情報セキュリティ政策会議　基本計画検討委員会
第５回会合議事要旨

１．日　時

平成 20 年４月４日（金）　９時 00 分～12 時 00 分

２．場　所

経済産業省別館　第 1120 会議室

３．出席者

【委　員】

有賀　貞一　委員　株式会社ＣＳＫホールディングス代表取締役
井川　陽次郎　委員 読売新聞東京本社論説委員
井上　雅博　委員　ヤフー株式会社代表取締役社長
筧　捷彦　委員　早稲田大学理工学術院教授
木内　里美　委員　大成建設株式会社社長室理事情報企画部長
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考査役兼企画役システム関連考査担当総括
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 「“大括り項目”ごとの“検討論点”」全体像について

○ いろいろな組織や企業で、例えば事業継続計画（BCP）やセキュリティポリシーは作ったけれども実際には機能していない、というケースが多々存在している。従って、事務局案の「第１次計画の下で構築された枠組みの下で具体的な取組みを機能させて行く」という方針には賛成であるが、本気で取り組む場合、かなり強い動機付けと具体的な推進体制が必要になる。これをどのくらい具体的に実現出来るかが重要になるのではないかと考える。

○ アウトソーシングの問題については、一部にのみ記載されているがより重要なテーマと考える。具体的な推進体制を考えたとき、先ずは企業や政府機関等の意識を高め、委託先管理をきちんとやらせることが原理原則となる。しかしながら、結局のところ、実務のかなりの部分は特定少数の委託先＝IT ベンダーに集中していることが多いので、何らかの形で、IT ベンダーに協力してもらう枠組みがないと、かけ声は掛けられても具体的に推進することは難しいのではないか。

→ 次回の議論のなかで、きちんと取りあげていくべき問題であると認識している。

○ 技術戦略の推進、標準化に関連し、技術的な先進性を持った具体的な暗号方式や認証基盤に関する我が国として推進するべき日本の国策のようなものが、明確な論点として入った方が良いのではないか。可能であれば明確に提示していただきたい。

→ フューチャーインターネットの議論でも、セキュリティは重要な要件になっていることを考えると、全体の IT 戦略との関わりで何らかのものを入れていくのが良いと思う。

○ 第１次情報セキュリティ基本計画においては、「はじめに」という章がメッセージに該当するのだと思うが、国民に語りかけているような感じがない。このメッセージに関する事項については、何らかの段階ではきちんと議論することが必要であると考える。

○ メッセージについては、全体を見通して議論する類のものであり、最初の段階で議論するものではないと考える。個別テーマについて色々と議論があり、理念などが決まった後、最後に出るものではないか。

→ 御指摘はもっともである。第一次提言の構成は、論文の書き方で考えれば良いのではないか。最初に「何を書くのか」という問題設定を行った後、議論を行い、全体が出来た後、最後に序論を書くのだと思う。

→ 事務局としては、御指摘を踏まえ、議論の順番を変更させていただきたい。

○ 一つの事業体あるいは企業主体でもって、そのサービスを完結的に提供している事業者は少ないのではないか。いろいろな事業者が提供しているサービスを利用しながら、サービスを提供している例が非常に増えてきている。そのため、例えばインターネットを考えた場合、うまくつながらないときには誰に文句を言えば良いのか、利用者の立場からはわかりにくくなっている。そのような現状を考慮すると、誰がどのように責任を分担すれば良いのかという視点は、今後避けて通れないのではないか。サービスの複合的な利用形態の存在を前提として、情報セキュリティ対策を考えていく必要があるのではないかと思う。

→ 自由な空間であるインターネットにおいては、責任の問題が出てくると思うので、そ

の辺りをきちんと考える必要がある。フューチャーインターネットの観点でも重要な論点である。

○　今の点に関連するが、責任について検討する場合は、責任を追及する根拠である規範性が必要である。「情報セキュリティ」概念が規範的に定義されていないと、議論が発散する。また、スタンダードがないと言うことになると、抽象的な論点を議論するなかでも、どこで議論することになるかは不明であるが、そういった議論を視野に入れながら進めていただきたい。

→　情報セキュリティ概念を規範的に定義することは難しい。そのため、具体的な施策を見た上で検討しようと考えていたが、必要があれば議論することとしたい。

○　既に想定されているのかもしれないが、計画の期限・スケジュールに関する事項が入っていないので、それは明確に書いた方が良いのではないか。

→　現時点では記載していないが、情報セキュリティ政策会議の委員からは、第１次計画策定の時から「いつまでに誰が何をする」ということを書く必要があると言われているので、最終的には入ってくることになると考えている。ただし、それはもう少し後の段階になると思っている。

○　期限・スケジュールの話に関連して一言。既に新聞・テレビの報道にも出ているとおり、電子政府の推進を急げと言う意見がでているが、資料にも記載のある電子私書箱の議論などは、情報セキュリティ基本計画とかなり関係が深いと考えられる。こうした動向も見ながら考えると、タイムスケジュールを前倒しせざるを得ない事態が発生するかもしれないと考えている。

○　議論全体を見ると、技術的課題の話とリテラシーや社会システムの話が混ざっているという印象。これを分けて整理した方がわかりやすいのではないか。技術的課題については技術開発の話に落ち着き、社会システムであれば事故前提社会の議論に落ち着くと思う。

→　第１次情報セキュリティ基本計画策定の時も、技術的課題の話自体と組織論や社会システム論は分けて議論されたが、その考え方は踏まえなければならない。第１次計画は理念の枠組み作りであったが、その枠組みは堅持する必要がある。他方、指摘の点について明確に意識し、第２次基本計画を策定する際には、より具体的な事を言う必要があると考える。それについても議論していただければと思う。

○　電子政府の情報セキュリティ対策の話は、一番重要なテーマになると思われるので、別途「電子政府」という項目をたてることは必須ではないか。

→　電子政府については、国と地方自治体という二つの事項がある。国については、直接的に影響力を行使できるので、現在の政府内での対策とあわせて、政府のところで書くことができると思われる。現在悩んでいるのは地方公共団体の側で、建前は国と同じ立場であるため、具体的な指示を出すことはできない、現実的には、幾つか調整しているが。また、地方公共団体には、重要インフラとしての地方公共団体という面と、国民へのサービスの最前線としての自治体としての面があり、地方自治体だけは別途記載した

方が良いのではないかと考えている。ただし、地方公共団体の問題については、既に述べたとおり、政府が地方自治体に対して直接指示するようなことを計画に書けないという問題と、具体的なデマケーションの問題があり、総務省自治行政局と検討していく必要があると考えている。

