

**情報セキュリティ政策会議 基本計画検討委員会**  
**第7回会合議事要旨**

**1. 日 時**

平成20年5月27日（火） 17時00分～20時30分

**2. 場 所**

経済産業省本館17階 第1共用会議室

**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

笈 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

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・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)

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

三輪 信雄 委員 総合警備保障株式会社参与

安富 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

##### (1) 「はじめに」及び「第1章 第1次情報セキュリティ基本計画と第2次情報セキュリティ基本計画の関係」部分

- 全体として大きな違和感はない。短期間にここまで纏め上げた委員長と事務局の方々に敬意を表したい。
- 事務局が悩んでいるキーワードの「事故前提社会」又は「脱・無謬性前提社会」に対する代替案を提示したい。「事故前提社会」という表現は物騒との声があり、「無謬性」はややこしい言葉である。三案出すので、その組み合わせで検討してはどうか。一つは「事故耐性向上社会」、事故をリスクと変えれば、「リスク対応高度化社会」又は「リスク対応発展社会」という表現がある。それから、「事故」を「対障害力」として、「対障害力強化社会」又は「対障害力成熟社会」ということもできる。こうした言い換えによって、多くの委員や国民のイメージにフィットするのであれば、それをキーワードに採用すればよい。
- なるほどと思うキーワードの変更案が出て、複数について良いなと思いながら聞かせていただいた。この点について、御意見を伺いたい。
- 先の委員の意見に全面的に賛成する。「事故前提社会」としては見えない脅威があるような気がするので、フォールトレジスタント (fault resistant) というか、障害に強いという感じがあつたらいいかと思う。たくさん、先の委員に提案していただいたので、その辺りがよいと考える。
- 「事故」や「耐性」という言葉は結構であると考えてるが、「リスク」という言葉は避けた方が良いかと正直思っている。「リスク」という言葉が理解できていない気がするので、「リスク」とうカタカナ言葉は避けた方がよいと思っている。
- リスク管理の専門家的に生きてきたので、いろんな意見があることは理解している。ただ、「危機」や「危険」よりも「リスク」と言った方が、世の中としては“やんわり”感がある。「リスク」という言葉の意味を皆が誤解しているだろうか、という気もする。「リスクテイクにより利潤を得る」など、極論というか正論まで考えるとイメージが違うだろうが、漠たるイメージとして「今日、ここに来るまでに電車が止まるかも」の概念で国民的には「リスク」という言葉も普及していると思う。「ザ・リスク」としての専門家の厳密な定義とは別に、キャッチフレーズに使っても良いのではないかな。
- 誤解を受けるかもしれないという点では、この言い方の工夫はあってもよい。インパクトは好きだが、事故前提社会の“構築”とあるから変に感じる。事故前提社会への“対応”や“対応の仕組みをつくる”とすれば、これが生きてくる気がする。“構築”と言ってしまえば、よく理解されないおそれがあるので、少しその表現を変えて、できるだけインパクトのあるものは生かしていければと思う。
- リスクとの関連だが、1頁目の第二段落でリスクの事例として、“自動改札”というのが挙げられている。鉄道事業の観点では、輸送や安全運行が一番大事であり、自動改札でトラブルを起こさないようにすることは当然だが、これはどちらかといえば、利便性のようなもの

である。鉄道のリスクといえば、輸送に伴うものに関する事などだと思うが、リスクの事例として自動改札というのは、全体的にかえって分かりにくくなるのではないか。ここで自動改札があることには、若干の違和感があるというのが正直なところである。

⇒ 特に他意はないが、利便性の向上も意識している。ITを用いて便利・効率的にしたいが、ITをどんどん使うと脆弱性も高まる、そこをどうするかということがある。運行システムだから情報セキュリティが必要で、自動改札だからあまり考えなくてもよいということではない。

- もちろん、利便性を考えなくてもよいということではない。
- この例示は、本提言が出る直前に何が起こったかで、書かれてしまう性格のものであろう。委員の側から「これは止めてくれ」と言うことは適切ではない。その時点で世の中を騒がしたものが原発なら原発、航空機であれば航空機と書かれる。事務局で大きな話題を選んで下さい、ということによいのではないか。縁起でもないが、今後も大事故は起こるだろう。
- ここは、一般的に起こったことを誰もが認識しているところで書いてあるので、問題ないと思う。ただ、「度重なる」という表現をもう少し弱くするという事は考えられる。
- 「事故前提社会」や「脱・無謬性前提社会」という言葉については、時間をかけてゆっくり考えればよいのではないか。これらの言葉は、今見ているものを言っており、目標を言っていないように思える。「対障害力」という委員の意見があったが、「復元力」のある社会というものを目指しているのだろう。第1次情報セキュリティ基本計画では、「しなやかな」という言葉もあったように記憶しているが、そういう言葉の方が好ましく感じる。やわらか過ぎるのであれば、「復元力のある」などがよいのではないか。復元力があるとすると、事故が起こった後のこともあるが、事前のこともやっておかなくてはならない、という二つのことが含まれるような気がする。そういう言葉ではどうか。
- 前々から表現をどうするかということで議論してきた「事故前提社会」と「脱・無謬性前提社会」の用語について、6月中旬には確定して政策会議に報告しなければならないので、ゆっくり議論はできない。ここで無理やり決めることもないが、だいたいの方向性はこの内容であり、あとは用語の使い方ということで理解いただければと思う。「しなやかな」という感性に訴える用語は、人によって定義があまりにも多過ぎる。定義不能な用語は使わないほうがよい。「美しい日本」と一緒に、「何が美しいんだよ」という議論になるので、これはやめた方がよい。できるだけ、ロジカルな言葉にした方が、このような文章の場合はよいと思う。字を読んで、あるいは発音を聞いて分かりやすい用語という点で、個人的な意見では、先の委員からあった「事故耐性向上社会」が字面などから一番理解しやすいのではないかと思う。「リスク」は定義が必要で、経済学と防災科学でリスクの定義が異なるように、ここでどういう意味でリスクという言葉を使っているか説明しなければならない。「事故耐性向上社会」であれば、見て字のとおりですと言えば良いので、妥当かと思う。アピールする、「おっ」と思わせるのは、「事故前提社会への対応」という表現がよいと思う。
- 「事故耐性向上」より「対障害力成熟」の方が、分かり易くないか。「事故」と言いたいのか

にもよるが、狭義セキュリティの問題つまりウィルスへの感染等の脅威まで含めて「障害」と言ってよければ「障害」と表現したい。私は「事故」と聞くと、例えば海外で電車が横転した、といったイメージを受ける。自分の仕事では、セキュリティの話も、安定性の話も、いろんな事案を「障害」と呼んでいる。最近では、格好をつけて「インシデント」と言う組織もある。「対障害力成熟」とすれば、後ろの方での「成熟」ともキーワードが共通する。いずれにせよ、今日は「前向きな感じにする」ということにして、後は事務局で決めてもらえばよいのではないかと。

- 「事故」という言葉は、人が実際に死傷する際に使われることが多く、その観点では、先の委員が述べられたように情報セキュリティに関するインシデントに対して「事故」という言葉を利用すると誤解を生じるように思う。実際、鉄道では「事故」というと、Suica等のシステム「事故」ではなく、死傷者が発生する「事故」を意味するという先の意見を考えると、「事故」という言葉が正しい意味で伝わるのかなという気がする。
- であれば「対障害力成熟」又は「対障害力向上」ということになる。「対障害力向上社会」ではいかがか。
  - ⇒ キャッチフレーズとしては、もう少し毒（刺激）が欲しい。言葉をきれいにすればするほど、よく分からなくなるということもある。「成熟社会」という言葉は、よく見ればわかるが、出した瞬間には何を言いたいのか分からなくなる。こういうことは言うてはいけないかもしれないが、政策を出していくときに「こういうものに向けて頑張るんだ」という頑張る部分で、このような「成熟」とか「円満」という言葉になってくると、“飢え”がなくなる。
- 「事故前提社会」が、言い得ているとは思いつつ、「表現がキツイ」とか、それを「構築」するのは逆ではないか、という意見があるので、“マイルド”にする方向での妥協案を提出した。言葉を強めるなら「対障害力改革」などがよいか。「成熟」がだめなら、「向上」又は「強化」ではどうか。
- 先の「構築」という言葉についての委員意見に同意。「構築」はおかしいのではないかと。「事故前提社会」は仕方がないと思うが、「耐性」という言葉には非常に反対であり、事故そのものを減らそうという努力が全然みえてこない言葉である。「耐えろ」というのは無茶な言葉のような気がする。事故前提としても、研究や開発の部分では、“凡ミス”は突き詰めて、事故を減らすという努力は永遠に続けていかなければならない。これはどの分野でもそうである。「耐えろ」というのが前面に出てくるのは無茶な話であり、例えば飛行機に関して「墜落前提社会」はどうやったってあり得ない。事故を減らすことには、警察庁でも交通事故死ゼロと、永遠にできないだろうが、目標として掲げおり、やはりゼロは目指さなければならない。その観点からも、「耐性」はいかがかと思う。「リスク」という文言を使うことが難しいのであれば、「事故前提社会」で問題ないと思う。むしろ「構築」について違和感を持っている。同じく毒はあった方がいいのだらうなという気はしている。
- 「事故」という言葉が人命に直接影響するようなイメージを持ちやすいために、こだわり

