資料２

情報セキュリティ政策会議　基本計画検討委員会
第６回会合議事要旨

１．日　時

平成 20 年５月 13 日（火）　17 時 00 分～20 時 30 分

２．場　所

経済産業省本館２階　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
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
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　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

(1) 「目標」部分に関する検討論点について

○ （「目標」とういことであるが、先に議論した「理念・哲学」部分に関連して。）「国家の根幹に関わる行政活動を行う機関や、公共的側面の強い重要インフラにおいても、業務におけるITの利用が所与となっていることから、」とあり、その後には「サイバー空間の安全保障は、軍事や外交といった国家機能的側面が中心になって実現されるというよりも、むしろ、官民様々な主体の自発的・協調的な参加によって実現される開かれた安全保障である。」とある。しかし、国家の根幹に関わる行政活動の部分まで、有事のときに機能できるか分からない状況では困るのではないか。その部分については、独立性を担保する、他に依存しなくともITによる業務処理ができる、という配慮は最低限考えていく必要がある。

○ 重要な指摘であり、同意。他の委員より意見が出されているが、クライテリアというか、切り分けの境界をどう考えるか重要であろうと考える。アカウンタビリティがある形で、ここは独自で動いていい部分、ここは拡大解釈への疑問が生じかねない部分、ということをどう考えるかということと思われる。

○ 根幹に関わる部分では、自分自身で独立的な通信手段、コミュニケーション手段を確保する必要があるのではないか。他方、根幹的でない部分は、非常に抽象的な言い方だが、割り切りがあってもいいのではないかと考える。

○ 防衛省の通信インフラについては、専用施設の整備だけでなく、民間企業からの回線借上等を組み合わせている。委員御指摘の点は、「自衛隊が支障なく行動できるか」ということだと受け止める。一つの切り口として、そのような通信インフラ構築に関心がある。

○ 文言について、「軍事」よりは「防衛」、”Military”より”Defense”の方がよろしいのではないか。

○ 電話の世界では伝統があり、通信網全体が機能しなくなったとしても、防衛関係・警察関係などの行政の主要機関については優先制御する機能が作られていた。インターネット利用の場合には、一般的に優先制御は具備されておらず、具体的な問題としては課題になってくる。

○ 専用線については、NTT グループとの協議により、政府の重要システムについては優先制御されている。インターネットでは御承知のとおり、優先制御は困難ということもあり、御指摘の課題はある。

○ IT障害における事業継続性については、政府も含め重要インフラでは十分意識されているところである。御指摘のインターネット・サイバー空間がいかに安全につかわれるかということについては、ISP 等の通信事業者が担っている部分でもあり、必ずしも政府だけでなく様々な主体が関与している。誰か一人では対策できないということで、「官民様々な主体の自発的・協調的な参加によって実現される開かれた安全保障」という表現をしている。

○ 航空管制は完全な専用線なのか。

○ 国土交通省の所管する事項であるが、例えば所沢の東京航空交通管制部と各空港の間は専用線ときいている。

○　安全保障というのは国家レベルの話であるため、この用語は「機微な情報を扱ったり、国家の根幹に関わる…」というパラグラフで使用した方が、読み違えが無いのではないか。第二パラグラフでの「官民様々な主体の自発的・強調的な…開かれた安全保障」といった文脈での使用は、先の委員意見にあった、国家の根幹に関わる行政活動の独立性の担保、他に依存しない活動の確保への懸念がある。

○　「官民様々な主体の自発的・強調的な参加」とあるが、「参加」という弱いものでよいのか。インターネットのコスト負担やこれまでの理念に関する議論などを踏まえると、「責任」という表現がよいのではないか。総務省でインターネットは誰のものかについての議論も行っているので、今後揉まれるところではあるが、主体には若干「責任」があるのではないか。コスト負担や復旧等、各主体にセキュリティ対策を行ってくださいという場合には、「責任」の方がよいのではないかという提案である。

○　第二パラグラフを見ると、「安全保障」という言葉を拡大解釈し、広義と狭義で使うことにより、必ずしも「国家」という強制力が存在しない時空間が広がっている、という認識を事務局は持っていると思う。