○　今の委員発言については、逆の意見を持っている。電子政府を別項目で立てるというのは、余りにもディテールに入りすぎるのではないか。日本社会全体の情報セキュリティについて論じていくなかで、電子政府がセキュアになることは、率先垂範という面では格別、果たして地方自治体や企業・個人にとって、どれだけの価値があるのか。

○　企業などの場合、その企業サービスが情報セキュリティの観点で信頼できないのであれば、それを買わないだけであるが、電子政府の場合、一定の手続に全国民が従わなければならず、拘束性が高い。また、時に強制力もある。このことを考慮すると、一段違った配慮がいるのではないか。現に住基ネットでも訴訟が起き、総務省で情報セキュリティに関する状況を確認するための委員会を設置して実験を行うなど、相当の議論がある。したがって、政府が電子政府を進めると言っている以上、基本計画のなかでも別途項目を立てることが、国民の観点から言っても必要ではないか。「深掘り」するという趣旨ではなく、問題意識としてここに挙げておいた方が、政府が動きやすいのではないかと思った次第である。

→　地方自治体に関しては、既に述べた特色のほか、国民に関する情報を組織的に収集し、業務に使用しているため、膨大な個人情報を保有している、税収が減少しているために情報システムへの再投資が困難になっている一方で選択可能なサービスではないことから、一定の情報セキュリティ水準が確保されることを国民が期待している、という特色がある。このように、地方自治体に関しては状況が今の中央政府と異なるので、政府がするべきことを考えるという意味では、切り分けて考えた方が良いのではないかと事務局では思っている。ただし、「切り分ける」というのは、その取り巻く状況が若干特殊であるため、そこは注意して書いた方が良いという意味であり、「深掘り」という趣旨ではない。

→　電子政府に対する問題意識は重要であり、かつ、政府が取り組みやすい分野であるが、基本計画の検討に際しては、例えば統一基準やPDCAサイクルについて今後どうするか、設計段階からのセキュリティ確保に向けた取組みや暗号政策をどうするか、ということについての大きな方向性を考えていただきたい。いわゆる「深掘り」については、別の作業で行うことになると考えている。

○　この論点については、議論が尽きないところであるが、これまでの意見については、何らかの形で反映させることとし、その他意見がある場合は、事務局まで送付願いたい。各委員からの意見を踏まえ、若干の微調整が必要になるかとは思うが、最初の手掛かりとして、基本的にはこの枠組みを採用させていただきたい。

⑵　「メッセージ」部分に関する検討論点：第１次基本計画との連続性について

○　第１次基本計画が本当に実現できていると断言できるのかどうか考えてみると、「形としてはできているが、実効性があるかどうか怪しい」というのが、正直なところかと思う。「できてきている」と国民に胸を張って宣言しても良いのか、再確認が必要と考える。もう少し具体的な取組み体制を整備し機能させないと、第１次基本計画の枠組みだけでは実効的な対策を推進し、定着させることが困難ではないか。

○　第１次情報セキュリティ基本計画の時は、データはあったにせよ、それに沿ったまとめ方はしていなかった。しかし、第１次基本計画を推進した結果、データなり事実が集まってきたのは事実であり、我々はそれを当然の前提として議論を展開しているが、可視化されたデータは認識的に提供されていない。それをある程度きちんとまとめていくと、論点全体がデータによって変わってくる事もあり得ると思う。

○　リスクや現実に起きている諸々のトラブルなどの話が第１次情報セキュリティ基本計画を策定したときから変化している、若しくは判明している。そこで、単に第１次情報セキュリティ基本計画に盛り込んでいたことの成否だけではなく、こうしたこともきちんと踏まえて議論していかなければならないのではないか。どのような形で盛り込むかは事務局の裁量だが、その議論によって、実現できていると認識されるのか、できていないと認識されるのか、かなり決まってくるのではないか。

→　第１次情報セキュリティ基本計画の下、実施パッケージとして「セキュア・ジャパン」を取りまとめているが、その取組みについては評価書を作成しており、現在、2007 年度版の作成作業中である。その内容であるが、全体として、リスクの変容や社会の変容について、データに基づいた議論をやるためのとりまとめを行っている。評価書については、４月 22 日の政策会議で事務局から報告をする予定であるが、でき次第、各委員にお見せしたいと考えている。

→　評価書では、単にどこまでできたかという進捗管理的な評価だけではなく、状況変化に対しての認識なども書いている。おそらく、議論がいろいろな形で展開できているのではないかと思っている。具体的には、施策自身、アウトプットというか、純粋なプロセスに関してはできているが、それが本当にニーズにマッチしたかどうか、時代の要請にあっているかどうか、どれだけのレベルまで行ったかというところの評価になると分かれて来る。データに基づいても、微妙なところがいくつかある。

○　トレンドマイクロのサイトが荒らされるなど攻撃者のレベルも相当上がっていることを考慮すると、第１次情報セキュリティ基本計画で考えていたことでは、とても間に合っていないこともある。こうしたことをきちんと分析しないと、第２次情報セキュリティ基本計画には反映できない。また、JPCERT などでたくさん統計を取っているが、その統計を分析することで得られる結論を、ある程度出す必要があるのではないか。

○　日本では2,000 社くらいの企業が ISMS を持っており、２位以下の国の取得数が三桁であることを考えると、フレームとしては情報セキュリティ対策が浸透してきたという印象を持っている。また、政府関係についても、公表された事項に対する反応が出てくるということは、

逆説的にではあるが、フレームが入ってきた一つの証明なのではないかと思っている。しかし、事故が減ったなどの実感的なところでは、まだまだなのではないか。

⑶ 「メッセージ」部分に関する検討論点：第１次基本計画からの変化について

○ 第１次基本計画から第２次基本計画に進化するに当たり、この部分が一番重要であり、ここで基本的な姿勢を示すことになるのではないか。

○ ポイントになるのは、実態を照らすこと、完璧性のないことをもう少し理解することではないかと考える。情報セキュリティに関して考えたとき、労働災害の事例と重なって感じる事がある。労働災害でも相当な努力をしているが、重大な事故につながる事項を完璧に防ぐ事は、絶対にできない。情報セキュリティに関しても防ぎきれないことがあるが、相当の努力をすることでかなり減らせるので、相当の努力はする必要がある。