があるのかと思う。一般的には、「事故」という言葉がよく使われている。手形不渡りは「手形事故」であり、郵便で不達があれば、「郵便事故」である。このように、「事故」という言葉がいろいろなところで使われていることを考慮したとき、ここで「事故」と使うことは不自然ではないと思っている。かえってその方が分かりやすく、それが前提であることにどう対応するかの訴えかけ、その始発になるのではないかと思う。

- 今の意見に近いが、第1次基本計画やセキュア・ジャパンの中でも、「事故」という言葉をたくさん使ってきたはず。「事故」は、セキュリティ・インシデントを日本語訳するときに、セキュリティ事故・事件と訳した。事件はないだろうということで、「事故」という言葉を使うようになってきていると思う。一般の人が「事故」と聞いたときに、違うニュアンスのことを考えられるかもしれないが、基本計画のコンテキストでは誤解はなく、インパクトとしても伝わるのではないかと思う。「事故」という言葉は残しても全然問題はない。「事故前提社会」は以前にも使われていたところがあるので、若干違和感があるが、インパクトがあるのでいいかという気はしている。
- 敢えて誤解も恐れず、見出しでこれを使い、本文できちんと説明する。委員意見にあった「対障害力向上」という言葉も本文の中で使い、「事故前提社会」という言葉について誤解のないような形で使用すれば、見出しではアピールしてもよい気はする。
- 「構築」という言葉についても再考が必要で、「対応」は素直だが、もう少し凝るべきか。
- ずばり「事故前提社会への対応力強化」ではどうだろうか。
- 本文では、皆で理解を増進する必要があると書かれている。「対応に向け」と書くと、やはり「事故が起きるのはしょうがないので、あきらめてね」という部分がどうしても出てしまう気がする。事故を減らす、しかも対応もする、どちらも両輪であるとの趣旨であれば、「理解増進」など本文に書いてあるとおりと理解する。「事故前提社会の理解増進」や「理解拡大」など、そういう前提に基づき、皆でいろいろとやろうということではないかと理解している。
- 今述べられた意見も含めて、この「対応力強化」に含まれるという理解が多数意見と思う。どうしても入れると、「理解…等を通じた」または「…を含む」等になり、タイトルとしては長過ぎる。
- 時間も限られており、まとめた。「対応力強化」ぐらいでコンパクトにした方がよいのではないか。先の委員が述べられたことも含めて、本文でくどく書いた方がよい。そういう方向で、「事故前提社会への対応力強化」を進めたいと考える。
- 「構築」はおかしいと思うが、私なりのイメージからすれば、ここで言いたかったことは「亀さんになるつもりですか、シーラカンスになるつもりですか、違うでしょう」ということであり、「外側を柔らかくしても、中に骨があればいいのだから、そういう社会を作ろうよ」という話のような気がする。発想の転換と進化、生物進化ではないが、そのようなことを言いたかったのではないか。「身を守らなければならない、事故がないように努力はする、そのために外側を固めたらガチガチになって動けなくなった」というようなことは止めようとい

うことを言いたかったのではないか。

- そういうニュアンスは、かなり多く含んでいると思う。発想をもう少し転換し、「守れないものまで守るのはおかしいよね」と、やはり限界がある。サイモンなど経営学者が言っているが、合理性の限界、限定合理性など、これは人間の認知能力で当たり前のことである。これを踏まえた発想で、「できる限りのことはやるけれども、起こってみないと分からないよ」、「それに対応する能力が今は重要だよ」ということで、委員の言うとおりであると思う。その意味では「構築」と使った方がよいのかもしれないが、文脈的に見出しとしては苦しいところがある。一旦は、「事故前提社会への対応力強化」ということで進ませていただきたい。どうしてもおかしいということであれば、後で振り返りたい。

## (2) 「第2章 第2次情報セキュリティ基本計画の基本理念（我が国のあり方）について」部分

- 文化のところ、括弧書きで社会風土とあるが、この括弧書きの意は何か。不適合についても括弧書きでミスマッチとあるが、無くてもよいのではないか。日本語としてない方がすんなり読める。
  - ⇒ 特に意図と言うよりも、分かりやすさの観点で括弧書きを付けた。委員の方が不要であるとするのであれば外したい。
- 文化という言葉がこの委員会の席上で言わせていただいたが、その際は、日本人が持っていた良さを外国にも広げるぐらいの勢いのことを書きたい、というつもりであったので、今ここに書かれていることについて特に意見はない。
- こだわりはないが、タイトルでは「文化」に統一してはどうか。「文化」の概念はかなり広く、社会風土的、社会通念的というニュアンスで使っている箇所も多いと思われるので、文中で適度に「文化」と「社会風土」を使い分け、文章の括弧をなくするのが落ち着きどころであろう。
- 12 頁の2段落目の最後の文章で、「情報公開の範囲に係る検討も今後必要である」とあり、一定の線引きのようなことをしなければならぬということだと思いが、この部分は難しく、本当に検討が必要なのか。この趣旨を入れるのであれば、その前の文章で「安全保障については、“可能な範囲で” …」などと逃げておいた方がよいのではないか。
  - ⇒ 政府における情報管理と秘密保護の話は役所の中でしているが、補佐官の目からすると、議論が少しぶれているところ、本来の議論ではないだろうと思うところがある。そういうところへ働きかけをすることを考えると、ここの記述については、少しすっきりさせる必要があるかもしれないが、“フック”を残しておく、いろいろと働ける。
- 趣旨は大変よくわかった。文書は上手く直して、是非“フック”を入れていただければと思う。
- 14 頁から 15 頁のところに書かれていると良かったのだが、「成熟した情報セキュリティ立国」については、自国の技術をどう高めるかについての記述が一切ない。技術については、15 頁目の、「世界における最高水準の取り組みや、最先端の技術の動向についても、情報収集

など…」とあるのみで、成熟した IT 立国にしては、いささかみっともないだろうという感じがする。ここに「日本の技術も向上させつつ…」ということは一言入れておかないと、後で「どうなっているのか」と言われかねない気がする。

⇒ 御指摘のとおりであり、どこかへ書き加えたい。

- 前にも述べたが (ア) 経済、(イ) 国民生活、(ウ) 安全保障の順番については、安全保障が一番に、(ア) にあるのではないかという気がする。国の安全保障が崩れていて、経済や国民生活の話をしてもしようがないのではないかという気がする。書いてあるから良しとするかは分からないが、順序が違う気がする。

⇒ 安全保障が一番先になっていない理由は、情報セキュリティに関わる製品やサービス等のいろいろなものの作用先が、インダストリーや国民であることが多い。情報セキュリティ政策は 2000 年から立ち上がってきたが、サイバーテロ対策だけでやっていった。そういう反省も含め、経済と国民をきちんと見る、その先で安全保障もあるだろうということが第 1 次情報セキュリティ基本計画では書いてある。その雰囲気、プライオリティーを考えたときに、そんなに変わっていないのではないかと思っている。今回、この順番を踏襲したわけだが、国民を前に出すという観点からは、(ア) 経済、(イ) 国民生活は順番を入れ替えてもよいと思う。

- 一文で簡単に済むのであれば、前文に安全保障が最後にある理由を入れておいた方がよい。その方が誤解されないと思う。
- 「(イ) 国民生活」を前へ持ってきたほうが良い気がする。その次に「(ア) 経済」が来る。
- この文章のアピールのしどころは、先の委員が重視されている点もちろん重要であるが、安全保障は大きく分けて二つで考えなければならないことを言っているところである。必ずしも一般でイメージされる安全保障にそんなにウェイトを置かなくても、他のところも重要だということが“売り”であると思う。これは前回もかなり議論になったところであるが、「サイバー空間」と「政府機関、重要インフラ」で分けて書いているのは、そのアピールでもある。東京大学の勉強会で、セキュリティについて議論する機会があったが、その時、狭義のガバナンス空間とは違う空間が発生しつつあり、成熟・ジェネレートされて来たという認識は持つ必要があるということ議論した。その意味では、ここではこの考え方を意識的に打ち出しているということアピールするのかとは思ふ。では、ガバナンスのあり方をどのようにするのかということについて、規制・法規も重要なところは重要であり、考えなくてはならなくなると思うが、皆が主体的に気付いて自らガバナンスの能力を上げる、自分たちで作ろうということ訴えていくのだと思う。その辺がアピールのしどころではないかと思われる。
- 「(ウ) 安全保障」を分けるなどしなければならぬと思う。最近はずいぶん、サイバーテロの危険性の方が昔よりずっと高まっていると思っている。それに対して、本格的に検討するなり、対策を考えていくところがきちんとあるか。それを NISC がやるのが一つの方法ではある。軍だとか政府機関では、NIST のようなものがない。経済だとか個人だとか言っているが、