○　世間では、根幹に関わる行政の活動や情報セキュリティは重要であるということを否定していない。表現として「安全保障」というものが大前提としてあると、いろいろな議論が出てくるのではないか。趣旨は理解できるが、表現を工夫されてはどうかという提案である。

○　広く社会の安全という部分、社会に必要な事業の継続という部分まで含めて「安全保障」という言葉で表現しているため、混乱を招いた。事務局としては御指摘を踏まえ、広義の使用か狭義の使用かわかる形で整理させていただく。

○　概念の明確化、用語の使い方については手を入れるよう、お願いする。

○　「セキュリティ文化」というのは既に出てきている用語かもしれないが、「文化」という記述の意味合いが十分わからない。具体的には、「情報セキュリティもその取組みによって、我が国に「セキュリティ文化」を定着させようとしている。」という表現がよくわからない。また、「情報セキュリティは我が国の文化面においても影響力を有していると言える。」という表現についても、具体的なイメージがわかない。もう少し具体的というか、わかりやすい内容にしてはどうか。

○　「セキュリティ文化」について、第１次計画ではOECDの「Culture of Security」との関係で言及した。また、国家目標のレベルでは言及せず、実施部分の方針として、セキュリティ文化の考え方と、それを我が国でどう考えるのかという観点から記述している。

○　今回の記載は、先の委員会での委員御意見をふまえ、記載した。ITが社会に出て行くとき、社会的な文化形成を役割としてもっており、それが妙な方向に行かないようにする一方、過剰な規制もおかしいのではないかということも考慮している。他方、OECDでの「セキュリティ文化」という意味合いもあり、この２つは微妙に意味合いが異なっているため、きちんと分けて書くのがよいのではないかと考える。但し、この点について御発言された委員には、この内容で良いか確認できていないが。

○　この部分だけ「セキュリティ文化」であるが、「情報セキュリティ文化」と「情報」が入った方がよいのではないか。

→　OECD の「Culture of Security」の仮訳という意味では、「セキュリティ文化」という文言がよいと事務局では考えている。

○　原子力分野で「安全文化」という表現がよく使われるが、その他の分野での「文化」という表現は、そこから波及しているのではないかと認識している。英語の”Culture”という文言と日本語の「文化」という文言では、微妙に用法が異なっているが、「セキュリティ文化」の「文化」について、むしろ風土とか土壌、安全的な思想を生み出す土壌という意味であると自分は解釈している。「IT による文化創造」の「文化」と混同するので、文言を明らかに分けた方がよいのではないか。「情報セキュリティを高めるという作業を通じて、日本の中で「安全文化」、「セキュリティを重視する文化」を築いた方がよい」という文脈がよいのではないか。

○　「文化」の話も重要だが「文化分科会」でも作って議論していただくとして、本日の議事進行予定通りに「目標」部分の話に入りたい。ここでは、予て議論してきた「最低水準や基準の提示」を検討すべきかという論点を方向付けることに意味がある。今回の資料で、既存の様々なガイドライン・基準が例示され、金融分野ではここに書いてある他にも、金融庁や日銀が各種のガイドラインや論文を出している。これらを踏まえてさらにどのような基準が必要かを「基準必要派」の方に説明していただき、それに基づき議論を整理する方が、実践的に検討が前に進むだろう。

○　今回、いくつかの基準・ガイドラインを例示しているが、基準・ガイドラインは多々存在し、また、具体的な分野、業界によって異なっている。前回、委員の意見である「基準に関しての抽象的な議論は建設的ではない。」、「抽象的な基準の良し悪しより、対策実施主体ごとの状況に応じてきめ細やかに検討すべきではないかなどを決めればよいのではないか。」に関して、そのための例として出させていただいている。

○　ここで挙げられている例の多くは、ガイドラインとして示されており、監査等でも使われてはいるが、目安という位置づけのものであると思う。例示の中で規範性という記述があるが、ある程度強制力をもった法律や規則という形にしなければ規範性は実現できない。今回例示されたものをどのように扱うか、情報セキュリティの戦略の中でどのように使うのか、というコメントが目標の中に出てきていないように見受けられる。これらをどのような方向で検討するのかということがなければ、ぼんやりとした例示になってしまうのではないか。