○ 国民に対しては、リスク意識をわかりやすく高めていくことが必要である。

○ 電子政府が進まない理由に、官の信頼性が欠けているということがある。電子政府的なものを進め横断的にデータをつなげるためには、国民 ID は必要だと思ったが、それを進める前提として信頼性がないと、とても踏み出せないと思う。

○ 企業でも、情報セキュリティ対策は一企業で成り立っている訳ではなく、多くのパートナーと成り立っているという事実を認識し、パートナーとそのレベルを上げないといけない。制度をアウトソーシングする場合でも同じである。周りを巻き込んで実施することは、大変な努力が要るし、やり方を考えないと恨まれる。相当な努力が必要であるということをわかってもらうことが一番大事なのではないか。

→ 人間は無謬ではなく、不確実性が常につきまとっている。それに直面したときの対応をどうするかというのが重要であり、今回、事務局のメッセージは、そこにウェイトを置いてやろうということであるが、今、指摘があったのは、可能な限り誤りを縮小する努力をするとしても、信頼性がないと完璧に限りなく近づくということは出来ず、ゆえに信頼性確保が重要であるということであった。この辺りをどうとりあげれば良いかは意見を聞きたい。

○ 先ほどの説明中、「IT ルネッサンス」という言葉を用い、IT から解放される必要があるという論点を提示していただいているが、この観点は非常に重要。ともすれば IT の完璧さを求める余り、人間が奉仕するような状況に置かれてしまうことがあるが、我々の目指す社会というのは、人間に対し IT が奉仕する形を目指しているはず。IT が人間に対していかに貢献するかという仕組みを上手く作る必要があり、IT に対し完璧さを求め人間が奉仕するのでは、立場が逆転してしまう。これをわかりやすい形で示すことが大切であり、表現を工夫しつつ、是非盛り込んでいただきたい。

○ IT は利便性を追求した人間の知恵であり、人間が作り出したものであることを考えると、IT からの解放という表現は、若干気になる。例えば、生活を豊かにするために生産を拡大した結果、公害が発生したが、それは人間の知恵で解決してきている。それと同じ現象が IT

の世界でも起こっているのであり、これは人間の知恵で解決することは可能であると考える。人間の知恵を活かそうというのであれば良いが、自分たちの作ったものに縛られているから解放しようという書き方は、いかがなものか。

○　人間の歴史というのは、自分が作り出したものに拘束される歴史である。お金がそうで、人間が作り出したものであるが、それに縛られている。作ったものを上手く使おうとするが逆に縛られる、それを相対化してもっと高度な判断で上手く使いこなせるようにしようとする、それが人間の歴史であることを考えたとき、解放という認識はあっても良いのではないか。今、我々はITに拘束されているが、次のステップに行きましょうというメッセージになると思う。

○　とらえ方によると思われる。ITは確かに便利なものだが、人間が本来生きていくという意味において、そんなに凄いものではないのではないか。余り真剣にとらえすぎると、そこに結構縛られるのではないか。

○　情報セキュリティは、必要悪というところまでは行かないかもしれないが、コストがかかるという印象がある。そこで、目的が情報セキュリティというのではなく、情報セキュリティを道具として上手く利用しようという表現を、このメッセージのところに込められたらと考えている。そうすれば、インセンティブの問題も解決するのではないか。

○　国民・個人へのメッセージを重視し、ITからの解放等に関する記述を入れることには賛成したい。また、ITは目的ではなく手段であり、いかに活用するのかということを上手に盛り込んでいただければと思っている。

○　資料中、「人間が」という表現を使っている部分があるが、「一人一人が」とした方がよく、「主体的に考える」という表現は「主体的に活用することを目指す」や「使いこなすことを考える」という表現にする方が良いと思う。また、「人間解放」は重要なキーワードであり、メッセージを少し工夫する事が必要なのではないか。さらに、「人間の潜在能力を最大限発揮出来る環境を構築」とあるが、「人間の潜在能力を最大限発揮して生活の向上に資する環境を構築」というように説明的な表現を入れれば、よりわかりやすいのではないか。

○　高品質と高信頼性と安心・安全というのは、どちらなのかよくわからない。執筆に際しては、一つ一つ、どのような観点から高品質、高信頼と言っているのかということは入れておかないと、同じ事について、人により「高品質を目指した結果」という人と「高信頼を目指した結果」という人が現れることになる。

○　今後、ITを使った社会的なサービス、しかも必要なサービスが広まると思うが、今後問題になると思われることとして、二つの情報セキュリティに関する問題がある。一つは誤信号・誤発報というハード面の問題であり、もう一つは内容を誤るというソフト面の問題である。特に、内容に関する誤りは、即時に大勢の人へ伝わるという点で非常に大きな意味を持つ。とすれば、個人がそのようなITの特質をよく理解する必要があり、それを踏まえて対処する必要がある。個人の知恵あるいは判断力を付ける事が重要であるということをメッセージに入れておかないと、今後、いろいろな意味でITセキュリティを語る、あるいは政策として目

指すうえで誤解を招くのではないか。また、自分が発する情報も場合により大きな影響を持つのであり、個人の責任ということも強く入れて行くべきではないか。

○　今の指摘は重要。教育のところなどと関係づけられるだろう。

○　「第１次基本計画との連続性の下でのメッセージ」の議論に関連し、具体的な取組みを機能させていくという話があったが、とすれば、何故具体的な取組みを機能させるのかという理由が必要なのではないか。

○　自分なりに整理したが、個人・各企業・政府職員が一定の責任を持って情報セキュリティ対策をやる必要があるとしても、セキュリティの専門家になれと言っているわけではない。専門家になれと言っている訳ではないので、一定程度のリテラシーでよく、それがまさに具体化ではないかと思っている。

○　レベルをつけるという議論は、恐らくこの具体化の議論に起因していると思われる。具体化のリテラシーというのをどうやって国民個人に浸透させるか、例えばレベルという考え方があるのではないかというのが私の意見であるが、その意味では今のフレームワークをそのままリテラシーといっても、それは多分理解不能であるので、それをわかる形にすることが具体的な取組みなのではないか。

○　第１次基本計画の大きな枠組みは、IT 基本法第 22 条の「IT を安心して利用可能な環境を構築する」に基づき、第１次情報セキュリティ基本計画のメッセージは発せられていると理解しているが、そういう前提に立ったとき、第１次情報セキュリティ基本計画から変化となるメッセージは、IT 基本法第 22 条の枠組みからはみ出すものを提案しようとする趣旨か、あるいは、従来同様 IT 基本法第 22 条の枠組みのなかでの「IT を安心して利用可能な環境を構築する」ということのメッセージとして伝えようとしているのか。仮に IT 基本法を前提としての議論であるならば、先ほど議論にあった「IT ルネッサンス」というところは、どのような理解をすればよいか。