対策を立てられるかと言えば、立てられない。「(ウ) 安全保障」のところで、本気で本格的なことを考え、それを「(ア) 経済」及び「(イ) 国民生活」に普及させていくことを考えなければならない。例えば、一定の経済活動に対してサイバーテロが起きたとき、NISC と民間で考えろと言っても、これからはそんなに簡単には行かない。このことが「(ウ) 安全保障」の記述の中から余り感じられないという気はする。「(ウ) 安全保障」を分けるのなら分けて、さらに対策面において、国として金を使って対策を強化するといったことは明確に言わないといけない。第2章で取り上げる問題かどうかということはあるが。

- 重要な点であると思う。また、委員指摘のとおり、“位置づけ”でどう書くかの問題はある。そこは各論でかなり踏み込んで、今回の第1次提言では各論に入らないので、7月からの議論再開でかなり皆さんのご意見をいただいなければならぬ。そこでの主要論点になるとも思っている。
- 今のお話を伺って心配になってきたが、「(ウ) 安全保障」を2つに分けてたほうがよいように思えてきた。サイバー空間の安保の部分をよく読んでみると、国家の強制力が必ずしも存在しないサイバー空間と断定してしまっている。チャイルド・ポルノや迷惑メールだとか、いろいろなことを考えると、むしろ世界では、サイバー空間への国家の強制力というものを、ものによってはある程度しっかりやらなくてはならない、という議論が出てきているのが現状ではないか。それに対してセキュリティは、どこまで対応するかは別にして、ある程度対応しなければならなくなっている時代でもあるのかと考えると、書きぶりは本当にこれでいいのか疑問になってくる。犯罪の件が抜けており、防衛と外交と書いてあるが、チャイルド・ポルノとか有害情報とかのいろいろなことを考えると、そういった側面も出てきているので、その点を考慮に入れた修文をしないと、後で軌道修正がいかなくなるという危険性はないのかと心配する。
- 私自身の素直な感覚では、今の順番が一番よい。安全保障は自分の生活や仕事と距離があるせいか、今一つピンとこない。話を聞いて「そういう危機もあるのかな」という程度である。
- 「経済」とだけ書くと経済学のような感じもするが、ここは「経済活動」「経済社会」の話であることを考えると、言葉を足した方がよい。国民生活のかかなりの部分は経済活動に拠っている。他の部分の記述を増強するのであれば、経済活動や経済社会が結局国民に影響するということも含め、経済のところもバランスをとり膨らませて記述願いたい。
- 「(ウ) 安全保障」の項の下に、「サイバー空間」と「政府機関、重要インフラ」ということがあるが、安全保障の概念について、私のイメージでは、万一の際にも守られなければならない部分が安全保障だと思っており、守られても守られなくても、どちらでもよいようなものは、安全保障には当たらないのではないかと思っていた。もしも開かれた安全保障ということで、責任をもたないベストプラクティスのようなことである程度頑張るとい程度であれば、国民生活や経済の項目の方で、ある程度割り切って適正な水準でやるという言い方になるだろう。安全保障でやるというのであれば、万一の際にも最低限守らなければならない

いレベルはあるので、それについては、もう少し国家、重要インフラ並みに扱い、そこを確保する対策をうつ必要があると言わなければ、何となく座りが悪いような気がする。文化の側面との関係についての記述で、これまでは暗黙の信頼で安心・安全が提供されたが、これからは契約によって明示された責任関係になるというようなことを言っているが、サイバースペースは、暗黙による安心・安全は得られないので、契約による責任関係の明確な世界にもっていくというのであれば、その契約の範囲内でしか責任をとれない。この点でも、安全保障という項目にあると座りがわるいのではと感じる。

- 順番等はこれでよいかと思う。若しくは、「(イ) 国民生活」が最初にあってもよい。安全保障の意見があったが、サイバーに対する安全保障は二つの考え方があって、一つは防衛、外交という部分があり、それとは独立に国民、官民がしなければならない部分がある。サイバー犯罪に関しては両者の観点は独立であり、両方とも必要であるが、今回の「第1次提言」で、主体にしたいのは官民の部分であるということに記載すべきである。現在の提言案は、防衛、外交のサイドからの安全に関して記載せずに、官民サイドの安全性の必要性だけが記載されているので、ぼやかした感じになっている気がする。二つの方向性が必要であるという記載のもと、官民がしなくてはならないことという形で分けて記載した方が、主張がぼけなくてよい。
- (ア) と (イ) の順番が変わった場合、先の話ではあるが、対策実施主体に関する部分も企業、個人、重要インフラ、政府機関・地方公共団体という順番になるのか。個人的には、今の順番が良いと思うが、もし替えるのであれば、他のところも替える必要があるのではないかと単純に感じた。
- 先ほど、国民生活を前面に出した方がよいと申し上げた理由であるが、IT 戦略本部でも経済財政諮問会議でも、国民視点というものが非常に重視されている。クライアントあるいはアウトカムのサイドから見て分かりやすいところから入る。まずは国民生活、生活環境のことから意識する。マクロで考えると、次は経済活動の関わりで生きていて、社会保障とか収入とか地域経済に関係し、そこへ広がっていく。安全保障は、ナショナルエコノミーの外の問題も含む。まずは、国民生活から入っていくという、そういう目線で意識した区分けである。文化はどこに入ればよいかということは、また考えなければならないが。
- 重要な問題として、安全保障の中身をこのような形で書いてよいか議論を始めると、中身のある議論が出てきている。その辺りをどう考えるか。
- 安全保障について政府が何をやるかは、書いていない。官民の連携、プライベート・パブリック・パートナーシップ (PPP) のことをメインに書いている。情報セキュリティ関係のところでも新しい話題として、安全保障のそこを変えてきたというところはある。従来の政府の中で国民の生命と財産保護などに関連して、サイバー面のところで何をすべきかということは、ある程度書けるとは思う。そこをまず、関係各省庁、特に警察庁・防衛省と相談しながら書いて、更に近年においてコンピュータを通じた社会活動の展開が広がり、その中で官民連携、今までとは違った開かれた安全保障というものがあるという二つの流れで書いていく。

そうすれば、より読めるのではないかと思う。

- 「(ウ)安全保障」の最終パラグラフにある重要インフラの話は、安全保障の問題ではなく、「経済活動」の話である。重要インフラをここに書くと、その直前までの国家機密対策のような内容から、いつのまにか金融機関もみんな政府の安全保障のためにやっているんだという展開になり、筋がおかしくなる。全体を見直す中で移植手術し、経済の記述を少し膨らませるとともに安全保障をスッキリまとめることが適当。
- 官民連携によって開かれた安全保障という新しい概念でいくということは、すなわち、安全保障は国が最初にやるということではなく、初めから官民連携で責任をもってやるというニュアンスになるのか。
  - ⇒ 議論になるところであるとは思いますが、現実として既に政策を行っているところで、国が 100%独占的に何らかの基盤を守るところは非常に限定されてきている。現実には、ある一定の法律や合意という形であったり、あるいはレギュレーションの中で官のディレクションと民による実装が現実に行われているのは事実であると思う。電力にしても、通信にしてもそれはある。その中でいかに上手く役割分担をしていくか、その役割分担が市場の開放性や透明性とどのように合わさって上手く動いていくか、日本も含めて各国で考えているところであると思う。政府が 100%頑張らなければならないところ、例えば防衛とか犯罪対策などは政府が 100%やっているところである。それに対して、更に官と民で役割分担を明確にもちながらでも国としての機能維持を意識してやっていくというところは、防災の観点でも、我々情報セキュリティの観点でも考えられており、その部分では官民連携は当然だと考えられているわけである。全部オープンあるいは官民連携だけでということではなく、当然両方あるということである。
- 「重要インフラ」のように第 1 次情報セキュリティ基本計画の中で定義されたものが、それに相当するような気がするが、それとは違う領域のものをここで新たに問題提起しようとしているのか。サイバー空間も重要インフラとして扱っていく。まさしく今おっしゃられたのは、重要インフラの考え方ではないかと思うが。
- 今の重要インフラの行動計画は、あくまで政府の側と民間の側で「手打ち」をした単なる 10 分野であって、これが絶対的な定義かといわれると、見直しを同時並行でやっている。「重要インフラ」の定義も国ごとに違う。我が国が入れていない分野で外国では入っている分野としては、例えば米国では教育機関やハイウェイがある。ここを重要インフラの 10 分野に限定しているのかと言われれば、そうは言わないと思う。ただ、開いていく、新たな領域を加えていくウィル (will) があるかといえば、事務局としては検討の最中であるというのが正式な答えであり、補佐官としてどう思っているのかについては、今考えていると言わせていただきたい。他の委員から出されている意見にもあったが、社会活動の部分にネットワークを使った活動が非常に広く入っており、これも広い意味で安全保障の基盤の一つになり始めている。その中、国ではなく民間が大きな役割を持ち始めているので、その部分での調整がある。この意見を組み込むとこのような書き方になったということで、御理解いただければ

