・附属図書館長
三輪　信雄　委員　　綜合警備保障株式会社参与
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

(1) 地方公共団体における情報セキュリティ対策の現状について

○　総務省の報告があったように、関東でやっている所が、おそらく市町村では３０％前後、拝見したところ、網羅的に積極的にみなさんが取り組まれているとの印象。この中で言いたいところは、まずこういったセキュリティ政策に関してどなたが行っているのか。これは、職員の方はもちろんだが、外部リソースを使っているか、そういったところをお伺いしたい。ＩＴの調達は地元で行われているか、それとも埼玉の都市部とか東京都内から調達されておられるのか、その辺をお伺いしたい。

⇒　監査の関係であるが、小鹿野町でも監査の体制はなかった。そこで、(財) 地方自治情報センター（ＬＡＳＤＥＣ）の御協力をいただき、監査法人の方が派遣され、監査を実施した。その後、埼玉県の事業で監査の業者を派遣していただいたり、内部監査の支援ということで (財) 地方自治情報センター（ＬＡＳＤＥＣ）から業者を派遣していただいたりというようなことを行い、今ではほとんど職員が内部監査を実施しているという状況である。調達の関係であるが、地元にＩＴ関連の業者がないため、大手の都内の業者や県内にある比較的大きい業者から調達するということを行っている。

○　外部委託の問題について、データを渡された側の外部委託業者の問題というのは確かにそうであるが、全ての市民分の生データを渡した市側の問題があり、それ以降は民間のＳＩ業者では、テストデータが本番前には絶対必要になるが、テストデータは生の物というのは、もはやご法度になっており、名前や住所は偽のものを使ってテストデータを作りそれでテストをしている。そういったことをきちんとやっていれば、本来、外部委託業者から情報が漏れるということはない。市が元々外部委託業者に生データの全部であれ一部であれ渡すこと自体が問題であって、そういったことを抑制すれば、漏れることもなく、罰せられることもない、悲しい事件も起こらないので、その辺りは出す側の規則というのは決められていたのか。

⇒　事件については、確かに情報を持って行かれたということであり、その後聞いたところ、事業者を内部に入れて、どんな時でも業者に来ていただき内部で処理してもらうというように方針転換したと伺っている。今回のこの事例は、テストデータではなく、市町村合併に関わるデータであり、平成１６年の合併から、発覚した平成１９年の３年分のデータがそのまま残っていた。市町村合併で住民基本台帳のデータを、一つのシステムに一緒にしなくてはならなかったため、生データを扱わざるを得なかったという状況があり、このようなことを受け、テストは擬似データ、本番のデータを扱う時はきちんと内部で扱うなど、

きちんと誓約書を書く、消去する、あるいは返却させるなどを確認しなさい、といった方針で対処している。

○　当方もかなり自治体の情報システムには関わっているが、経験では外部委託の契約が今までの慣行で、明確な責任や権限が規定されていない契約が多いように思える。それについては、総務省はどういうことお考えか。

⇒　資料２の最終頁の３つの取組みをおこなっており、「運用の手引き・ツールの作成」にある、「外部委託時の個人情報の漏えい防止対策（契約書のひな形等）」契約書の中にそういったことをきちんと書き込み、そのためにはどういったことを書き込めばよいかということを現在検討しており、自治体の方にご提示しようといった取組みは行っている。

○　セキュリティ研修の一部に、高度情報セキュリティ研修と e-ラーニングの情報セキュリティ研修とあるが、e-ラーニングは年々増加しているが、高度情報セキュリティ研修の受講者が増えていないのはどういったことからか。また、実際に受けて、本当に受けることによってセキュリティに対する意識、考え方や技能などが向上しているということを保証できるような仕組みのようなものがあるか。受講する%があげられているが、実際に受講されている方と内容との関係を教えていただきたい。

⇒　まず、高度情報セキュリティ研修は専門的な研修を行っており、あまりにも専門的すぎたところは反省があり、なかなか受講者も納得いかないというようなところがあった。もう一つは、予算の関係もあった。受講者がついてこれなかったのではないかというところが一つ反省点としてある。他方、e-ラーニングは新規採用職員からベテラン職員まで幅広く受けていただけるようにということで、成功したのではないかと考えている。また、研修の繰り返しサイクルで、e-ラーニングに限っては、基本的に一般職員コースを受けていただき、次のステップで情報システム関係の職員であれば、もう一つ受けていただくなどをおこなっている。これは役職で分けたステップであり、昨年までは初級・中級・上級と三つのコースを設定し、昨年、一昨年に実施している。下から上に、上がるやり方で行ってきたが、もう少し幅広く職域に合わせてということで、今年から新規採用にもそういったものも入れてきた。このように内容は毎年見直している。できれば毎年一回自分の職域のところを受けていただきたいという方向でやっている。受けた方が、どれだけ成果が上がったかまでは検証していないため何とも言えないが、色々なセキュリティ関係の事故を見る限り、かなり減ってきたとは思っている。実際、確たる数字がないため、分からないというのが現状である。コースの設定と受講者のレベルを、今年６月から始めたばかりで、まだ集計はこのような状況である。

○　e-ラーニングの統括責任者コースの冒頭１５分にお話させていただいている。そこで、主に話したのがＮＩＳＣの第１次基本計画について述べさせていただいた。

○　監査項目の簡素化として、どういった選定基準で項目を選ばれたのか。

○　当時担当していなかったため詳しくは存じていないが、省庁やベンダー、監査法人の方々に入っていただき、検討会を設け、縮小したので、おそらくかなりのきちっとしたものを用いて取り組んでいる。細かい内容については調べてみたい。

○　小鹿野町の方にお伺いしたい。セキュリティ体制、スコープに入っている職員の数とパソコンの数はどの程度か。対策を行った後、インシデントはどうなったか。情報政策関連予算は８，１００万円程度だが、そのうちセキュリティ予算と考えられるのはどの程度か。また、セキュリティ対策を積極的に進められたきっかけは何か。