→　第１次情報セキュリティ基本計画が IT 基本法第 22 条に基づいて書き下されており、第２次情報セキュリティ基本計画においても、IT 基本法の枠組み内にあると思っている。よって、「第１次基本計画からの変化となるメッセージ」に関しては、社会の変化によって IT の安心・安全が変質してきているところをとらえることであると考えている。

→　ただし、我々の活動が IT 基本法第 22 条だけに限定されるとは考えてはいない。御指摘の点は、IT 基本法の上の方の条項を読むと出てくる。また、元々情報セキュリティ政策会議の設置根拠は、IT 戦略本部からのアウトソーシングという形式、ある領域を固め、特出しして議論するというものであり、IT 基本法の枠内にあるのだということを事務局としては認識している一方で、情報セキュリティに関わることが IT 基本法以外の法律等でも出てきているので、それに関しては必要に応じて研究をする必要があると考えている。また、重要インフラに関しては業法との関係もあると考えている。

○　資料を見ると、第２次情報セキュリティ基本計画では、具体的な実現可能性なども考慮し、より実際的な視点に立つとある。そして、客観的に許容可能な水準にリスクを管理していく

とあるが、情報セキュリティのマネジメントをやっている考え方からは常識である。基本的には、それにのっとっていくのが正しいと思われる。

○　問題が生じることを前提として、事業継続性の確保など従来よりも柔軟さを持ち、現実に適した政策を考えるべきとあるが、何となく曖昧性が高い気がする。我々が考えている情報セキュリティというのは、周りの環境にいろいろ影響されるので、良い政策や対策であるとしても、それが機能しないことがよくある。それをPDCAサイクルの中で修正していくのであるが、この国のセカンドメッセージである第２次情報セキュリティ基本計画としては、何かが足りないからこれを加えようというのではなく、preparednessという、先に備えた考え方というものを少し重点的に盛り込むのがよいのではないか。何かが起こっても対応が早く、その次の対策が効果的に行く、そのようなメッセージがここに入ると、今までの議論が上手く収まるのではないかと考える。

○　「100%の安全・安心はない」というメッセージについては、上手く伝えないと、政策の大転換がなされたという印象を多くの人が受けないか。今までと同じ話であるということを、是非上手く記していただきたい。

○　表現について、かなりきちんと書かないといけない、という意見に同意。分量もかなり費やした方がよい。誤解されるのが一番問題である。

⑷　「理念・哲学」部分に関する検討論点

○　「文化」に関する記述について。どのようにつなげるのか気になっていたが、その意味では、「メッセージ」に関連し「IT がどう機能しているか」という話にあわせ、非常に重要かつ有効な手段として、経済的側面だけではない、まさに我々の人間生活のなかの文化まで含め有効な手段になっている。それもあわせて、情報セキュリティを通じてITを考えていくというメッセージにしていただければと思っている。

○　資料中、「セキュリティに軸足を置いて、主要な国家目標と情報セキュリティの関係について明らかにしていくための検討を行うべきではないか」とあるが、具体的にはどのようなことか分からない。

→　IT 基本法からひもとく形で国家目標を書いたのが「第１次情報セキュリティ基本計画」であった。すなわち、IT 基本法で IT 戦略本部が行うべき役割が示され、そのために情報セキュリティの観点からは何をすべきか、という形で書かれていたが、今回は、正面から情報セキュリティの役割を書くべきではないかという指摘を踏まえ、このような提起を行った。要するに、第一次の触媒的な書き方ではなく、もう少し主体的な書き方をすべきではないか、という議論があったので、それをここに入れた。

○　「コストや利便性とのバランス、現実的で冷静な対応」を確立できていないのは、日本特有の現象ではないか。欧米では冷静に受け止めるちょっとした障害等が日本では大騒ぎになってしまうなど、社会的な認識にギャップがあると思われる。従って、これをもって「世界の見本となり得る取組み」と言えるのか大いに疑問。「世界の手本」と謳うなら、もう少し進

んだことを書き込むなど、内容を組み替えた方が良いと思う。

○　「高品質、高信頼性、安全・安心に加えて、コストや利便性とのバランス」という記述があるが、IT 導入の目的は、恐らく第一には利便性を求めてであり、あるいは事務の合理化等の手段、コミュニケーションの手段として IT が使われるケースが多いと思われる。セキュリティのために IT を入れる訳ではなく、利便性を追求した結果、情報を守ることが出来ない、国民生活に支障をきたすということから、情報セキュリティの確保が必要だと言うことになっている。このことを忘れ、セキュリティの確保を先に考えてしまうと、非常に使いにくいものになる。利便性の向上とあわせて考えることが必要であると考える。

○　情報セキュリティの確保について、リテラシーを高めることで対処するという考え方もあるが、限界があると思われる。リテラシーのない弱者をどのように救済していくかということも考える必要がある。この点、法的には、情報を管理する者の責任が重く、情報を窃盗した者は犯罪として扱われないという現状があり、バランスを欠いているのではないか。

○　IT 技術だけで情報セキュリティを守ろうとすると、IT が非常に使いにくいものになる。法律も含め、対処する必要があるのではないか。

○　今指摘がなされた法的な問題については、同じ認識を持っている。しかし、現実問題として、情報を盗取した者に対する罰則体系をどのように作るのかということは、まず、情報というものの価値をどうするのかという問題がある。そこには、「誰の情報か」という視点があり、そこを上手く整理する必要がある。また、例えば個人にとっての情報であるとしても、それがどのように使われるかによって、その価値もまた変わってくる。こうしたことの全体を見通した罰則体系を作れるかというと、なかなか悩ましいところがあり、情報窃盗に対する包括的な罰則が規定されていない。但し、特定の切り口から見れば罰則を規定することは可能であり、例えば営業秘密については不正競争防止法で規定されている。このことを考慮すると、罰則体系を作ること自体は、決して不可能ではないと考えている。

○　その際、情報セキュリティとの関係における情報の法的な評価、情報が情報セキュリティとの関係でどのような意味があるのかということについて整理をしないと法体系を作ることは困難であると考えているが、これを作らないと、責任という問題にも、保護という問題にも対応出来なくなると考えているので、何らかの方向性は第２次基本計画のなかで示していければと考えている。