と思う。

- ここに書かれていることに反対するわけではなく、現状がこうなっているのはそのとおりであるが、現状のままでは非常に脆弱な形であり、それを追認するだけではよろしくない。強固な対策をとっていく必要がある、というニュアンスを入れていただいた方がよい。先ほど、他の委員からも政府が果たす役割が書いていないという指摘があったが、何をやっていく必要があるのか、もう少し書いた方がよいと思う。
- 今の指摘は重要であるが、書くとなると各論の議論も綿密に踏まえないといけないと思う。昨日、首相に答申された携帯電話の保護に関するもののように、法規制で行うか、政府が全面的に乗り出すか、フィルタリングも含め民間の自主的な規制でやるのか、そういう問題が含まれてくるからである。このサイバー空間をどうジェネレートするかで官民の協力が必要だと書いてあるが、これは今までどおり規制が少ない分野で民間が自発的にやってよいのか。官民連携で政府ももっとやるべきだと言ったとき、政府は全面的に法規制で乗り出すと受け止められる可能性もある。その辺りは、我々の腰が定まっていない限り、書き方を相当注意しないと変なことになる。官民連携が重要ということくらいであれば、まだ問題はない。これ以上書くとなると、細部の議論をある程度した上で書かなければならないと思う。
- 順番については、(イ)の国民生活を先にもってくるということ、(ア)の経済をもっと拡充して、(ウ)の中から経済に関連するところを引き抜いてくるということは、やった方がよい。(エ)の文化についても、社会風土は削除し、文化ということで良いと思う。サイバー空間、政府機関、重要インフラについては、みなさんから重要な意見をいただいたところだが、サイバー空間のあり方、ガバナンスのあり方については、官民連携という今までどおりの記述を基本的に踏まえることとし、どうしても必要であれば意見をいただこうと思う。また、政府機関、重要インフラについても意見をいただいているが、どうしてもというところがあれば、意見をいただきたい。
- 重要インフラの記述だけは前にもっていった方がよいと思う。政府については、後で出てくるのでここに書き込む必要はない。開かれた安全保障とは何なのか、という疑問は依然としてあるが、これはこれでよいかという気はする。
- 後ろの方であまり政府部分が出てこない感じがある。また、心配であるのは、政府のところにサイバー攻撃という言葉が全くない。政府に対するサイバー攻撃は一番要警戒であり、2行目のところに「サイバー攻撃等に対する事業継続性を…」などを入れておいた方がよいのではないか。
- サイバー攻撃については、記述を加えるということで進めたい。
- 「成熟した情報セキュリティ立国」とまで書くのであれば、先ほど国民を前に持ってくるという話があったが、国民が実際に使うときに安心・安全を感じて使用され、しかも本当に安心・安全でなければならない。今の延長であれば、安心・安全を感じる状態では全くない。安心・安全を感じられない理由をいろいろ考えていくと、日本はもともと安心・安全な国であるということと同じ治安状況をネットの中では感じられないからである。その大もととな

る法整備、法はフィルタリングをするといった法ではなく、悪い人がいれば捕まるという法律、それが治安であると思う。犯罪取締りに関して、情報漏えいがネットにつながりでの不安だと思うが、情報を持ち出した者を処罰する法というのではない。Winny やそれに感染するウィルスの作成又は配布についての取締りに関しても、いろいろな議論があることは分かった上で言うが、できないとか言っていないで、議論をきちんと終え、きちんと法律を作り、それが世界各国の中で見てもなかなか合理的でいいものができていて、それを取り締まる機関もしっかりして初めて「成熟した情報セキュリティ立国」の一つになるのではないかと思う。

- 国がモニタリングしてフィルタリングに乗り出すといったことは極端な例であるが、今問題になっているのが、政府が乗り出していくと、一方で IT 産業の発展を妨げていくという議論である。治安が良いということと、当然それでも国民には自由があり、IT 産業も発展しているという、この三つのバランスが取れているのが「成熟した情報セキュリティ立国」だと思うので、その辺りのコンセプトを入れて欲しいと思った。
- 今の意見に賛成である。今回、法制度についてはあまり触れられていないことは残念であるが、各論のところでは踏み込んだ議論をすることになるのかと思う。その意味では、前提として大きく捉えておこうというのが、第 1 次提言であると理解したので発言はしなかったが、一言いれておいていただければと思う。
- 「その他」という見出しはよくないが、第 6 章のこれから各論で議論することの中には入ってはいる。しかし、第 2 章でも規範性の問題は入れておいた方がよい。  
⇒ 第 6 章の見出し「その他」については、「今後の検討が必要な課題について」と直すこととしたい
- 第 1 章とも関係するが、13 頁の第 2 段落で、「第 2 次基本計画では…」というところから「事故前提社会の構築及び合理性に裏付けられたアプローチの実現の観点に基づいて…」という部分の後に「1) 冷静で迅速な対応」、「2) 最適な水準の対策の効果的・効率的な実施と説明責任の明確化」とある。このうち、1) は後段のレスポンスやリカバリーにつながるかと理解するが、気になるのは、事故前提社会を考えたときに企業等でもそうだが、自分のところで何か基準をつくって、このレベルでリスクをハンドリングしながら対応を行う。事故が起こった場合、そこで会社、企業の中での運用が止まる。止まった段階から、一生懸命リカバリーやレスポンスをするが、これは当たり前のことである。「事故前提社会」という言葉を上手く使うのであれば、一つの考え方として、何かが起こったときにプリペアードネス (preparedness) という言葉が入っているが、上手い準備をしていたため被害が限定的であり、すぐに回復出来るといったような概念が欲しいかなという気がする。例えば、自分の一つの企業なり、一つのエンティティの中でハンドリングしていたら、知らない情報を外から事前に知ったので、その準備ができたので、その事故が起こりそうになっても非常に早いリカバリーができる、被害が大きくならなかつた。このことは連携とも繋がる。そういったメッセージが欲しい。1) 冷静で迅速な対応の中に含まれるかわからないが、そのようなメッセージが私には見えない。そういったレベル、レディネス (readiness) という言葉、プ

リペアードネス (preparedness) でもよいが、うまい準備をすることによってインパクトを最小限に抑え、早いリカバリを迅速にするといったようなニュアンスが入ると、一つの進んだ方向としてよいのではないかと思う。まずは、皆さんとイメージがあっているかどうかを伺いたい。

- 個人的な意見では、指摘の点は入れたほうがよいと思う。細部の議論を7月以降やる時も、また ITIL の議論等も考えると、どうやってショックの度合いを減らすか、事業継続性がどう繋がっていくか、IT 投資も全部絡んでくるので入れておいた方がよいと思う。  
⇒ どこに入れるかは相談に乗って欲しい
- 時間も限られているため、第2章はここまでとさせていただきたいが、どうしてもご意見があれば会議の後、事務局までいただきたい。例えば、IT ルネサンスという表現等について、意見・サジェスションがあればお願いしたい。

### (3) 「第3章 第2次情報セキュリティ基本計画下で実現すべき基本目標について」部分

- 「事故前提社会」という思想が頭の中に入り書かれているものだと思うが、17 頁の(c)に、「事前対応をやってもだめだから」というような否定的なことが書かれている。また、18 頁の(b)の第1段落にも、「完璧な事前防止が容易でないことにかんがみると…」と、これも否定的に書かれている。21 頁の(e)説明責任の明確化にも、「完璧な事前予防は容易に存在し得ず、」とあり、3箇所出てくる。あまりにも強調しすぎているのではないかと思っている。よい案は浮かばないが、これを例えば「事前対応は重要であるが」などのニュアンスに変えられないだろうか。「事故前提」があまりにも表に出すぎているという感じである。
- 22 頁の中央、②の第一段落の最後、「情報を預ける側の自身の情報に関する所有意識、オーナーシップ (ownership) を高めることも必要である。」との記述は、文脈の流れとしてはよいと思うが、この文だけを読んでしまうと個人情報の意識が強くなって、「私の情報はどうなっているのか」といったことをあおることにならないか。かえって対策がやりにくくなるのではないかということを感じた。
- 重要な点だと思う。事故前提社会を強調しすぎだということは、それぐらい言わないと誤解を招かれるということで、繰り返し言っているということもあると思うが、事前対応が役に立たないと意味するように受け止められるとおかしなことになるので、「やる必要はあるが、それでも不測の事態はあり得るのだ」という書きぶりをする必要があるということだと思う。それはしないといけないと思うので、対応させていただく。
- 所有意識、オーナーシップ (ownership) を「高める」というのは、イメージが違うのではないかと思っている。要は所有意識に基づいたというか、前に書かれている対策を実施する主体であるとか供給する側、それらにおいてもオーナーシップ (ownership) がどこにあるのかということのを考慮した対策が必要だということである。一つの意見だが、「高める」というのは少し違うのではないかと思う。
- 「高める」というのは、やはりおかしなので、対応させていただく。実は微妙な問題であ