⇒　職員数について、正確な数は手持ち資料がないので把握していないが、対象としている職員数は概ね３００程度、小鹿野町職員、学校の教職員を併せてである。パソコンの台数は、小鹿野町では学校のパソコン教室の端末も管理しており、あわせて８００程度である。次にインシデントだが、やはりセキュリティ対策を強化しても無くなるものではないと考えている。できるだけ少なくしていくという効果はあると思うが、インシデントをゼロにすることは、費用を限りなくかければ可能かもしれないが、費用が少ない中でできるだけのことをやっていく考えであり、完全に無くなるということはまだ先のことだと思う。実際のインシデントであるが、やはり今年の３月にあったが、これは漏洩等の問題ではなく、住民票系のシステムを取り扱っている業者が、データベースの操作を誤り、２時間ほど住民票の発行や税帳簿の証明書発行等の業務が停止したことがある。システムが停止したということを想定して訓練を実施しているため、住民票を発行する部局では、手入力発行ということで、台帳を見て入力して発行し、取組みが上手くいった。次に予算の関係であるが、情報システムの保守・管理の部分はセキュリティ対策と一緒になっているのが現状であり、セキュリティ費用がいくらかかったのかを出すのは難しい。単純なセキュリティ対策の費用というと、ウィルス対策であるとか、ファイヤーウォールのライセンス料等であるが、それらの費用は、３００万円程である。通常の機器管理、システムか構築等でセキュリティ対策を考慮しながら構築していくため、分離して明らかにすることは難しい。次にセキュリティ対策を積極的に進めたきっかけは、特に首長から指示があったわけではないが、合併時に情報漏洩等の報道が多くあり、新しい町になるにあたり、情報漏洩等がないようにということで、担当レベルから上がり条例化し、セキュリティ対策を強化していった。

○　予算を通すにあたり議会等から反対はあったのか。なぜセキュリティ対策を進めるのかということをどのように説明したのか。

⇒　情報システムの管理運用では、合併時には比較的財政支援が多い。合併時にシステム統合は必要なことであり、それにあわせセキュリティ対策も必要なことであるため、国や県の支援をいただきシステム構築を行った。その後については、そのような支援がないためできるだけ費用を抑えて行っている。

○　小鹿野町は、地域情報化や電子自治体のランキングがいろろなところに出ているが、ほとんどが財政規模がある程度充実した市ベルがほとんどである。町レベルでは２カ所だけ、ランキングに載っている町があり、それが小鹿野町と北海道の長沼町であるが、この２カ所は規模が小さいが非常に良く取り組まれている模範的な自治体である。

⑵ 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ついて

○　特別管理秘密は各省庁が決めるということであるが、だいたいどれぐらいのボリュームがあるのか。答え方が難しいと思うが、例えば、情報が１００あるとすればどれぐらいの量といったような感覚的なものでよいのだが。

⇒　確かに答え方は難しいが、普通の秘密は大抵の役所にあるが、極秘や機密といったものについては、そもそもそういった制度がない役所もある。防衛等については、それなりのものがある。通常の役所においても全くゼロということはないと思うが、国の安全に係る秘密に関しては、役所においてはそれほど大量のものではない。正確な情報はわからない。

⇒　ご参考までに、NISC は、現時点では特別管理秘密は持っていない。

○　イメージがわかないので教えていただきたいのだが、資料によると、特別管理秘密については物的管理とされているが、これは物理的に鍵をかけてしまうとか、そういったことを意味しているのか。

⇒　物的管理とは、鍵をかけてしまうなど、そういったものも入っている。情報システムを構築するということもある。

○　物的管理というのは鍵をかけて物理的に隔離してしまえば非常に管理しやすいが、情報が電子データになった場合には、論理的にファイヤーウォール等で隔離するなど、ハッカー等の問題にどう対処するのかといった技術的な問題をたくさん抱え込むようなところが

ある。例えば、うろ覚えであるが、イージス艦のデータがウィニーで出回ってしまったというようなことを新聞報道等で以前目にしたことがあるが、今後はこのようなことが防げるようになると考えて良いのか。

⇒　最近の役所の秘密情報は、基本的には全部パソコンで作成しているので、そういった分野におけるセキュリティは重要であるとの認識は持っている。そういったセキュリティ管理についても、十分対策をとってまいりたいと考えている。

○　特別管理秘密はシステムの中で保たれると思うが、そのようなシステムの指定を行うような予定はあるのか。また、範囲をどのように決めるのか、その点の考えを聞きたい。特別管理秘密について、物的管理として統一基準の厳格な適用等を行うとしているが、セキュリティ対策はやらなくてはいけないとは思うが、個人的には統一基準じゃなくてもよいのではないか。統一基準というのはISMS等のISOからきているが、これは一般ユーザが守るべきセキュリティ対策に特化している。システムのアーキテクチャから変わってくるのかと思う。変わるべきとは言わないが、変わってくるという可能性もあるのではないかと思うがどうなのか。

⇒　特別管理秘密は、専用のシステムを使えば、その方がセキュリティ上よいかと思うが、混ぜてはやってはいけないというようなところまでは決めてはいない。特別管理秘密を扱っていないシステムについては通常のシステム運用である。統一基準に関するものはＰＤＣＡサイクルに則り、なるべく見直しを行っていく必要があると考えている。情報セキュリティの観点からの運用に関しては、今回の基本方針の中では、それほど細かく記載していないが、そのようなことについては必ずしもオープンな場での議論とはならないかも知れないが、NISCの知見を借り適切に対処したいと考えている。

○　秘密取扱者適格性確認制度は、それぞれの秘密の内容に応じて色々な異なる適正を考えられ、それ毎に確認方法や手段があるということを意味しているのか 。また、物的管理との兼ね合いであるが、本来秘密そのものにアクセスできるのは職務上関わっている人、それを物理的に管理している人もいるだろうが、本来の職務に就く段階において、それらの全てのポジションの方がこういった適正検査をうけているという意味合いか。それとも、これは秘密であるからコピーしてはいけない、或いはそこにそういったものがあり、自分が扱っているということを話してはいけないといったことを、チェックするという意味合いなのか。

⇒　適格性というのは、一種の資格のようなものであるが、特別管理秘密というカテゴリにアクセスするために必要となるものである。公務の秘密へのアクセスについては、適格性