○　高品質、高信頼性、安心安全に関しては、日本においてはやりすぎるという面がある。やることは良いが、どこまでやっているか、わけも分からずやるという国民性があり、結局は国際的に負ける。ルールや法律、国際規格のレベル等は設定した方が勝ちである。IS015408 の７つのレベル等は既に決められており、変えようがない。日本が参画して決めたかといえば、決めていない。高品質、高信頼性、安心・安全についても、ヨーロッパの国などがレベルを決めてくる可能性がある。政府の各種委員会において、グローバルな観点から国際ルールや規格を押さえたものが勝ちという感覚がなさすぎる。レベル感がなければ議論は進まないと考える。

○　全体的な理念や哲学の部分でのジャパンモデルというのは、レベルを設定し、国際規格にすることなどが表明できると良いのではないか。今やろうとしていることは非常にレベルの高いことで、日本はレベル７のうち５だとか６を目指しているが諸外国はまだ３か４だ、ということが言いきれることをやれれば日本のポジショニングは上がる。

→　レベル感を議論することは戦略的に大事であるが、日本の取組みがレベル感を言えるレベルまで来ているだろうか。

○　議論できると考える。議論を出すとマスコミに叩かれるので最高レベルの話しかできない、というだけの話である。レベル感の議論自体はできるし、どんどんやるべきだと考える。それをやらない限り、従前からのコストの問題などは片付かない。議論を巻き起こし、多少叩かれてもやるということが必要だ。アメリカも国際規格を作ることにまい進している。

○　どのレベルで何を出すかということをしっかり書き、議論して合理的にこう決めた、こういうところを目指す、ということを書けばよい話である。

○　「世界の見本となり得る取組み」とあるが、「見本」というのが良くないのではないか。主導的に世界に対して発信していく、世界を主導していくことではないかと考える。

○　IT の利活用ということで情報セキュリティがあるが、情報セキュリティを追求することで IT 技術そのものがもっと高レベルのものになる、日本独自の技術等を年月をかけて作っていく、情報セキュリティ技術だけではなく情報技術そのものを発展させていく観点を盛り込むことはできないかと思っている。

→　できれば、技術戦略推進の重点施策に盛り込んでいけないかと考えている。実施も考慮したインプットが必要であるが、このパートの多くが総合科学技術会議へのインプット項目になると考えているので、技術戦略推進の重点施策の柱として入れるほうがより具体性があると考える。

○　先ほどのレベルの話は、製品の評価保証レベルのお話だと思うが、誤解があると思われるのは、一番高いレベルがよいと一般的な認識があることである。本当は、妥当なところへ行くべきだという議論であるべきである。コストや利便性とのバランスというようなことだと思うが、高品質、高信頼性ということを強調するにしても、適切なところへ行くべきであり、それを認識するためのカテゴリが欲しい、というイメージである。レベルは必ず高い方がよいととらえられると、それは誤解があると思う。

○　IS015408 のレベルで良いかは分からないが、軍事関係であればレベル７、などのカテゴリなりレベル感があるわけで、そういうものをある程度決めていかなければならない。民間であればレベル３、４で十分だとか言われているが、そういうレベル感、ある意味で「割り切り」に関するルールなりガイドラインを設定することも含めてやるということを、理念や哲学の中でも言えれば良いと考えている。

○　レベル感に関する議論を聞いていて、ゲーム理論の利得票の話を考えた。そこでは、国民的厚生がある程度の水準をキープして、個別のプレイヤー、国民や企業の利得表があり、これがパレート最適というか、誰かの利得を上げればば誰かの利得が減るとことがなく、妥当

な水準をキープするというのが重要である。情報セキュリティにおいても、情報セキュリティをやたら高くして、他の厚生（Welfare）を下げては意味がなく、その辺りの妥当な判断が重要であるが、そこにはある意味で指標やマトリックスがあるとよいのではないか。その指標は、こうだというのではなく、このような例示ですという形で、こういう考え方で考えてみましょうという形で提示すれば理解してもらえるのではないか。

○　「世界の見本となり得る」という部分について、今回は身の丈サイズになってくると思うが、そこを一歩踏み込み、今できることプラスアルファの成長目標として、例えば国際的な基準づくり、技術的開発、リテラシーの教育、法的なもの含めた情報上の治安等について国際社会へ向けたリーダシップをとっていくというようなこと、そのことによって産業面の国際競争力、やりすぎずに生産性を上げる手法を我々は日本としてこうやってる、こういうレベルでやっていけば十分だと思っているというようなこと、電子政府を含めた部分では高いレベルでやっていて、普及率は何パーセントぐらいでやっているというようなこと、こうしたことを外向けに打ち出すため「リーダーシップ」や「国際社会へ向けて」などの言葉を思い切り書いてみてはどうかと思う。

→　おそらく書けると考えるが、ＩＴ戦略本部の成長目標設定との重層構造も考慮する必要がある。

○　規定・ガイドライン、レベル感を含めたものを日本の中でうまく議論して、世界に提示してリーダシップをとるといったことを議論してたいただくことは良いことだと考える。ただ、例えばCommon Criteria、ISO15408を作るときに、１つの国では絶対にできない。日本は傍観者であったが、いろんな国が集まって、会議を重ねて皆でレベル感を合わせた。日本だけで、このような指標を作りましたと提示しても、全く乗ってこない。先ほどおっしゃられたように、まだそこまで日本はリーダシップをとれる程にはなっていないのではないか。ただ、日本では17799とかISMSに関わることを通じて、考え方は整理されてきていると思う。国際的な基準作りの議論については、大局的な議論としてはよいが、具体化を考えると、何となく待てよという気がしている。書き方はお任せするが、考えていただいた方がよいと思う。

○　リーダシップは分かるが、国際協調や国際連携等のコンセプトを組み込んでおく必要があるのではないか。規格化においては、ワーキンググループに入り、ロビー活動を行い、主幹事国ぐらいにならないと何もできないというのを体験している。そういう戦略も含め、理念・哲学に入れていくことが必要であると考える。

○　金融立国やコンテンツ立国等、いずれも先進性を目指したが、気が付いたら負けていて、追いつくことに必死になっているという状態にある。情報セキュリティ立国ということで、情報セキュリティ先進国を目指すことは賛成だが、書き過ぎることは問題である。

○　国際的に協調して連携し、いいものを作って世界に貢献するというコンセプトは、是非入れていただきたいと思っている。

○　世界と協調し、その中で一定のイニシアティブをとっていくという書き方がよいのではないか。ポストインターネット、フューチャーインターネットについて、日本、EU、アメリカ、