○　規範性の議論については前回もあったが、現段階で抽象的に「規範性があるものを作るべき」「ガイドラインに留めるべき」という議論をしても、各論に落としたときに本当にできるか分からないので、今回の議論では避けたい。例えば米国の FISMA のような、ある種法制度的なものを考えるべきか否かも含めた議論はありうると考えている。

○　「理念」のところに関係して、文化について先ほど紹介された OECD の文化であるが、政治学・法学で議論されているものとパラレルなところがある。COE でソフトローの研究をやっ

ているが、このソフトローとは、法規ではなく規範、慣習、文化である。また、政治学の分野では、ハーバードのジョセフ・ナイが議論するソフトパワー、ハードパワーというものがある。ハードパワーは、軍事力・経済力であり、文化・規範で他国に影響力を及ぼすものがソフトパワーである。おそらく、OECD で意識しているのは、その議論を踏まえてのことと思われる。ここでの規範性の議論もこのソフトパワーの概念の議論と関係しており、どのレベルで規範を定義して捉えていくかということである。ハードな法を求めるという議論は、構成要件等様々あるため、フィックスしないと今の段階では議論が難しい。それをやるにしても、その前段階として、現状認識等を議論する必要があるということだと思う。

○　若干の補足であるが、先ほどのハード・ソフトの議論に加え、誰を対象とするかについて、例えば政府の情報セキュリティ対策について考えれば、法制化について書けなくはないと考える。しかし、一般論として、あまりぼんやりと書いてしまうと、よく分からないものになってしまう。事務局としては、ぼんやりとしたまま議論を進めることはリスクがあると考えており、他方、対象がスペシフィックに書けるのであれば、検討の項目として書き下すことはできると考えている。また、重要インフラについては、所管法との関係があるため難しいところがあるが、その他の部分については、きちんと議論できると考えている。

○　世の中全体について、抽象的に最低基準やマルチグレードの基準を作ることは難しいと考えている。したがって、例えば政府機関の対策について議論する部分で政府機関に関する基準の要否について、企業の対策について議論する部分で企業に関する基準の要否を議論をしていただければということである。この先も議論は行わないというわけではないことを補足させていただきたい。

○　主張ではなく一般的な意見として、世の中で ICT が様々な取組みの道具として使われるという大前提に立てば、各々の活動に対して一定の要件を定めた法律はあるはずなので、それを満たすことに使われる ICT の基準があるということは、当たり前のことと思われる。ICT が使われる分野で、「その目的を満たすようなものになっていなければならない」という当たり前のことは書けるのではないか。「その基準が何か」ということは個別に議論があるにしても、考え方として、政府なり業界なりのガイドラインがあってやっているということと同時に、全体の底上げというものを検討してもよいのではないかということは、書いてもよいのではないか。

○　最終的な結論へ向けた原点・アンカーポイントとして、法律から行くかという議論をしなければならない。法律というツール自身が特性をもっており、適用が難しい領域があるが、特に情報セキュリティや IT の分野において、実効性を担保していくことと法律というオーバーヘッドとのトレードオフの中で、どのようにやっていくかということがある。ハードパワーであるのかソフトパワーであるのとかいう議論もあり、現実問題としては、適用する主体ごとの特性との関係もある。この部分をどう書くのかということは、事務局としてもかなり逡巡しており、委員から御指摘のあった「当たり前」ということについては、議論が分かれるところであると考えている。これまでの３年くらいのオペレーションの中で、本当に法律

があれば行けるのかという疑問もある。法律があれば最終的にそこへ帰着できるが、所管法は別として、情報セキュリティに関する一般的な法律がない状態で、そもそも法律が必要であるという議論をここへ入れることができるかは、非常に難しいのではないか。