を確認した上で、さらに、それぞれの秘密にアクセスする必要性があるかないかを個別に判断することになると考えている。業務によって秘密を取り扱う者は、課長であっても係員であっても適格性の確認が必要であり、適格性の確認が得られない者は秘密を扱う職には配置できない。

○　国の重要な情報や職員等の保護を図るというのは、秘密情報を扱う職員を身の危険から保護するということなのか、それとも職員を他からのアクセスからガードしてそこからアクセスできないようにするということなのか、又は職員が情報を漏洩させないということなのか。責任を限定し、担当している職員が漏洩の責任を負わないようにするといったことか。

⇒　職員等の保護とは、不審なことがあったときに組織として対処することにより職員の情報漏洩を防ぎ、職員が情報漏洩の犯人になることがないように保護するということである。悪事に手を染めさせないよう保護するといった、パターナリズム的なものである。

○　人命を保護するといったこととともあるのではないか。

⇒　もちろんそれはある。情報漏洩に関しては、命を狙われたりといったこともある。そういったことを受けた場合にどう保護するかということもある。

○　例えば金融政策であれば、基本は専門機関である日銀に任せたうえで、一定の情報開示を基に「金利を上げろ・下げろ」などの議論は自由にできる。この件に関してはここで討議して欲しいのか欲しくないのか自体が良く分からない。「特別管理秘密を取り扱うシステムに係わる情報セキュリティ対策は内閣情報調査室に任せる」というのであれば、それで終わる気がする。一方、機密情報の中身に触れてこの場で議論することは有り得ないとしても、仮定した秘密の情報やシステムのセキュリティについて皆が論じることは可能である。その辺りの整理を同じ内閣官房内のＣＩセンターとＮＩＳＣ間で行い、叩き台を提示していただくか「ここまではＣＩセンターのマター」というように仕切った方が良いのではないか。

⇒　内閣官房としては、この会議自体が情報セキュリティの基本計画ということで広く一般に政府間の行動を含めて考えるとしているため、その中でこのような高度な秘密の情報についてどう扱うべきか、何らかの方向性を出す必要があると考えている。その議論の過程において内閣情報調査室においてこのような取り組みを進めているというのがあるので、内閣情報調査室に任せるというのであればそういった方向性にしたい。まだこの辺は議論したほうがよいのではないかというのがあれば、情報セキュリティセンターと内閣情報調査室を含めもう少し整理をしなくてはいけないと考えている。そういったことを含め、ど

ういう考えがあるのかを議論できればと思っている。

⑶ 政府機関の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

○　２階層で確実に回すという表現があるが、２回ＰＤＣＡを回すとなど変に捉えられる可能性があるので、別の言葉の方がよいのではないか。政府機関と政府全体の２階層でということではないか。また、セキュリティ対策の適切なインプリメンテーションは、システムだけではなく、いろいろな例があると思うので敢えてシステムに限定する必要はないのではないか。

⇒　文章はこれからも考えていくが、２階層という表現が必要なければ訂正するが、色々と説明する際に、個別の政府機関毎にＰＤＣＡを回すと同時に、そこだけではなく政府全体として回しているという意味で２階層という表現を用いており、各政府機関と政府全体ということである。。それから、敢えて意識して情報システムと限定したわけではなく、電子政府のプロジェクトや各政府機関のシステム開発等の中でＳＢＤの考え方をもとに適切に組み込みたいと考えている。

○　かなり大きなことを書かれているため、政府全体を通して基本的にセキュリティの対策の仕組みが適切に構築すること目指して、何々をやっていくと書いた方がよいと思う。また、情報セキュリティ報告書の定量的評価とはどういう意味なのか。

⇒　ＮＩＳＣ側で各省の重点検査を通じて、例えばメールサーバー等の検査をしている。この先、政府機関の中で評価についてどう求めるかは確定していないが、当然、現在やっているレベル程度のことは報告書の中に書いていただくことを期待しており、そうすれば、端末についてどの程度、今となっては全ての機関がＡになると考えているが、もしそうでないのであれば困るとか、当然Ａになっているだろうということを並べてみるなど、そういったものも一つだと思う。他にどのようなものがあるのかは、これからどういう報告書にするのかという検討があるので、定量的評価とするか単に評価とするかそこはまだ考えていく。

⇒　定量的評価にはこだわりがあり、「やっている」という報告書がでてくることでは、耐えられないので、きちんとベースラインとして何％以上やっているとか、保有台数は何台あるとか、いわゆるデータを元にした、全うなことをやっていただきたいということもあり定量的評価と表現している。

○　今の意見に賛成である。作文ではなく、本当のエビデンスに基づいた報告書を作成して

いただきたい。定量的という言葉を残すべきだと思う。台数や%というような単純な数値もあるが、データがある程度集まれば多変量解析ができるので、ＮＩＳＣがやるべきだと思う。我々は電子政府で多変量解析をやっているので、いくらでも技法を協力する。

○　全体的な印象としては無難にまとまっているが、迫力が足りない気がする。これまで議論してきたことが今一盛り込まれていない。議事要旨を改めて読んで、前回のポイントを整理すると、現状「各省庁の個別最適に止まり、それを底上げするというアプローチをとってはいるが、全体最適になっていない」との議論であった。最初からできないので順々にやるという現実論はあるにせよ、横断的な統括機能、つまりＮＩＳＣの機能を強化した方が良いという意見が多かった。そうした方向性を「定量的評価や比較評価」として書いてきたとは思うが、受け身的であり、もっとトップダウン色を出して良いと思う。「２階層のＰＤＣＡ」つまり各省庁と政府が別々にやっているのではなく上から確認しているのだ、というニュアンスに意味があると思う。政府機関と重要インフラを跨ぎ、全体整合的なリスク評価が必要と主張しているが、重要インフラまで跨ぐのは今の状況では難しそうだ。せめて政府機関の中の重要度ランキングだけでもやっていただき、プライオリティ付けしないと、むなしい感じがする。ＮＩＳＣの独断と偏見でも良いのでランキング付けする方が、現実的に対策を進めるには良い。今の書き方では、推進力が感じられない。