韓国が研究開発をお金を掛けてやっているが、どのようなパートナーシップで、どこの部分を強くして存在意義、利用価値をアピールするかといった課題はある。フューチャーインターネットで、情報セキュリティの部分でリーダシップを取りたい等、それなりの国際戦略性と協調性を何かの形で出していきたい。あっけらかんと世界で一番になるとは言えない。

○　基本理念について、あれもできない、これもできないという気持ちになりつつあるような気がして、危惧している。経済大国という言葉は削った方がよいとは思うが、基本的には何をやりたいかを主眼として書くべきで、例えば、主要な国家目標と情報セキュリティの関係を具体性をもって書き込むことなどは充実させるべき。

○　制約や合理的な水準をあまり強く入れ込んでいくと、「気配りのすすめ」の基本理念みたいなことになってしまう。技術的・工学的な合理性、国際協調を日本国が目指すのは当然の話であって、どう高きを目指すかのという目標がないと、基本理念としていかがなものかと思う。合理的な御懸念がいろいろあることを批判するわけではないが、基本理念であることは忘れてはいけない。

→　国家目標との関係において、第１次では経済、生活、安保と関係づけていたが、時代状況に沿って、新たな情報セキュリティの目標をどう描くかということが重要である。この辺についての意見があればお願いしたい。

○　電子政府では、日本は遅れているという問題意識を持つべきである。情報セキュリティが一定のレベルにはあるが、国民のコンセンサスが得にくいこと、地方公共団体の問題がある。情報セキュリティについては国が主導するべきであるということは、重要な国家目標として入れておくべきではないか。財政の面でも、この計画のなかで一定のバックアップするんだという強い意思が必要ではないか。

○　技術水準や標準等の国際協調は必要で、総合科学技術会議に出すという部分が大きいとは言え、研究水準のレベルアップと技術開発は相当強力に進めなければならない。この部分は、相当強調して書き過ぎてもよいのではないか。それを生かしていくときには、工学的な合理性が求められるかもしれないが、研究水準のレベルアップと技術開発は不断に進められなければならないもので、この２点は譲れないものである。

○　「セキュリティ立国の思想に基づく情報セキュリティ先進国」という考え方との関係では、第一次基本計画より更に踏み込んで詳細にみると、この表現で妥当かといういう確認までだとは思うが、言い方をもっと工夫しなければならない。国家目標としては、大きな志を大きな枠組みで掲げるべきである。

○　電子政府については、経済財政諮問会議で、早急に支援を行い、また企業・政府（行政）・地方自治体のデータベース連携、システム連携を図るべきとの意見が経団連（御手洗会長）より出されている。そうなると、情報セキュリティは極めて重要になる。したがって、電子政府の情報セキュリティについても十分考慮し、意見を出していくことは重要である。

○　IT 戦略本部でも SaaS、ASP の活用が重要視されており、それらのソフトウェア／サービス提供業者の在り方、情報セキュリティについては極めて重要になってくる。これまでの電子

政府の各部局の最適化だけでは済まない議論になっているということも念頭に置くべきである。

⑸ 「目標」部分に関する検討論点について

○ 無謬性（むびゅうせい）や完璧を求めて様々な施策を十分に行い、その結果として事故が発生してしまうというのではなく、各対応がそれを目指すまでのところに至っておらず、様々な事故が起こってしまっているということも考えられるが、それは、目標が明確に示されなかったり、目標をクリアしていくという状況が見えなかったことも原因としてあるのではないか。したがって、目標・水準を設定する際には、これをクリアしていくためのステップ、段階を追う小目標を併せて提示する必要がある。

○ 「「利益提示型」の奨励」とは何か。

→情報セキュリティ対策について、何かのモチベーションがあった場合、一時的にはよいが、なかなか持続可能な状態にはならない。「対策疲れ」などの声や「どこまでやればよいか分からない」などの議論もこれまであった。利益提供という表現が良いかという点はあるが、何らかのインセンティブが示される方がよいのではないかという趣旨で言及した。

○ 基準等を提示するのはよいが、何らかのメリットを提示することは、それが出来ないところ、ある意味弱者になるところを切り捨てるというメッセージになるのではないかと危惧している。こういうことを基本計画に含めることが良いかは少し迷うところであり、他の委員の意見も聞きたい。

○ 「利益提示型の奨励や自律的に進むような市場構造」というのは、理念としてこのようなものがないと実際の対策がなかなか進まないのは実感。一方で、具体的にどうするかとなると、非常にハードルが高く困難な内容を書くことになるのも間違いない。具体的内容については知恵の絞りどころであるが、強制＝「北風」型では限界があり、何とか「太陽」型にしたいというのが考え方としては正しいと思う。

○ 現在の記述では、「最低水準や基準と、メリットの提示」と一括で書かれているが、両者は方向が全く異なるので、それぞれ独立して書き分けたうえで検討すべきテーマではないか。

○ 最低水準や基準の提示、何らかのレベルやルール、ガイドラインが必要だという点については、これを実際に作ることは非常に難しいと考える立場ではあるが、これまでの議論を通じ、何らかのものがあっても良いのではないかとも考え始めた。ただし、あくまで強制ではなく、目安として参照できるものとすることが適当。

○ 懸念されることは、何らかの基準が定められた場合の対応として、「自主的・合理的に判断し妥当な線で手を打つ」ということであれば良いが、監督官庁や社長が、「全て最高の水準をクリアしろ」というような運用をしてしまい、いわば基準が悪用されてしまうリスクである。

→ マルチグレードの何らかのインデックスを、規範性を担保しないという状況で提示することは、逆に下振れの懸念、つまりは易きに振れる懸念がある。易きに振れないよう

にするにはどうすればよいかということを考えると、政府機関対策についての議論はよいが、産業政策で議論すると規制強化側に振れる可能性がある。これをどうするかということがある。規制強化は自由市場化を目指していることと合致しないと感じているのは事実。

→　どうするかは別として、きちんとした議論をしなければ、一律にマルチグレードのインデックスを示し守るべきだとするだけでは、実施段階において、首が絞まることを懸念している。

○　基準等の提示については、やるべきだと思っている。BCP（事業継続計画）等を防災面で作り、また国内の事業実態に合わせ、大手企業向け・中小企業向けに作っている。これは規制側に走るのではなく、取引や営業等を含め自らの経済的利益に繋がるという観点で作っている。それは必要であって、有効性もある程度自信ができていると理解している。情報セキュリティについては、これに加えて金がかかるという観点からすると、当初導入時に補助金等を付けたりするなどの援助措置をとることは、事務局レベルで一生懸命汗をかくべきことである。必要な政策的ツールというは、他の分野でもバラエティがあり、重要なのは基準を上手く作るということをやることである。