○　「目標」部分で経済活動・企業組織の分野がフォーカスされており、国民生活に関しての目標の書き込みがないように感じている。「理念・哲学」までは、網羅してバランスよく書かれているが、「目標」部分では経済活動のことが大半のように感じられる。情報セキュリティ・IT の推進において、そこでの弱者・取り残されていく人を理解し、どういうことを行っていくのかを考えた方が良いのではないか。

→　経済に偏っているということであれば、国民・生活のところで何か書けるか検討したい。

○　今回の「第１次提言」へ向けた重要な検討論点である、「情報供給主体」と「情報管理主体」のアプローチの必要性については意見を伺いたい。今後の全体に関わってくる論点である。

○　電子政府構想、電子私書箱の検討に携わっている者からすると、データベースがかなりの影響を持ってくるが、これのセキュリティの考え方をどうすればよいのかという論点がある。民間サービスでは、グーグル等が医療分野・健康管理分野へ進出し、e-health などを行っているが、国民生活全般、ディバイドの状況にある方々への影響力を行使したり、あるいはサービス自体を受けられないなどのことがある。また、知らない間に情報を取られたりという状況もある。この部分の認識を共有しておかなければ、同じ言葉を使いながらも異なったイメージで議論することになるのではないか。御意見と質問があればお願いしたい。

○　情報を預ける主体についての考え方について、定義が必要ではないか。先ほどの弱者の話を含め、そこへの配慮を行わなければ個人の保護等が見えてきにくいのではないか。そこまで言及する必要はないのか。

→　情報供給主体では、個人がまず念頭に置かれるが、企業に関しても他の企業に情報を預けるなどということが考えられる。すなわち、情報を預かる者、情報を預ける者の２つがあり、自分の情報は自己の基準で管理できるが、預けられた情報は預けた方の基準を考えなければならず、ある種の制約がある。個人情報は制約が強いものの一つである。ここでは、情報を預ける主体を念頭においた政策を考える必要があるのではないかという趣旨で書かせていただいている。

○　具体的に言えば、SNS やブログ等で知らないうちに個人情報を自ら出してしまっているということに関して、社会的保護が及びにくくなってきている。そのような情報を預ける主体へのセキュリティ教育などの必要性であるとか、そういう観点からの政策に対して言及する必要があるのではないかという気がする。

→　御指摘の点はもっともである。ただし、この部分で書くか、各論として個人や供給主体についての取組みが出てくるので、そこでの具体的な取組みの方策として書くかということはある。

○　個人情報の受け渡しなどをみれば、供給側と管理側の２つのアプローチは必要であると思っている。また、それと同時に受け渡し方が問題になってくる。単純な受け渡しが多く、個

人情報を下さいといえば、名前から何から全て渡すという概念が多い。２つのアプローチに加えて、供給側と供給側の受け渡し方、やり方・プロセスを考える必要がある。

○　国民生活審議会の個人情報保護検討部会において、先ほど委員から指摘があった、SNS・ブログ等で個人情報をどんどん出しており、それを悪用しようと思えばできる状況があるので、教育等が必要であろうという意見も出されていた。学術的にも取り上げる意味があるというような意見もあった。情報セキュリティの文化の側面、ソフトパワー的な側面という意味合いからも、NISC で議論するべきと考える。次の情報化ステップでは、すでにグーグルであるとかヤフーをみれば明らかであるが、データベースの多用の側面が更に発展すると思われる。ここは、リアリティのある次のステップのセキュリティとして、はっきりとするべきである。

⑵　「枠組み設定」及び「推進体制」部分に関する検討論点について

○　２点確認したい。先ず「児童への目配り」について。同様にＩＴ利用に疎い高齢者と比較し、児童だけ特別に書き抜いているのは、投資対効果等の観点からメリハリを付けたなど、何かお考えがあって敢えて児童に的を絞られたのか。また、主体間の責任分担の前提となる「規範性」とは、何を意識しているのか。

→　児童については、人格形成途上のものには教育を行わなければならないのではないかということから、記載している。また、評価 07 の中でも、若い世代は情報セキュリティ対策をあまり取っていないというデータもある。高齢者についても、対策をやるべきではあるが、定年を迎えたばかりの方はある程度自分で対策が出来ると思われることや、IT をよく利用している状況を考慮し、特出しはしていない。