⇒　第１次計画時の各省庁からのレスポンスは何かと言えば、あまりにも強権的にやり、スルーされたといったところが沢山あるというのは事実である。そうすると、トップダウンでやるだけではなく、きちんとやる人だけに言うという構造も必要だと思っている。今の横断的リスク評価に関し、ランキングの話があるが、現実問題としてＢＣＰの真面目な設定を行っていくと避けられない状況になると思う。現実問題として防災の観点から、首都直下地震を考えると、独断と偏見などしなくても、今回は落ち着くところに落ち着くはずであり、ただ、現状として、今ＢＣＰはまだできていないという認識があるため、そういった意味でもまず作らせなければ駄目ではないかという考えである。ただ迫力が無い、メッセージが少ないことは、要望を出している。

○　前回から「次善の策としてＢＣＰで勝負するんだ」と話してはいたが、まずは主戦場で戦う姿勢を見せて欲しい。現実としての次善策は、次のステップで検討していただきたい。

⇒　いただいたご指摘を踏まえ、文章にどういったメリハリをつけるかは整理していく。

○　第１次で現状どこまでできていて、何を新たに付け加えたのかがわからないのだが、情報セキュリティ報告書は今回からやることにするということなのか。また、最高情報セキュリティ責任者というのは既に設けられているのか。セキュリティ責任者が全責任をもって情報

セキュリティ報告書を出すということを強く言っているのか。最高情報セキュリティアドバイザーは現在設けられていないが、最高情報セキュリティ責任者が情報セキュリティ報告書を実質的に関与し、それが働けるようなスタッフを置き、その方々が言ったことがその省庁の動きの中に染み渡るような仕組みを作るという解釈でよいのか。

⇒　情報セキュリティ報告書は今回から行うことにしている。最高情報セキュリティ責任者はポリシー上、各省に置くことになっている。最高情報セキュリティアドバイザーは基準上必要に応じて置くことになっており、形式上と言っては語弊があるが、殆どの役所に置かれている。ただし、その方が本当にセキュリティ専門かどうかは様々であり、それについては、専門家が必ず関与する仕組みを作りたいと考えている。

○　そういったことで基本計画のドキュメントが仕上がれば、各省庁の方がそういうことをやれと言われていることは、ピンとくるようになっていると解釈してよろしいか。

⇒　それはこの先よく考えてまいりたい。

○　全体論調であるが、事故前提社会というのを掲げているので事業継続や事故対策を一つの柱として入れてよいのではないかと思う。CISO については、最高情報セキュリティアドバイザーを全面に出し実態としてもそうしたいというのはわかるが、私の今までの経験からすると責任者側のラインは明確に作っていただきたい。最高情報セキュリティ責任者となる職員がいろいろなことを決定し、最高情報セキュリティアドバイザーはあくまでもオプションのようなもので、いろいろな選択肢の提示はできるが最後の決定権は持っていないと思う。責任者側の決定組織のラインとそこに対する専門的なアドバイスをするアドバイザーといった構造にしたほうがよい。最高情報セキュリティ責任者側のラインをもう少し明確にする必要があるのではないか。また、定量的評価は、情報セキュリティ報告書を定量的評価するように見えるので、若干違和感がある。情報セキュリティ報告書の中に定量的評価を含むというような情報セキュリティ報告書だと思っている。

⇒　事業継続性の件については、ご指摘のとおり考えていきたいと思う。責任者側のラインの明確化については、情報セキュリティ政策会議の下に情報セキュリティ対策推進会議という会議があり、最高情報セキュリティ責任者である各省庁の局長による会議があるので、そういった場を使いながら報告書をまとめて公表するという仕組みもあるかと思うので、今ある仕組みも活用しながら情報セキュリティ報告書を作りたいと考えている。報告書を一つにまとめて点数を付けるつもりではなく、数量的な部分をベースとした比較評価が良いだろうと思っている。ベースとなる情報が満載されていて、それをもとに政府機関としての現状が定量的に明らかになるようなことを考えたい。

○　ＰＤＣＡサイクルに関してであるが、これ自体はマネジメントサイクルでいわゆる自主管理というものだと思う。外部監査の活用について導入可能な政府機関は積極的に推進するとされているが、外部監査と言わないまでもＰＤＣＡのマネジメントサイクルかマネジメントシステムとして有効的に機能しているかどうかということを客観的に見る何かがあると思う。例えば、ＮＩＳＣが統一的に見るとか、客観性を持たせた準拠性の確認はあったほうがよい。

⇒　現在、統一基準で求めているのは、それぞれの役所でＰＤＣＡサイクルを回しなさいということで評価の仕組みが書かれており、自己点検をしっかりやり、その結果を踏まえた監査もしっかりやりなさいということを求めている。その上で、内部監査なのか外部監査なのかそれはそれぞれの役所がしっかり選んでやっていただくということである。最終的にできあがる報告書は単に点検だけやってその結果に満足するだけでなく、本当に有効だったかどうかを含めて、そこまでチェックされたものが報告書としてまとまることを期待している。そのためにガイドライン等にどういったことを求めるかはしっかりと考えたい。

○　ＰＤＣＡを回すということなので、何を測定するのかというのが一番重要になる気がする。報告書類を読んでも、セキュリティポリシーを作っているのか、監査をやっているか、教育をやっているか、というようなことが定量化されて出てくるというケースが圧倒的に多く、それも重要ではあるがそれは第１段階の話であって、本当の目的は情報セキュリティが守られているがどうかということを直接的に測定する結果の指標が必要で、それを守るための代替指標であるプロセス系だけで語ってしまうことが多い。是非、第２次のＰＤＣＡとしては結果系の指標で測定するということを明確にし、指標を作っていただきたい。可能であれば、こういう結果系の指標であるというところまで踏み込んで書いていただきたい。

⇒　具体的によい指標の案はあるのか。

○　例えば、インシデントの数を管理し、インシデントの分類をし、それに対しどうであったかを定量的に評価するとかというのは、結果系の指標としては考えられると思う。そもそもインシデントの管理はされているのかという問題もあり、第２段階としてはやったほうがよいのではないか。ポリシーを作って、終わりというのではまずいと思う。

⇒　当然ポリシーを作ったかどうかということは卒業していると思っており、委員からお話のあったインシデントを含めて、どういった結果指標があるのかというのは考えていきたい。当然インシデントの数は把握して欲しいし、しっかりした統制構造ができれば、上がってくると期待しているので、そういったものをどのように盛り込むのかは詰めて行きたい。