○　実施主体側の責任ばかりが問われているが、実施主体に情報セキュリティを供給する業界はどうなっているのかという素朴な疑問がある。日本のソフトウェア業界がかなり疲弊しているということをよく聞かされる。実態はよく知らないが、悲惨な状況で優秀な技術者が海外へ逃げてしまう。このような業界が、適切なパッケージを提供できるのか危惧がある。言い過ぎかもしれないが、情報セキュリティを供給する業界を育成するという事業を並行して進めることによって、大企業・中小企業が容易に対策のための手段を得られるような施策を強力に推進しなければ､質の悪いものができるなど業界が空洞化してしまうような気がする。この部分は、相当書き込むべきであると考える。

→　産業界の育成は大切だと思うが、育成する場合にどう育成するかが課題となる。予算面の課題もある。

○　切り口・観点を変えて既存の予算を活用し政策を打ち出すことにより、使い方に工夫も出て、別の観点の目標もつき、予算の使い勝手も良くなるということもある。とにかく書かないと始まらない、ということだけは申し上げたい。

○　大手企業では、例えばセキュリティ報告書を出すことなどで、信頼性、ブランドを生かすような活動を行っている。問題は中小企業である。情報システムの提供側の品質の問題があり、ここを何らかの形で向上させなければならない。情報セキュリティは技術だけの問題ではなく、リスクマネジメントの問題も多くあり、中小企業でもコストを掛けずに実施できる部分は、たくさんある。他方、それらが実施できていないことで問題が生じるという面もある。

○　SaaS モデル、ASP 等を上手く活用してもらう、提供側で技術的な面はちゃんとやるということで、中小企業でも許容されるコスト感になるのではないかと考える。情報セキュリティ

に関する費用は利用料金に含まれる形になると思うが、改めて情報セキュリティのコストだと認識する必要もなく活用することができる。

→　将来的に議論していただきたいことではあるが、ソフトウェア、情報システム開発のコスト計算のやり方が変わり、これがどのようにセキュリティに影響するかという課題がある。発注者側が情報セキュリティの部分に対してコストを払うのか、その妥当性をどう評価するのかなどを、提供側だけではなく発注側の責任も大きくなってくるのではないかと考えられる。2009 年に実施されるので、この辺りも品質に関連するものとして、将来的には議論いただきたい。

→　甲府市役所では、新庁舎建設に伴い大規模システム構築し、データセンターでの管理することになっている。機器の調達ではなく、SLA に基づき複数の事業者からサービスを調達する形態になっている。ここでは SLA が重要であり、これらは発注者の責任になる。職員が要件を定義し、基準を設定、チェックを掛け、モニタリング能力も必要となる。基準の到達度に応じて、契約金額の支払い又は減額を行う、基準超える場合は、契約金額より多めの額を支払うなどのことを行っている。このように、契約で基準をきちんと定義し、企業側の責任・発注者側の責任を明確にする画期的な取組みを行っており、今後、このような調達が自治体ではモデルケースになるだろうと言われている。これには自治体が相当な能力を持つ必要があり、研修等も大変になってくる。情報セキュリティサービスの在り方、セキュリティの基準・指標づくりが非常に重要になってくる。

○　進行基準では、工事進捗状況を把握することと、それに応じたコストを計上することが義務づけられる。フェーズ毎の進捗状況や内容がはっきりしないと計上できない。顧客と開発業者側で契約をきちんとしてないと会計上は計上できないため、先ほど指摘があった状況が、かなりのレベルで実現するのではないかとの期待はある。下請けを含めた部分でどこまで到達できるかについては、これからの業界の課題である。

○　自分の家に鍵を掛ける話とそれを破って入ってくる者をどうするかという話は、分けて考える必要がある。構築段階できちんとしたことをどこまでやれるかは、各ユーザなり、対象組織の問題だと考える。自分でどこまでのことをやるかを決め、それを指示できる能力がない限りは、鍵も付けずに侵入されたと怒っても仕方がないのではないか。それでもなお、侵入してくる場合は、情報セキュリティ対策ソフトを入れて防ぐ、さらに駄目な場合は警察等でなんらかの対策を立てることになる。情報セキュリティ対策というと、受け取る人によってシステムの信頼性を高める話にもなり、ウィルス駆除ソフトを入れたかどうかという話にもなる。そこをしっかり識別すべきである。

○　理念・哲学のところで挙げられる３つの国家目標のうち２番目及び３番目と関係するが、情報セキュリティには、攻めの情報セキュリティと守りの情報セキュリティの両面がある。「事故前提社会」の構築等は、防御防衛的な発想が強く出ている。国家の方をみると、安保のところで、防衛的であると思われる。電子政府の更なる展望というと、攻めという面が強く出てきているかと思われる。すなわち、国や社会・個人の主体の中で、攻め・守りが入り

組んで輻輳したマトリックスが書けると考えられるので、この辺りを整理しないと議論してもわかりにくくなる。国家については、今回は電子政府等の攻めの話が出ており、社会・個人との関係での経済価値では、第１次基本計画の展望的で攻めのようなものに対し、第２次基本計画では防衛的な面を出そうというようにも見える。第１次と第２次の連続性がありながらも、非連続として現れる新たな側面であると思われる。そうした観点から整理したほうがわかりやすいのではないかと思う。

○　情報セキュリティを提供する側の問題はあると思う。フルスクラッチでパッケージを作る（０からプログラムを書く）人たちは、情報セキュリティの専門家ではないということは押さえておく必要がある。そういう専門家でないプログラマ、こういった方々にどのようにセキュアなシステムを提供させるようにするかという観点でのアプローチが必要であり、そのためには、サプライヤーと要求仕様書を書く発注者側との共通言語が必要である。個別に議論していくやり方もあるが、中小企業等では、この基準で行きましょうといった一言で済む共通言語、その意味での基準は必要だと現場にいて感じている。

○　最低水準については、基本的にはなくてもよいのではないかと思う。最低水準のレベルがかなり低いものであれば問題ないが、これが高めになってくると、先ほどの切り捨てという議論も出てくると思うので､最低水準がない上での基準ということだけでよいのではないか。最低水準を定義することが大変であるということではないが、それは市場原理の中で適切に定義されるものではないかと思っている。

○　中小企業で情報セキュリティを意識した投資というのはそもそも難しいという意見もある中、少なくともここをクリアしていれば良いという基準のようなものがあれば良いのではないかと気になっている。