るが、個人情報保護に関する意識、過剰反応が問題になってきている。国勢調査等でも弊害が出ているが、調査を拒否される方が増えている。あまりにもそれを意識して、結局、誤解が結構生じている。誤解を助長しない方がいいだろうと思うと同時に、ある程度個人情報を意識して、それを今度は他者に預けて、もっと自分の生活や福利厚生に役立つように使って欲しいというようなことも意識していただく必要があろうかと思う。その書きぶり、表現の仕方は考えて出した方がよいと思う。お二方の委員が述べられたように、この文章だけでは不足なので、書きぶりは考えた方がよい。委員に協力をお願いしたいと思う。

- 「所有」という言葉の意味であるが、法的には財産権に結びつくようなイメージを持ってしまう。情報の「保有」という方が、ニュートラルな言葉であるという気がする。
  - 「所有」という言葉は使わない方がよいとすると、その前の「対策を実施する側（情報を保有する側）」とあるが、そことの関係ではどう表現するのがよいか。
  - 考えることとしたい。
  - 書きぶりについては、協力をお願いする。
  - 見ていて気になったところとして、18 頁に「情報セキュリティのリスクを的確に評価（アセスメント）」だとか、19 頁にも「投資効率を把握する」だとか、いわゆる水準を認識するという話が出てきている。もう少しまとめてやらなければ、まだ情報セキュリティのリスク評価をきちっとできるような話は聞いたことがない。それを数式を使って、投資効率を測ると言われても、かなりしんどいと感じる。少なくとも数式活用で科学的な手法で投資効率を明らかにするということは、IT 投資そのものでもうまくできていないので、情報セキュリティはいわんやという感じがする。気持ちはわかるが、書きぶりを少し変える必要がある。全体に水準であるとか、アセスであるとか、レベルだとかいう言葉が出てくるが、少しこれをまとめるような方向でやらなければならない。NISC でまとまるのかということはあるが、どこかで一つルールをつくらないと、皆が勝手に、ばらばらにやってもなかなか上手くいかないということがある。現実には、ヨーロッパ辺りのムーブメントだと、そういうもの自体を ISO 化する、国際ルール化するという動きがあるので、そういったものをきちんと取り込んでいかないと、日本が勝手にやってもまた世界的には孤児になる。そういったことを踏まえ、書き方には工夫がいるのではないかという感じがする。
- ⇒ 委員指摘のとおりであり、個別の施策のところでは何を書くか、もう少しきちんと情報収集と解析が行われた結果が集約できる機能が政府内にあるべきであるということは考えている。どこへ書くかは別であるが、そこへ繋がるような流れが書ければよいという下心で散りばめていたのは事実なので、もう少し書きたい。
- 指摘のとおりであり、定量分析手法であるとか、ISO 化の流れであるとか、ITIL の基準などは影響力が出てきていると思うが、その辺をフォローアップした上で、できるだけ客観的なものは追及するけれども、それでもまだ限界はあるという現状があると思うので、それらを踏まえた形の書きぶりには、ある程度しておく必要がある。各論では、かなり突っ込んで議論をする必要はあると思う。

- 先ほど「事故前提社会」の議論では、「リスク」という言葉は定義不明瞭だから使わないという話があったが、ここには「リスク」が数多く出て来ている。先ほどとは事情が異なり、どこかで定義が明確なので使ってもよいのか、確認したい。
- 一般的によく使われているリスクマネジメントの「リスク」という意味で議論しているということであったと思う。リスクについての議論の中で発言があった委員は、どのようなニュアンスで使っていたか、自分の意見で結構なので表明していただきたい。
- 先ほど、「リスク」という言葉はちょっと…ということを出したが、タイトルとして「リスク」はやめたいということである。本文で説明していく中では、「リスク」という言葉は理解していただけたと思う。その意味で問題はないだろう。
- セキュリティに関しては、事故前提である、完璧性がないということを前提に考えるわけであり、そういうことに対してマネジメントしなければならない手法が、リスクマネジメントの手法である。それと極めて関係が深いわけであるから、リスクとか、リスクコントロールとか、リスクマネジメントという文言を多用しても、あまり違和感はない。それよりも、リスクマネジメントの概念があまり共有化されていないということが心配である。リスクがあるから予見をする、予防する、損害や障害を極力小さくするための方法を決めておく、そのためにはいくつかの手段があるなどの共通認識がないと、うまく「リスク」が理解されないと思う。どこかでリスクマネジメントをわかりやすく、いわゆる完璧性がないものに対してのマネジメント手法としてのリスクマネジメントの手段が解説されていた方がよいと思う。
- それは必要であると思う。こういう意味で使っているということを本文で書くべきだと思うが、長くなるのであれば、注をつけるということでもよいと思う。
- 私は注でいいと思う。
- 昨日、柔道の谷亮子選手へのインタビューを見たが、練習は二、三百通りの方法を持っていると言っていた。「役に立たないものも出てくるのでは？」との質問に、「もちろん出てくるが、三百通りの練習をしていけば、確率は極めて低くても試合中にそういうことに遭遇することがあり、それですぐ対応することができる」という趣旨のことを言っていた。これはリスクマネジメントであり、「もしやっていなければ負けるだろう」というニュアンスであった。経済学で「リスク」を使わないというのは、全く想定できない、対応不能なものは「リスク」とは言わず「不確実性」というように言うからであり、「不確実性」という言葉は、いま言ったような意味での使い方になる。ただし、リスクマネジメントの「リスク」は、もう少し“未知との遭遇”のようなものも含まれていると思うので、その辺りは定義して使う必要があると思う。
- 根本論のお話になると思うが、可能であれば是非、リスクへの対応ということを少し書いて欲しい。軽減する、回避する、移転する、受容するの4点である。そこで感じるのは、受容がほとんど見られない。「事故前提社会」は、無謬性が受容性を全く許容しないということだと思っており、そこからの脱皮だと思う。ある意味、全部を受容するというのではなく、一定程度の受容はしなければならない。その意味でも、リスクへの対応は少し書いておいて

欲しい。

- 先ほど ISO の話が出たので簡単に補足すると、ISO27004 というのが、ISMS がいかに上手くいっているかを測定するメジャーメントのモデルである。ISO27005 は、既に国際標準になっているが、インフォメーション・セキュリティ・リスクマネジメントである。委員がおっしゃったように、リスクにはリスクを算定したり、見積もったりして、最後にそれに対するトリートメントというリスクへの対応がある。そこにいくつかのパターンがあり、このリスクはいいかと思うのと、このリスクを自分できちんとレスポンスしようというのと、ひょっとしたらこのリスクは別のところへ移してしまえといったものはいくつかある。フレームワークは参考になるが、そこで言っているリスクマネジメントは本当に雛形しか書いていないので、ここの議論ではあまり参考にならない。ここのどこか、アネックス (Annex) やアペンディックス (Appendix) でよいが、今議論されている皆さんの中でのリスクマネジメントを共有するため、3 頁程度説明があった方がよいと思う。提言の中にあるのは変なので、どこかのステージで、もう少し具現化したときにあった方がよいと思う。次の具体的な議論をするときに、情報共有のためのペーパーでもよいので、なにかあった方がよいと思う。準備するのであれば、サポートはさせていただく。
- よろしくお願ひしたい。
- 前に CIO 会議に出て e-ガバメントの説明をしているとき、審議官が「官房長は先生の説明を全然わかっていません、まず、専門用語が全然わかっていません」とおっしゃっていた。その後、官房長に付いている課長補佐級で用語辞典を作ってくださいとお願ひした。用語辞典は必要である。どうしても立場上、わからないとは言えないと思う。
- 前から気になっていた言葉で、どこかに定義が明確にあればよいが、20 頁の(C)に「最適な水準」とあるが、「水準」という言葉は他にもたくさん出てくる。リスクの水準ではなく、最適な水準のセキュリティを確保するというような使い方をされている。よくリスクマネジメントの本や規格では、セキュリティレベルという言い方をする。ここでセキュリティレベルというのは案外スペシフィック (specific) なので、水準という意味で少しぼやかした又は広めに書かれているのかという気がした。何か定義などが必要なのかと思うが、いかがか。
- 私は、恐らくぼやかしているのかと思っていた。特に今回の時点では、このくらいで良いのではないかと思う。もちろん、各論の中では議論しなければならない。
- 同意見である。情報セキュリティ対策に関する投資効率の把握に関してであるが、これは難しいという先の委員の意見に同感である。こういったことをやりたいという気持ちがあり、やるとするにしても、ただこの章に出てくることなのかという気はする。今後具体的な対策を考えていく中で、できるなら書き込んでいいのではないかと思う。例えば、「数式を活用するなど…」とわりと具体的などころまで書こうとされているので、自縄自縛に陥って出口がなくなってしまうのではないか。次からの検討のときから、出口を考えてここは書いた方がよいかと思う。既にあれば別であるが。
- 後で詳細に検討すればよいので、その言葉は外して幅広に押さえておけばよい。要は「ロ