（４）行政情報システムの最適化の取組みとの連携、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確保に係る検討について

○　業務システムの個別最適化が図れなければ、連携させても、全体最適を望めるものではない。その根本は、ＩＴガバナンスがない状況で、最適化の信頼性が認められないことである。個別の最適化を連携させることによって、情報システムのＴＣＯを低減することに十分貢献できるか。

⇒　行政情報システムの最適化は総務省の行政管理局で進めているところであり、これまでバラバラであったシステムを整理し、各省横断的に行政に使うシステムについて計画的にきちんとしたシステムを作る取り組みである。ここ４、５年で一通りの計画が実施され、最適化が図られている。我々としてはセキュリティという方針を入れることによって、更に上のレベルでの最適化を図ることを行っていきたい。行政管理局とも、どのように検討するか整理を行っていきたい。現状の最適化のステップの中で、セキュリティの観点を盛り込むべきではないかということである。

○　ＮＩＳＣと行政管理局でしっかりとした検討をしていただきたい。現状の最適化はコストと業務時間を中心視点と置いた最適化であり、各省個別システムの最適化になっていると認識している。コストや業務時間の観点だけではなく、セキュリティや横の広がりが必要である。ＧＰMO等で全体最適が行われているが、情報セキュリティに関しては、同等若しくは同等以上の取りまとめの機能を強化していただきたい。最適化とは異なり、情報セキュリティはＮＩＳＣというセンターが設置されており、その機能強化、組織構造の強化は図れるのではないか。

○　ＧＰMOは機能しているか。

⇒　ＧＰMO補佐官である立場で述べたい。ＧＰMOはＰMOが実施することの支援を行うものである。共通業務における最適化があり、省庁横断的な管理システムについてはＧＰMOが積極的に関与している。多数のシステムがあり、いくつかの特徴的なシステムについて関与するという形になっている。セキュリティの面で関与が必要ということで、情報セキュリティ補佐官と併せて行っている。機能はしているが、量的に全てをしっかり行えているわけではない。かなりの部分はＰMOにお願いしている。

○　特定システムでサポートしなければならい案件では、かなりの部分でサポートされている。しかし、全体のバランスをみることについては、若干まだ手が回っていないという印象であ

る。

○　今回の案にあるように、最適化とセキュリティを計画的に行わなければならないということだと思う。

○　事業継続性の確保は今回の基本計画の目玉になる部分であり、機密性の高い情報の保護等とは分け、充実させて記述する方が良い。流れとしては、「本来は重要度評価を行いメリハリを付けるべきであるが、当面それが難しいのでＢＣＰから攻める」ことを明確にしたうえで、そこに重心を置くということではないか。これまで複数の委員も述べられていた、「本当にいざという時に大丈夫なのか」といった危機管理対応が一番重要との強い問題意識を受ける意味でも、力を入れて書くべきである。なお、可用性の問題はこの事業継続性確保に係る検討であぶり出されクリアになる一方で、機密性についてはＢＣＰとは関係ないため引き続き底上げ型で行く、という理解で良いかは確認しておきたい。

○　事業継続性の確保に関しては、「やってみて如何にできないかを思い知ることからスタートする」ことが手っ取り早い。首都直下型地震対策大綱において、当日中に復旧しなければならない業務があり、一方で新型インフルエンザの検討も進んでいる。首都直下型地震で被災当日中にも絶対にやらなければならない業務と、新型インフルエンザが蔓延した時に這ってでもやらなければならない業務はほぼ重なる。それらを抽出し、テストや訓練を行うのが良いのではないか。抽出される業務が多数あるところは、実際に対応できる人が集まらないなどといった課題が浮き彫りになるであろう。そのようなアプローチで、机上の議論ではなく、具体的にあぶり出し、日本全体で重要な業務を特定し、それらについてはＮＩＳＣを中心に徹底マークしていくのが良い。一方で、その他の業務については、自主的な取組みや啓蒙のようなことでカバーしていくことが現実的なアプローチではないか。

⇒　首都直下型地震と鳥インフルエンザなどのパンデミックについての問題は、現実には性格が違うという理解で取り組まれている。それぞれについて動いている部隊があり、そういったところとの調整も今後努めていきたいと考えている。

○　性格が異なることは理解しているが、被災当日に突然影響を受ける重要な業務と、普通の状態から徐々に欠けていき、最後に残る業務はかなりの類似性があるはずで、そのことを考えてみるだけでも面白いテーマである。

⇒　そういった仮説は、現実問題としてまだよく分かっていないが、おっしゃるとおり面白いテーマである。事業継続性確保と機密性の高い情報の保護は分けた方が良いというご意見については、元々分離して考えている。可用性はＢＣＰで押さえており、秘匿性の管理

については統一基準等で取り扱うということになっており、その意味でも分離されている。

○　行政業務システムの最適化の取組みとの連携に関して、「情報システムや物品の調達に際して、必要となる情報セキュリティ対策を設定するために参考となる各種情報を提示し、・・」とあるが、ある水準を維持するという観点では、基準やガイドランを提示する必要があるが、記述されおらず、その点もケアする必要があるのではないか。

⇒　米国で行われているよな、どのようなシステムにどの程度の対策が必要かということを示すことも行わなければならないのではないかということについて、意識としては持っている。米国の進め方などを見つつ、我が国で上手くできるのか、あるいはそこまでいく必要のない範囲でできないかという方向性の検討は第２次の中で行っていきたい。情報システムの格付け等の検討は行ってまいりたいが、いきなりはできないだろうと事務局では考えている。

⇒　例えば、米国のシステムへのインパクトのカテゴライズや fixed and security configuration(フィックスド・アンド・セキュリティコンフィギュレーション)という考え方があるが、このようなものを政府調達へ適用することは難しい面がある。基準を政府が設定し、政府調達へ適用することはハードルが高い。これをどのように切り抜けていくかは、事務局として今後取り組みたいと考えており、このような表現になっている。