○　その意味では、最低水準のようなものがあるべきかもしれないが、細かく議論をしなければ、それこそ切り捨てにもつながってしまう。それをやるのであれば、結構議論を詰めなければならないと思う。

○　経済産業省からモデル契約書の第１版が昨年出され、IT ベンダと対等な交渉ルートを持たない企業等を前提に、パッケージや ASP を使う場合のモデル契約書として第２版が出されるのだが、その中では、受発注者間の共通言語として、共通フレームの 2007 をベースとして作っている。そういったものをベースとして、分かり易くかつ精度を上げることが必要だが、モデル作成の委員会に参加して感じるのは、ユーザ側の参加が極めて少なく、ベンダー側のトーンに流れた作り込みになりがちだということである。求められるのは、受発注者の共通認識、合意形成をいかに作るかであり、バランスを図るべきと考える。ただ、このような具体的なものができつつあり、そういったものを中小企業も活用していけば、少なくとも今よりは良くなると考えられる。

○　基準・水準については、基本的な考え方と最高水準、目標水準だけ示し、特に民間企業等がどの程度の期間でどこまで対応を進めて行くのかについては、自主性に任せるのが良いと思う。「最低水準くらいは要るのではないか」という話であるが、これを示してしまうとモラ

ルハザードを起こしてしまい、「上のレベルに行こう」という成長・改善意欲を削ぐのではないかと危惧する。

○　今日の議論で、「ガイドラインを目安としてマトリックス的に示すことが良いのではないか」という話があった。「最低水準は要らない」という声もあったが、ガイドラインとしてマトリックスを示してしまえば、その中の最低ランク（レベル１や０）が事実上のミニマムスタンダードになってしまうのではないか。当初の議論にあった、第三者機関による監査が有効であるが監査に当たっては基準が必要ではないか、という流れもあり、この辺りをどのように進めるのが良いか、いくつかの案を出し合いながら、次回以降に合意形成を図るのが適当と考える。

→　適用領域に応じて、答えは様々であるというのが現実的であると思う。政府機関では、最低水準は示さなければならないというのはある。ただ、企業に対して示すことは大変難しく、モデル契約書や一定の到達目標点を示すといったことは経済産業省もやられていることであり、適用の文脈によっていろいろなものが実施段階で出てくると考えているが、フレキシブルに対応したいと考えている。

○　PDCA のＣについて、NISC で基準等を明確にし、もっと評価をすべきではないか。

○　レベルや水準は、企業、政府、個人に対応していくつか用意されるとは思うが、例えば重要インフラについては、比較的強制であり、このレベルになければならないということになると思われる一方、そうでない場合は主体がレベルを任意に選び、選んだ以上は責任をもって対策を行う、ということで良いのではないかと考える。その際、任意に選ぶ中で業態や企業レベル等に応じた推奨レベルを提示することにはなるが、選択はあくまで主体側の意思で行うという形にしてはどうか。そして、それに対するメリットが提示され、メリットを共有する場合には、外部的な監査・評価が必要であると考える。また、重要インフラについて強制というものがある場合には、客観的な監査・評価というものが必要となる。水準については、そのような形で整理すればよいのではないか。

○　基準というものは必要であると考える。例えば建築基準法は最低レベルを示すものであり、原子力発電等でも経済的に合理的な範囲でやれといったようなものもある。技術的に可能な水準というのはあると思われ、基準を入れておかないと何処を目指すかわからないということがある。

○　基準作りに当たっては、産業界にある程度やっていただく、業界のプロの方々に専門的知識に基づいてやっていただき、国が基準作りを振興し、ある程度オーソライズするという形をとるのが普通のやり方かと思う。なんでも上から国でつくるというだけではない。同時に基準づくりが産業界の高度化を促すということにもなるので、やっていただくのがよいのではないかと考える。

○　「対策疲れ」があり、インセンティブやメリットが必要であるとのことであるが、対策に疲れるのは、似たような基準を三つも四つもやるからである。ISMS をやりました、プライバシーマークもやりましょう、今度は J-SOX で似たような話が出てきて、今度もう一つ基準が

でてくるとなれば、もういいのではないかという感じがしてくる。既に対策ができている人ではなく、対策をやっていない人たちを対象にするのであれば、最低ここまでやって、できればこうやって下さいという基準があるのはよい。

○　ISMS が良いのは、その基準が一定のところで止まっているのではなく、PDCA のサイクルを回しながら少しずつ高みを目指していくということがメカニズムとして組み込まれている点である。ここで、最低基準のようなものを決めてしまうと、基準自身が自動的に上に向かって歩いていかなくなり、何となく時代遅れの基準がずっと残っているということにならないか懸念がある。

○　基準、ガイドラインが存在するほうが、議論がしやすく評価がやりやすいというメリットはある。NISC の方でも政府統一基準があり、重要インフラでは安全基準等があり、産業界では ISMS がありプライバシーマークがあり、または J-SOX がありという環境で動いている。例えば、総務省で ISP、SaaS に関するセキュリティガイドランを作られたが、一つの業態でも一つのレベルを決めるのは大変なことである。一つの業種の中でもいろいろなタイプがあり、レベルが異なる。レベルや基準というものは案外簡単ではない。否定するわけではないが、既にあるいろいろな基準、政府統一基準等を踏まえて議論をすべきである。できれば、次回このアイテムで１時間半程度時間をとっていただいて、議論していただきたい。

　→　もう少し詰めた議論をする必要はあると考えている。

○　第２次基本計画では、対策推進がメリット、強みであることを対策実施主体が実感できるような利益提示型の奨励へと軸足を移していく必要があるのではないかということについて、基本的には考えなければならないということを合意できたと思う。ただし、その書き方、考え方はこれから詰めていく必要がある。

○　第２次基本計画では、「事故前提社会」の構築と「気付き」をもって自ら考えられる主体の育成の観点は重要であり、これは教育の方にも絡む、という部分についても合意できていると考えられるので、今後この方向で検討を進めさせていただきたい。

○　２つの主体を念頭に置いて２つのアプローチを採ることも有効ではないかということについては、今後詳細な検討が必要であると考える。

○　市場での対応の促進、最低水準・基準やメリットの提示については、基本的にはこの方向を詰めて議論することについて合意できていると思われるので、次回、時間をとって詳細な検討を進めることとし、皆さんの御意見をいただきたい。

○　今回いただいたご意見を重視し、基本計画の策定に向けて進みたいと考える。

⑹ 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。