「ジカルにきちんと考えましょう」ということが言えればよい。

- 21 頁の一番下の部分、「対策を着実に実施するとともに、説明責任も十分に果たしている者の方が、対策を十分に実施していなかったり、説明責任を果たしていなかったりする者よりも批判を受けるような場合も想定されることから、このような事態が生じないような検討も重要である。」は、ここにあるべきなのか。入れる必要があるのか、何故あるのかがよく分からない。もし必要であれば、「きちんと説明をするように」であるとか「すべきである」と書くのが良いと思うが、敢えて入れている理由がわからない。
- ここにあるのがよいかは分からないが、これも場所の問題であると思う。いろいろな情報セキュリティの事件の現場に立ち会ってきた経験から言わせていただくと、記録も何もっていない、対策も何もしてなくて情報を持って行かれた場合に、持って行かれたという記録すらないので「漏洩した事実はございません」という公式発表になる。ログもきちんと取って、対策もやって、記録している人は「何件漏れました」という発表になる。その点はアンフェアであるということもいつも思っている。「全部持って行かれている」と思っても、「持って行かれてたと思います」とは言わずに、「持って行かれた記録はございません」となり、「ああ、漏れてないのか」と皆が思ってしまう。このようなことが続いており、きっとこれからも続くので、「どこかに入れられませんか」と申し上げたところ、ここに入ったというのが経緯である。
- 今の説明を聞かなければ分からなかった。長大な説明を要するが、長大な説明を要するほどの事態なのかというのはある。各論にするか、あるいは、全ての大前提としてしっかりとした対策をとり説明をするということは謳っているもので、そういう人たちは相当けしからん奴だという認識を共有するだけで終わってもよいのではないかとは思っている。
- 少し書き方が幼くて喧嘩を売ってるような感じになっているので、書き方をもう少し練れば、きちんと入るようになるかとは思っている。
- もう少し練って、表現を大人にして入れていくこととしたい。もし他に意見があれば、メール等で事務局にご意見いただければと思う。

#### (4) 「第4章 我が国が情報セキュリティ問題に取り組む上での政策の枠組みについて」部分

- 26 頁の「(4)横断的な情報セキュリティ基盤について」の2行目で、犯罪の取締りとあるが、取り締まるための法整備ができていないので、捕まえることができない。法整備を前提とした、あるいは法整備を含む犯罪の取締りがきちんとできる、という言葉が一言あればよい。

⇒ ここは第1次情報セキュリティ基本計画を受けた説明であるので、ここに法整備について書くとおかしくなる。いろんな観点はあるかと思うが、法整備はやはり法律をつくって、国会を通さなければならない。政府が国会のことを言うのは限界があるが、法整備のことについて書くのであれば、第6章の個別具体的な検討項目の中で書くか、もっと前の大括りのところで触れるかということはある。しかし、ここで触れると少しやり

にくいのではないかと考えている。

- (3)において、メディアに対して期待されるとあるが、大いに期待するし、それにより国民が影響を大きく受ける。報道の内容について、例えば情報漏えいであれば、件数が大きくなければ報じられない、「何件もれました。以上。」といったものではなく、「成熟した情報セキュリティ文化」というのであれば、もう少し突っ込んだ背景や、何がよくなかったのか、きちんと対策をしていたら漏れたのか、対策をせずに漏れたのかということに踏み込んだ充実した報道にしてもらえればと思う。これはここには書けないかもしれないが。
- 書いても良いと思うが、メディアといったとき、かなり限界がある。インターネットやITのことを詳しく知っている方が新聞から時事情報を得るとは思えない。一般の方ということでは、もっと厳しいことを書いても全く問題はないと思う。ただ、個人がメディアリテラシー、ITリテラシーを持っていないと、所詮は仕方ないのかとは思っている。メディアがいくら書いたとしても、分かりやすく書くのは難しいと日ごろ思っており、ここはハードルが高いのかなという気はしている。
- メディアをマスメディアとすると、マスメディアの報道によってITリテラシーが上がるという期待はあると思う。昔は取材されて、「サーバという言葉は絶対わかりません」と言われたり、言葉で説明できないような内容で情報セキュリティについて語れと言われたりということがあった。今ではサーバという言葉は新聞でも出てきたりする。マスメディアの報道の中で、少しずつでもITリテラシーを上げていく効果は期待できるので、そういうものがあればよいと思う。
  - ⇒ メディアについて、前向きな内容であれば書けるような気はする。委員長の了解があればではあるが。
- 25頁の様々な類型云々という記述があり、その中で「下請け事業者」という言葉があるのが気になりである。下請けは大変で苦勞しているというのは現実としてあるのだろうが、類型の中で下請けの存在を認めるのはどうだろうか。下請けというと、非常に過酷な環境で働いている事業者というイメージで世間の人にとられるが、こういう言葉をざっくりと使っているいいものか。他の業界であれば、協力会社と言い換えてみたり、関係事業者としてみたりということはあるようだ。IT業界は、その構造自体をいろいろ言う人がいる中で、これを政府がなんの迷いもなく認め、「しょうがない」だから「それにあったように事業をしましょう」と言っているものかどうか疑問だということ指摘だけさせていただきたい。
- 下請けという言葉は法律にもあるように、客観的事実は存在する。問題は、そこに価値観が言葉を使っているサイドにあるかどうかということである。下請事業者という表現に付随して過酷であると言うニュアンスは、大半はそうだと思うが、必ずしもないと思う。例えば、ベネトンであれば、下請け、元請け関係は簡単にひっくりかえる。日本型の従来の二重構造ということであれば格別、下請けという言葉自体には過酷というニュアンスがないと思われるので、ここでは使っても良いと思う。また、関係会社とか取引先とかいう言葉も併せて入れた方がいいのではないか。下請け企業・事業者というのは厳然としてあるわけであり、

これは入れた方がよいと思う。

- 26 頁の(3)で「情報供給主体」という言葉が使われており、22 頁では対策実施側と情報供給側の双方からの検討という言葉がある。「情報供給」は耳慣れない言葉であったので事前にお伝えし、22 頁に「潜在的にそうなり得る者も実際に情報を預けている者も双方を含む。結果、全ての主体が情報供給主体となり得る」と注を付けていただき、表現されている。そして26 頁の「情報供給主体」というのが出てくるわけであるが、情報というとき、特に個人情報でよく使われたのが「提供」という言葉で、「提供」と「管理」という言葉が耳慣れている。「供給」というと「需要と供給」のようなことを経済の方からつい考えてしまうが、「供給」で違和感があるのは私だけなのか。「供給」という言葉で一般的な理解が得られるのか、他の委員の意見を伺いたい。
- 何気なく提供する人も供給主体に入ると考えると、「提供」の方が良いような気がする。
  - ⇒ 「供給」と「提供」については、国語辞典的な言い方で申し訳ないが、「提供」の方は相手の用に出すというイメージであり、「供給」の方は積極的なイメージで、相手との取引での必要性に応じて情報や物を出すというイメージである。積極的に情報を出す場合を意識したので、ここでは「供給」という言葉を使った。
  - ⇒ 個人情報保護の議論の中で「提供」と「管理」が対で使われるのであれば、ここは「供給」という言葉にこだわりたい。今回は情報を処理する、加工する業に対して情報を出すことについて「供給」という形で呼んでおり、個人情報保護の議論の中での「提供」がこれと同じで捉えられるのであれば置き換えてもよいが、今言ったような、より強い委託などのイメージと違うところがあれば、「提供」という言葉と「供給」という言葉を使うところは注意したい。まずは個人情報保護の議論での意味と同じかどうかを確認させて欲しいということである。もし同じであり、「提供」と「管理」が広く使われているのであれば合わせればよい。もし違うのであれば、「供給」という形で、供給主体とは何かを定義した上で使っていけばよいと思う。
- 注の方で預けるという言葉が使われており、全ての主体が情報供給主体となり得るとある。「預ける」という意識が大切なのであれば、個人情報にまさに預かっている、管理に関して預かっているからという議論をしていたので、ここをどう区別して読んでいいか分からなかった。個人情報の場合、必ず“個人”情報ということで、情報だけが一人歩きすることはなかったなので、どういうふうに照らし合わせればよいかはわからない。
  - ⇒ この言葉の使い方については、個人情報保護法での使い方を確認した上で、事務局で判断させていただければと思う。
- 先ほどメディアの話があったが、メディアも情報供給主体あるいは情報提供主体という位置づけになるのか。
  - ⇒ 一般論でのメディアが社会に対して発信するという部分は、供給主体のコンテキストでは読まない。