○　基準やガイドランをやや緩和した形で含めることも考慮し、「参考となる各種情報を提示」とされているということか。

⇒　その通りである。

○　システムと情報システムという言葉が混在している。重要インフラなどでは使い分けに意味があるということで分けられているのであればよいが、そうでなければどちらかに統一すべきである。ただし、全体として情報システムに偏ってしまっており、情報システムを使用する周辺のもの、業務フロー等についての記述が少なすぎるのではないか。

○　機密性の高い情報の保護と事業継続性確保の部分は、分けて記述するほうがよい。事業性確保について、災害や障害についての記述があるが、攻撃などについては敢えて触れないのか。あるいは、災害のうちの一つと読むのか。災害や障害だけとすると、システム障害は非意図的要因のみで起こるというイメージがベースとなってしまう。意図的な攻撃、悪意などに対する事業継続計画は多少異なるものになるのではないか。意図的なものに対しても備えるべきということは盛り込まれるべきである。

⇒　災害や障害として認知するプロセスをＢＣＰで書き出した方が、素直にいく。その中で障害の中に含まれると考える。首都直下型地震に関するＢＣＰ策定のガイドラインが出されているが、それ以降政府でもシステムの工夫とＢＣＰ策定に苦労している。その中で、どこまでできるのかという意味でも、優先度を置いて取り組むほうがよいのではないかという印象をもっている。特出しとして攻撃、意図的行為を位置づけるより、リスクアセスメント、評価の中での優先付けをまず行い、そのようなものを検討するアプローチを採るほうが、各省もつくり易いのではないか。これはあくまで印象である。

○　人間系の記述が少ないのではないかというご指摘も重要な点である。ＩＴ担当室の電子政府評価委員会の委員をやっているが、そこでは、業務改革の観点からある程度セキュリティを加味して検討している。しかし、セキュリティに焦点を当てているわけではないので、ＩＴ担当室とＮＩＳＣの協働作業が必要になるだろうという認識をもっている。

○　「企画・設計段階から情報セキュリティを確保するための方策」とあるが、企画・設計段階だけで情報セキュリティを確保すると採られることはよくない。企画・設計段階で情報セキュリティを確保することは当然であるが、製造、運用を含めた全てのフェーズで、早め早めにやることで、トータルコストを抑えつつ、情報セキュリティが叶うはずである。企画・設計段階に、構築、運用段階に至るまでという言葉として追加した方が誤解がなく、よいのではないか。

○　ＳＱＬインジェクションの被害を調べると、あちこちにたくさんあったというようなことは、皆がバラバラに作り、後から調べるのでそのようなことになる。検査に多大なコストがかかるが、今後もそのようなものを無数に作り続けることになる。それに対して今後も場当たり的に予算をとって調査をしてもしょうがない。既に検証されたもので、ライブラリ単位、アプリケーション単位に共通化を図ることがＴＣＯの削減に繋がる。

○　パンデミックにしろ震災にしろ、データがなくなることについては議論されるが、データを取ったところへのアクセスする手段がなくなることもある。パンデミックになれば外出もできない。データのバックアップを考えるのであれば、セキュアなリモートアクセスの手法の確保も必要である。技術的には可能になっているので、そのこととセットで書いておく必要がある。

⇒　上流工程から開発段階、運用段階までのトータルな情報セキュリティ対策が必要であるという認識は全体の中で持っている。今の統一基準は運用段階の情報セキュリティ対策である。政府のシステム開発では様々な面で統制構造がなかなかうまく行かない。少なくと

も上流工程については、統制構造が効く部分であり、そこをきちんとやれば全体のコストは下がってくるという書きぶりなっているが、誤解を与えるのであれば、書きぶりは考えたい。

⇒　共通化を図った部品を使うことについては、かなり難しい面がある。これは検討させていただきたい。

⇒　セキュアなリモートアクセスについては、書きぶりは考えさせていただきたい。

○　マネジメントハンドリングの中ではインシデントハンドリングというものがあり、攻撃、インジェクションに対して具体的なレスポンス、分析を行うなどの構造がある。事後対応力に関して、レスポンス・リカバリーの強化とあるが、これは何か起こった際に、早くリカバリーするということだけを記述しているのか。その他に、二重系の考慮などの事前対策で、リカバリーを早くするなどの対処を考えなければならないが、それは含まれるのか。

⇒　今後も盛り込む内容については、議論があるところである。少なくとも事後の振舞について、レスポンスと呼ばれる部分、定常状態に戻していくリカバリーの部分を分けて考えており、その中の粒度が情報システム単位なのか、省庁の機能単位なのか、省庁や政府全体をみたときなのかは多様であり、悩んでいる。各省庁にこの部分を頑張って作れと言っても、どうやればよいかということになるため、何らかのことは書かなければならない。委員が述べられた、情報セキュリティにおけるレスポンスワークやリカバリープロセスに限定したくなかった。広い意味での組織機能の観点からのレスポンスとリカバリーから行ってはどうかと考えている。よい書き方があれば、お願いしたい。

○ まだご議論があると思うが、ご意見がある方はメール等で事務局までお寄せいただきたい。

（5） 政府機関における人材の育成・確保及び職員の意識啓発について
情報セキュリティ対策を適時に行うための予算面の取組みについて
技術面の知見を蓄積・活用する仕組みの構築について

○　政府機関の内部人材については、「既に決められた方針を踏まえて積極的に取り組もう」というトーンであるが、今までどおりの方策で人材が育っていくかは怪しい。人事ローテーションの長期化に関する意見が採り入れられないにしても、何か具体性を持った対策がなければ今までと変わらないのではないか、という気がする。

⇒　もう少し具体性をもって書かれるべきであるとは思う。検討していきたい。

○　委員の積極的な案というものがあればお願いしたい。

○　２・３年で全員が変わるローテーションを変え、専門的にＩＴやリスク管理を行う人材を育て、そのような人材がＣＩＯなどに就いていくという路線が一案である。これは前回も議論があり、何人かの方は、それが有効な方法であるという意見だったと思う。そうは言っても当座は困難だから、繋ぎとして外からの人材を活用するということではないか。このままであれば、「ずっと助っ人集団のままで行く」ことを認知する結果になる。

⇒　政策として人事に踏み込むことは難しいところがある。人事ローテーションの長期化と専門性育成については検討できる範疇かとは思う。専門職員について、少しずつ長期化しようという動きはある。最終的にＣＩＯまでになるといった、キャリアパスまで構築することは難しいのではないか。

○　銀行に入る人と役所に入る人の学生からのキャリアパスは似たようなものであり、どちらに行こうか迷うような感じで分かれている。今や、２・３年異動でジェネラリストという名の下に育ち、民間に転出しようと思ってもどこにも行けないようなキャリアパスが良いとは必ずしも全員が思っていないのではないか。ＩＴの時代であるから、地道にその道の専門家になって良いと思う人もいるはずである。

⇒　電電公社がＮＴＴになった当初、人事ローテーションは２年であった。その後、５年になったが、それまでに２０年かかっている。ノンキャリ・キャリア制度がある中で、ローテーション制度があり、ローテーションで回っていくので専門性が全くなく、下の専門性を持っている人たちに支えられているところでのローテーションの長期化は、言うは易いが、実現には１０年はかかるのではないかという気がする。少なくとも内部人材を育てようということを挙げている。そこで人事に関してどこまで踏み込めるかは、書きぶりとしてあるかとは思う。人事ローテーション、キャリアパスの検討については第１次基本計画でも触れているが、結果として難しいということであった。

○　人事ということではあれば、今補佐官が述べられたようなことでよいと思う。情報セキュリティについて知っている部門は、結構たくさんある。その中でローテーションを行うということは、ＩＴ人材については書かれている。そのレベルではまだ実施できるかもしれない。ＩＴ人材の育成・確保指針と、それに基づく実行計画を作ったときの目標を考えると、各省庁の計画レベルに落とすということが非常に重要である。自らが作れば、それをどのように実行しようということなる。ＩＴ人材の育成・確保実行計画は各省庁にあるので、情報セキュリティをそこへ盛り込むこともよい。各省庁の計画レベルに落としていただきたいという

のが意見である。

○　最高情報セキュリティアドバイザーやそのスタッフとなる人材の確保とあるが、それは是非お願いしたい。ＣＩＳＯなどの承認ライン、決定ラインの人材教育についても、そういったラインを作った上でお願いしたい。

⇒　決定ラインについても含めてしっかりとしたＩＴの統制構造を作っていくという目標は出していきたい。大きな役所ではシステム部門がいろいろなところに散らばっており、それをまとめたキャリアパスは考えられる。個別のＩＴ部門がポツポツと島のようにあるのではなく、そこを繋ぐ橋、そこをコントロールする仕組みも人材育成としてはあるかとは思う。

○　技術面の知見を構築・活用する仕組みの構築について、「関連する独立行政法人や情報セキュリティ関係団体などの研究者・実務家の知見を集合的に活用」とあるが、この活用イメージが分からない。ＮＩＲＴというようなものをイメージしているのか、情報セキュリティアドバイザーと言っている上に、さらにアドバイスを受けたいのか、そこが分からない。

⇒　元々の考えは運営上のアドバイスをいただくというようなことではなく、例えば技術的な進展具合、新しい技術の投入、また他の国の動向を調べるグループが独立行政法人などの中にもたくさんある。内閣官房情報セキュリティセンターだけで行うことは困難であり、整合性を持った知識を集めて、政策展開する際の助けにするということである。オペレーションに対してアドバイスをいただくといったことより、技術、他国の政策、標準化、暗号の危殆化についてというイメージである。ＮＩＣＴ、ＩＰＡ、産総研などといったところの、研究、標準化、動向調査チームと連携するイメージを持っていただければと思う。

○　そういったイメージであれば、最初の書きぶりが誤解を招いている。「情報セキュリティ対策の推進にあたって」となっており、オペレーション的に読めてしまうので、先進的な情報を得たいのであれば、そのような書きぶりにした方がよい。

⇒　今般のＤＮＳキャッシュポイズニングのような問題をきちんとした言葉で説明できる人間がなかなかいないので、ＪＰＣＥＲＴ／ＣＣから先生に来ていただいたりしている。そういった意味では、必ずしも企画・立案だけではないというところがある。

○　書きぶりのところで、例えば「企画立案の際の情報収集」や「特殊な状況における専門知識の必要なとき」などの例示があった方がよい。

○　人材育成は重要なテーマであり、職員一人一人の意識を高めていくような、教育・研修も重要である。一方、お役所の場合、人事ローテーションを長期化するのは、なかなか大変だと思う。そのことを考えると、専門家がなかなか育ちにくいということを前提に、人にノウハウを蓄積するだけではなく、組織に蓄積する方法を強調することも、人材育成と合わせて記述しておく必要がるのではないか。具体的には、内部統制で考えれば、ものの管理はＩＴなどで行うのか、文書のマニュアルによる取り扱いを定めて、それを守ることで担保するのかといった手法が一般的になっている。同じように情報セキュリティを担保するためドキュメントの整備をきちんとやるということも、人材育成と併せて強調していただくことも必要である。

⇒　そのことも含めて、書き方を検討したい。

○　まだご意見があると思うが、ご意見がある方はメール等で事務局までお寄せいただきたい。

（６）その他の情報セキュリティ対策の推進について

○　アウトソーシングの問題については、他の暗号利用の推進やＩＰｖ６対応化とは性質が異なり、ＰＤＣＡサイクルの実効性強化や事業継続性確保等を担保することに密接に絡んでくる重要なテーマである。「その他」の項でなく、全体を貫くテーマとして書いた方が良い。

⇒　この文書は第１次提言の章立てに沿って、まずは書いており、全体の文章整理の中で適切に項立てを整理していきたい。

○　運用・管理を委託している情報システムの情報セキュリティ対策の強化とあるが、外部にアウトソーシングする際に、運用や管理を情報システムとして委託している場合のことを書かれていると思う。これは重要なことである。セキュリティを考えた場合にアウトソースを広めに捉えることはできないか。業務を委託するなどあるが、アウトソースを考える際のセキュリティの対策をもう少し幅広に書いていただいた方がよいのではないか。

⇒　先ほどのように、そういったことも含めて整理したい。

○　「政府機関のドメインであることが保証されるドメイン名」があると書かれているが、そういった技術を確保する実現可能性やコストはどうなるのか。メール等の場合、どのドメインから来ているのかについて、我々が見ることはなく、いくらドメイン名を確保しても意味がないのではないか。