## (5) 「第5章 第2次情報セキュリティ基本計画の下での政策推進について」部分

- 27 頁から 28 頁にかけて記載されている、政府機関における技術的な知見及び人材の蓄積の不足と政府機関には様々な機能が必要であると強調されていることについては、全く書かれているとおりでと思う。18 頁の(イ)の(a)で変化し続ける脅威の把握とリスクへの柔軟な対応ということが書かれているが、変化し続けるリスクを継続的に誰かがフォローし、蓄積・最新化していくことが必要だということを強調した方が、より必要性が高まると思うので、可能であれば入れていただきたい。
- 27 頁の第2段落の、「アウトソーシングの活用といった対策についての検討も必要である」との記述は、基本的には、政府機関等で「アウトソーシングし過ぎている」反省の方が大きい状況を見ると、表現が単純過ぎる。例えば「専門分野における」と入れるか、「アウトソーシングのより選択的な活用」、「戦略的な活用」という文言に変えた方がよい。
- 28 頁の記述中、「我が国全体を視野に入れながら」の部分と、「政府機関も含めた公的役割を担った機関全体として」の機関全体の「全体」については、分かりにくいのではないかと。  
⇒ 書き直させていただきたい。
- 人事ローテーションの話について、「2～3年を基本としており、…問題もみられている」という表現は弱い。「2～3年では話にならない」、「これを抜本的に変えよう」という感じに強められないか。人事の基本が今のままであれば、いくら専門家を連れてきても、結局、その専門家に良いようにされるだけである。いろいろと難しい問題はあるだろうが、考え直す価値がある。ちなみに金融界の場合、私は28年間働いて25年間IT関係の仕事に従事している。金融機関では、システム部署に20～30年選手は当たり前で、全ての職員が2～3年で異動してしまう組織運営は、ITガバナンス上有り得ない世界である。
- ここの記述については、今の意見を踏まえ、もう少し踏み込みたい。文面については、協力していただきたい。再検討し、今言った趣旨で書き直したい。
- 20年選手、30年選手が当たり前という話は、全くそのとおりである。ただし、政府機関のインソースで人事ローテーションを止めればいいのかといえ、そんなわけにはいかないもので、一言どこかで、民間の達人の活用などの言葉が入れば、連携の感じが出てよいのではないかと。
- 27 頁から 28 頁は政府機関のことを書いていると思うので、まさに人事のことは書いていただいてもよいと思う。また、一度議論になったことであるが、予算制度について、情報セキュリティの場合は初めから完全に計画してできるわけではなく、他方完全に自由に使ってよいというわけでもないので、柔軟な予算活用という話も、もしフッキングするのであれば、入れていただきたい。政府機関では人事の話と予算の話がボトルネックになっているのは確かであると思う。
- セキュリティ予算をとるためにも、やはり指標を作って出す必要がある。そのあたりの体制は、NISCがガイドラインを作って担うべきである。

## (6) 「第6章 その他」部分

- 29 頁の第二段落において、各論の検討における例示としてある程度細かいことが書かれているのだと思うが、監査に関する記述については、かなり各論的などところに触れられている気がする。何回も議論があったとおり、規範があって監査ということになるので、視点を加味する、基準化といった別のニュアンスでは書いてあるが、やや規範めいたことも監査の言葉の前に入れて強調した方がよいのではないか。また、政府機関に対して監査ということを書くのであれば、重要インフラについても規範や監査ということが、むしろ出てこなければならないと思う。さらに、監査に伴ってアドバイスを行う機能とあるが、どういうことを言っているのか。かなり各論過ぎることをいっているような気がするが、ここまで書いた方がよいのか伺いたい。

⇒ 監査に伴ってアドバイスを行なう機関については、政府機関のことを書いている。政府機関については、各省庁毎に事情が異なるため、そこに無理に介入することは困難である。そこで、「監査を自分たちで実施するべき」と言っている。次に「監査結果の開示はきちんと行うべき」と、「公開しろ」とすると議論を呼ぶので「開示しろ」としている。そして、開示したら放置するのではなく、「悪いところがあったら直す」、「アドバイスをきちんと聞く」という機能がないと動かないので、そういうことを踏まえ、書いている。細か過ぎるかもしれないが、ここは書かせて欲しい。

- 説明を聞き、かつ、背景を知っていれば理解できるが、わからない人はわからないと思う。
- 委員の指摘は、一般社会における監査との関係を心配してのことと思うが、ここは政府の監査についての記述であると思うので、政府ということを明確に出せば問題ないのではないか。また、アドバイスの件は、“監査に伴って”というのを外してはどうか。アドバイスはアドバイスとして必要なので、実際はそうするのだと思うが、監査に伴ってのアドバイスというのは、語句的に引っ掛かるというイメージがある。
- 委員の指摘は、監査という意味を厳密に捉えているからではないか。
- 例えば、改善に関するアドバイスといった言葉遣いが良いかもしれない。改善とすると、もともと悪いというのが前提になってしまうので、あまり良くないかもしれないが。
- 監査は政府機関についてであり、重要インフラで監査がないのはどうなのかという点についてはどうか。

⇒ それに関しては、検討項目としてここに並べる。委員の意見については、基本的に第 6 章に入れる。検討すること自体は良いことなので、入れて良いのではないかと思う。

- 「官庁は王国連邦化しており、各王国（省庁）が自分で監査を受ける仕組みがやっと」との話があったが、共通の機関が横並びで監査を行えば、他の機関を見てきた目で比べるので、仮に基準ははっきりしなくても、誰がどの位できているか比較し易い。「自分で監査しなさい」つまり各省庁が独自に監査法人を選びバラバラの要件で契約・実施し、出てきた通知表を横に並べても比べられない。現行の方式では目線や基準が揃わず、自己点検と殆ど変わらない怖れがある。何かしらの統一的な監査実施が必要だということろまで、議論なり検討はする価値がある。

- 例えば、金融界の場合、金融庁や日銀の検査・考査なども通じて、業界全体としての目線、具体的にはFISCを含めたガイドラインや基準、日銀のサウンドプラクティスペーパー(Sound Practice Paper)論文が蓄積されている。日銀が、障害原因と対応の一覧や、新型インフルエンザを含めた対応策等を公表できるのは、いろいろな金融機関を見ているからである。政府機関でそうした監査を実施する機関がNISCなのかは分からないが、第2次基本計画の段階では、そこにステップアップしないと、実効性の確保が厳しいと思う。
- いろいろな機関が別々のことをやっている、別々の基準なりレベルに沿って監査をやるのではなく、ある一定のクライテリアに基づいてやった方が良いという意見に賛成である。ただ、個別に監査をやることは意味が乏しいのではないかと指摘については、助言型監査や保証型監査というのがあることを考慮すると、それなりに意義はあると思う。
- 「各府省庁の対策の監査にあたる機能(PDCAサイクルの点検段階)」という記述があるが、書き方が若干気になる。PDCAサイクルの点検段階ということで監査を行うと、プランに対してプランどおりやっているかどうかということになる。そもそも、絶対的な水準として最低限守らなければならない水準等があり、そのプランそのものに対する妥当性を評価しなければならないという観点で監査を行われればよいが、PDCAで各省庁が作ったプランに基づいて評価しても、実のある結果になりにくいのではないかと。「(PDCAサイクルの点検段階)」という記述は除いた方がわかりやすいのではないかと。
- 微妙であるとは思いますが、プラン・ドゥ・チェック・アクション(Plan・Do・Check・Action)のサイクルというのは、イメージした方が良いと思う。そのときに相手のプランがあり、その遂行状況や達成状況をチェックするだけではあまり意味がなく、改善案を言えるチェックが重要である。独自の基準もあるが、大局的にみたと、もっとうこういった点を満たさないと、世界的な基準は満たしてないのではないかと、ということを行わなければならない。そういう意味を含めるべきだと思う。狭義のPDCAではなく、政府の場合はもっと大きな意味で良いということも、言っておいた方が良いと思う。

⇒ 第1次情報セキュリティ基本計画の中で各省庁がやらなければならないことは、政府機関統一基準をつかってやっている。政府機関統一基準では、最低限やらなければならないことは決めている。また、最低限のことについては、各省庁が主体的に考え、自分たちの業務特性を考慮して計画を立てるとしている。役所の場合、計画はみんな頑張るが、その後の実施の確認が不十分であるので、政府機関統一基準の強い問題意識は、PDCAサイクルを作らせることである。その意味で、我々としてはPDCAサイクルができているか、できているとしたら状況はどうであるかということを通一基準の実施の中でやっているという意識である。更に踏み込んで行かなければならないというところが、監査という書き方になっている。希望として、PDCAサイクルの点検段階ということは、第1次情報セキュリティ基本計画からの継続性を考えた上で外したくない。言い方がまずいのであれば、言葉を足して書くことを検討したい。第1次情報セキュリティ基本計画ではここまで要求していたが、第2次情報セキュリティ基本計画ではここまでになるための

検討を必要とする、と書こうかと思っている。

- 言葉を少し補った方が、初めて読むものにもわかりやすいと思う。
- 全体の枠組中、第6章「その他」というのは、仮置きで「その他」ということか。今の文脈からしても、タイトルは「情報セキュリティの実効性の確保に向けて」というようなことではないか。
  - ⇒ 先ほども申し上げたように、タイトルは修正する。「今後の検討が必要な課題について」と直すこととしたい。
- 第6章は、実効性の確保のような章にしていただくと、しっかりした表現が出てくるのではないかと思う。言葉のことを申し上げると、「それは直します」ということになるので、あまり申し上げたくはないが、全体的なバランスを見たとき、第3章の計画のところまではしっかりした感じであるが、第4章～第6章は、非常に大事であり施策を遂行する人たちに伝えたいメッセージがたくさんあると思われるにも関わらず、分量的に少ない。第4章は全部「検討が必要である」と結んであり、これが第6章の検討を進めることにつながってくるのだと思うが、もう少し読みやすいとよいのではないかと正直なところ感じる。例えば第4章は、もう少し具体的に書ける部分は書いた方が、読む人の理解の助けになるのではないかと思っている。検討するという気持ちは非常に伝わるが、もう少し具体的に言わないとわからないこともあるのではないかと感じた。
- 第4章及び第5章は確かに指摘のとおりであるが、これはまだ第1次提言であり、まず基本方針を世に問うてみるということだと思う。それを踏まえて各論の議論を7月から再開することになるが、それとの関係で今後ボリュームが増えてくると思われる。その時点で議論してほしい。今回はまず、基本的な方向性を示すということを明らかにしたい。
- リスクのところでは柔軟な対応ということに言及されているが、行政評価などの例を見ると、計画をつくる段階で各省庁は柔軟性に乏しい計画を策定しており、評価段階では、最初に決めたことに対する事項にしか自己評価を出していない。そもそも評価する目的は、変化する社会に対して柔軟かつ機動的に対応できるのかということの評価するためであり、これが大変重要である。そこで、情報セキュリティについて、社会の変化や技術の進歩に合わせて柔軟かつ機動的に対応し実効性を上げる、ということは是非書き込んでいただきたい。
- 重要な点だと思うので、是非書き込みたい。硬直したもののほど意味のないものはないので、ニーズ、社会の変化に対応するというをかなり意識的に書いた方がよい。評価のシステムは、それを踏まえた上でやるのであろうと思う。5章(3)で書くということで進めたい。
- 29頁第四段落目には、今後考えられる施策が網羅的に書かれているのだと思うが、ここに「企業等のセキュリティ対策に対する援助策の検討」というのを是非入れておいていただきたい。企業の施策の中で議論があったと思うが、対策コストとならないようにする施策の一環であり、企業の積極的な対策を推奨するものになると思われるので、是非入れていただきたい。
- 第6章(1)の最初の段落について、「委員会としては」「中心に検討を進めることとすること

になる」というところは問題ないが、その前に掛かっている部分は違うものが並んでいる。最初から3つまでは主体に関することを言っており、4番目は基盤などの個別施策、具体的な対象物と違うものが並んでいるので、言い方の工夫をする必要があると思う。

⇒ 適宜読みやすくはするが、意味的には、それぞれの主体での個別施策ということである。

- 第6章の第四段落で、「人材育成・確保に関して」という文言を受けて、「高齢者」が入っている。確かに、これからは高齢者が多くなるので、人材育成・確保に資するかと思わなくもないが、少し整理をする必要があるのではないかと。

⇒ 第6章の書き方については、必要に応じ各委員にお手伝いいただくことを認めていただければ、言葉を足す作業をやりたいとは考えている。

- 30頁で「情報システムに係る事故があった場合の調査や評価」とあるが、これは政府の重要システムのことを言っているのか、民間を含めあらゆるものを言っているのか。

⇒ 日本学術会議が「情報システム調査委員会の実現に向けて」という提言を6月はじめに出すとのことであり、その内容を見た後、この部分の表現をどうするか考えたいと思っている。

- 気になったことが二点ある。一点目は、「情報システムに係る事故があった場合の調査や評価」については、前の部分で全く記述がなく唐突に出てきたという感じであるということ。二点目は、「情報システムに係る事故があった場合」とあるが、もう少し広い意味でセキュリティの事故であるとか、人間系、運用系のものもあると思われるので、情報システムに係るということで限定してしまってよいものかということである。

⇒ 許されるならば、先ほどの学術会議の提言をみてから、事務局において検討し、相談させていただきたいというのが正直なところである。ここの表現を含め、前後のどこで立てていくかを考えたい。この点は、重要インフラの行動計画にも影響が出てくる可能性があるため、いまのところは変にアンバランスであり、唐突ではあるが、留保とさせていただけないか。

- 29頁最後の段落で、「暗号方式や認証基盤などの先進性が重要な分野に係る国策としての取組みの要否の検討や、…」とあるが、他の検討項目と比べ、ここだけ“要否”と書いてあり、迷いがうかがわれる。この“要否”は取れないか。

⇒ 相談させていただきたい。

- 29頁の最終行で「情報セキュリティとの関係での情報の法的な評価方法」とあるが、この部分がよく分からない。法整備が立ち遅れているということで、法整備に関し29頁最後から三行目の「犯罪の取締り」の前後に入れればよいのではないかと。

⇒ この部分は、他の委員から発言のあった事項であるが、情報には財産的価値やプライバシーなど様々な性格があり、それぞれの情報の法的な位置付け、保護法益についてよく検討し、必要であれば制度化を図る、という趣旨で言われているのだと思う。

- 先ほど、サイバーテロのお話があったが、サイバーテロについてあまり真剣にやりましょ

うと言うつもりはない。ただ、どういうことが起り得るのか、どんな手口で、どんな技術で起り得るのか、そもそもどこが狙われるのか、それは個人のパソコンかもしれないし、原子力発電所かもしれない、それは分からないが、それについて真面目に粛々と考えるところがあればよいと思う。情報セキュリティはよく“いたちごっこ”と言われるが、サイバーテロには“いたちごっこ”は許されないので、必ず先回りをしなければならないというコンセプトの下、たくさんの方は不要だが、よく考え時々訓練などをやるという内容があればよいと思う。

- 国際標準に対するイニシアティブをきちんと取っていかなければならない、という議論が過去にあったと思うので、それについても、どこでもよいので書き込みがあるとよいと思う。  
⇒ 国際標準については、別途記述している。
- 29 頁の最終段落の技術戦略の推進に関して。15 頁のところでは IT 戦略及び技術戦略についてはもっと書き込むべきである、という委員の意見があったが、15 頁のところではなく、安全保障の観点から見ても技術戦略は重要であるということを書き、ここにつながってくるということにしていただけでないか。  
⇒ 書かせていただきたい。情報セキュリティ政策会議の構成員からも、技術的な面でのきちんとした役割を持つと言われている。
- 29 頁の最後の段落で、「暗号方式や認証基盤などの先進性が重要な分野に係る国策としての取組みの要否の検討や、…」とあるが、先進性が重要なのではなく国産であることが重要だと思うので、「国産でかつ先進性が重要な」のように、「国産」という表現を入れた方がよいのではないか。
- 「国産」という表現は、あった方がよいのかもしれないが、必ずしもそうとは言えない。また、「国産」という表現を入れることは、微妙な問題も含まれるので、今回は「先進性」だけとさせていただきたい。
- 今日、様々な意見をいただいた。これでかなり良い記述になると思う。どうしても気になる点があれば、今週中、できれば明日までに連絡して欲しい。今日いただいた意見でかなりよくなったと思うので、更にということであればお願いしたい。

## (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 －