⇒　政府機関のドメインは go. jp であるが、政府機関の中でこれを使用していない部局や期間があるので、まずは go. jp を使うということが初めにある。go. jp は一般は取得できない仕組みになっており、JPNIC から政府機関に対して割り振られている。金融機関などから送られてくるメールには電子署名が付き始めている。そのことを確認できる、あるいは確認することを明示するメールソフトが増えてきている。そういったことを go. jp について、政府機関から出て行くメールに対しては、電子署名による保証ができるのではないかというとを後段では書いている。これに関するコストは、電子メール送信者に電子証明書を発給するというプロセスが必要であり、政府機関でそれを発給する基本的なフレームワークはあるので、どれだけ活用し、どのように使っていくかによって、膨大なコストが発生しないようにできると考えている。国民からすれば、政府が出す電子メールには電子署名が付き、メールソフトで確認ができるということである。

○　運用・管理を委託している情報システムの情報セキュリティ対策の強化について、運用管理を委託している情報システムに限らず、いろいろな業務をパートナー企業と行わなければならないのが現実である。様々な外部委託のセキュリティ管理は厄介なことだと考えている。実際には相手先に監査はできないので、チェックリストや教育等でレベルを上げようとしている。ここに「適切な運用が行われているかを確認するための取組み」と書かれているが、具体的にはどのような取組みを考えているのか。

⇒　今、おっしゃられたようなことをまずは行っていくことを考えている。統一基準の中で外部委託の際の要件が書かれているが、そこで挙げられていることを着実に行っていく、どういったレベルで行っていくのかを検討すべきと考えている。

○　民間では格付け会社ができている。情報セキュリティ対策をきちんと行っているか、仕事を出す側が１０社個別に仕事を出す際に、個別に監査を行うのは大変なので、格付けがＡ、Ｂであるということが分かる仕組みがあれば、個別に監査を行うコストが省ける。そういった仕組み、考え方を取り入れてはどうか。

⇒　財務状況における格付けは、政府調達でのカテゴライズ、社会的にも広く活用されており社会的合意はされている。情報セキュリティに関する格付けの費用効果は、政府調達も含め、広くつかっていくという社会合意があるようには、未だ見えない。今の段階で明示するということは、リスクがある。そういった格付けがあれば楽だが、どのような評価がなされていくかまだ見えない。企業をこちらから監査できないので、外形標準で締めこむか、部品調達のように数値化する法律を作ってやるのか、あるいは社会通念的に合意された企業評価ができてくれば、活用可能かもしれない。今の段階では、それを方向性として表明することが難しいのではないかと考えている。動向を見ていないわけではない。

○　格付け会社を使う、使わないというところだけに捉われず、ある省庁が企業に外部委託している際に、監査やチェックリストの確認を行った場合に、その結果を他の省庁で活用するなど、ミニマムに考えることはできないか。

⇒　競争入札の環境の中で行うことは難しいのではないかと考えている。

○　情報システムの場合は、預かる情報の重要度、要求されるセキュリティが異なる。データセンターの場合、非常に高いセキュリティレベルのセンターに収容する場合もあれば、それなりのところに収容する場合がある。格付けは会社によって変わるというより、システムへのセキュリティ要求条件によって変わるということが一般的である。会社によって格付けをしようというアプローチではなく、発注側のセキュリティ要求をＡ，Ｂ，Ｃ等、グレード化するようなガイドラインを作っていただく方が適用しやすのではないか。

⇒　それについては、「情報システムや物品の調達に際して、必要となる情報セキュリティ対策を設定するために参考となる各種情報を提示し、」といったところで、セキュリティリクワイヤメントのレベル付けや適用、明示化を行いたいと思っている。しかし、非常にチャレンジングなことである。特別管理秘密を取り扱うこととそれ以外のところは、政府基本方針で分かれている。政府システムへそれをどのように分類するかは、いろいろな考え方があり、諸外国の失敗の事例などもあるので、それらを勘案し、チャレンジを試みたい。

○　なりすまし等の話で、インターネット上で何を信じるかという根本を考えた方がよいと思い始めている。トラストアンカーをどう設定するかということであるが、現在のＩＥで電子政府の証明書は入っているが、ＩＴ業界のトラストアンカーのイメージと、政府がこうですといって作ったトラストアンカーはずれていると思う。グローバルには明確にずれている。そこをきちんと考えることが第２次では必要ではないか。

⇒　それについては、いろいろと調整の中で行われている。地方自治体についてのＣＡの運用に関しては、Ｗｅｂトラストのリクワイヤメントでどの程度かということを明示し、ブラウザへの組込みと、ＤＮＳ含めたＣＡ側の責任について組み込まれている。ＣＡを含めた電子政府の部分のついては、政府がこうですよということで、マイクロソフトや他ベンダーのコストが上がっている。マイクロソフトや他ベンダーにおいても、世界標準できちんとしたことをやらなければ、入れられませんということを言われているので、適切に対応していくことを粛々とやっていく必要があるとは思っている。個別の取組みについてＮＩＳＣが言及することは難しく、第三者のなりすましについて取り組むということでは調整を始めている。具体的なことは年次計画の中で言及していくことになると考える。

○　各省庁の方で、これまでのところでご意見があればお願いしたい。

○　当省の組織の中では、いろいろと役職を位置付けていが、最高情報セキュリティアドバイザーはＣＩＯ補佐官の兼務ということで、あまりはっきりしていないというところはある。専門性をもってアドバイスしていただきたいということで、いろいろな方にお願いしこういった状況になっている。今後、特定の方を置くということになれば、そういった人を探してくる必要があるので、その辺りのバランスを考えながら実現をしていきたい。

○　予算の部分で成果重視事業についての記述があるが、目標を定めて、事後にそれを達成できたか評価する代わりに、ある程度の融通を認める仕組みである。定量的な目標を定めていくことが重要である。セキュリティの観点から、アウトカムが測れる指標があれば、我々も目標の設定、評価が行いやすくなる。

○　資料５－４に基づき説明

○　まだ、重要インフラ分野の検討状況については、お手元の資料を目を通していただき、今後ご検討いただきたい。

（7）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　－