→　規範性については、義務というよりもむしろ、責任分担の根拠という意味合いで書いている。議論途上ではあるが、先の委員会でも意見があったように、様々な主体がサービスを提供し、ネットワークがつながっているため、責任分担・対策分担をどうするかということについて、その根拠も含め考えていかなければならない、という意味で書かせていただいている。

○　対策実施主体について、全て国内の話にとどまっており、海外の企業が日本人の大量の個人情報、企業の機密情報等を持っているという状況もある。日本だけで法律を作っても全く意味がなく、政府間の連携の中で何かやらなければ、向こう任せになってしまう。こういったことの記述も必要ではないか。

→　対策実施主体のところでも海外企業を考えるが、国際という横断的部分のなかで、国際展開を日本の企業が図る、海外の企業が国内に進出するという文脈でも考えたい。

○　「理念」のところで言及されている、情報セキュリティに完璧はないという前提に立ってという言葉は、事実ではあるが、全面的に出すと「完璧はないので失敗してもよい」という捉え方にもなるので、表現はフォワード・レジスタンスのような形にした方がよいのではないかという気がする。

○　児童が中心との話があったが、可能であれば情報弱者として、高齢者若しくは児童という

形でエグザンプルのような入れ方が良いのではないか。高齢者の利用状況についても、使わなければ生きていけないという状況になってきている。日本はとても良いことに高齢化社会であり、高齢化社会は長生きするということであり、これからもどんどん使っていくという考え方をすると、児童だけとするのはどうかと思う。

→　弱者論でフォーカスをぼかすと、最終的に施策に落ちてこない。ここでの児童への目配りは、最終的には学校教育の中でセキュリティ教育をどのようにしていけばよいのか、現状の情報科目の中で情報セキュリティを教えていない課題をどうするかということを「てこ入れ」のターゲットとして考えている。IT 戦略本部での会議でもそうだが、IT 弱者という言葉になった瞬間、政策がランディングできないという悪い経験をみているため、あえて弱者という言葉はここでは書かないようにしている。

○　情報教育の中にセキュリティを入れていかなければならないことは同意。本来、情報の分野は文字を書くことと同様、高齢者も受けていなければならない教育であるが、先に生まれたがゆえに教育の機会を得られなかったと考えることもできる。その人たちも含められる形で書けるとよいのではないか。情報弱者とすると曖昧になってしまうのであれば、非識字者のような者を生んではならないという観点で情報を位置づけていただき、高齢者も含め基礎教育をさせて行くことが必要ではないか。

○　児童がここにあることもおかしいのではないか。児童を入れても良いが、この対策実施主体４領域の中に、産官学の学がない。対策実施主体として教育・研究というものを新たな分野として入れて、その中に情報セキュリティについて考え方を広め、かつ基盤的な研究を進めるということを入れた方が、児童も高齢者も入るわけであるから、より良いように思える。

→　対策実施主体をどのような定義にするかという定義の問題であると考える。事務局としては、教育・研究機関は問題の理解解決支援主体（対策支援主体）として分類しようと考えている。

○　児童を入れるかという問題で、先ほど人格形成途上という言葉があったが、人格形成途上であるから児童を入れるのかということについてお考えをうかがいたい。また、児童については定義が複数あり、児童福祉法や国際的な児童の権利に関する条約で言えば 18 歳未満ということになるが、学校教育法や道路交通法で言えば６歳以上 13 歳未満になる。そのため、年齢的な定義を置かず、ここで児童と入れてしまうことには問題があるのではないか。何故、その年代の子供たちに対し重点的に何らかの施策をする必要があるのかということを、ここで議論して明らかにしてはどうか。

→　小学校の IT 教育で情報セキュリティをどう取り扱うかは難しい議論なので、IT 戦略本部の方でも出されているが、我々の守備範囲ではないと考えている。社会へ出る前の基礎的な教育を与えるということでは、高校生までが現実的な手段と考える。大学も現実的な手段ではあるが、約半数以下という進学率、教育の中身に関しての枠組を考えると、高校までが現実的に考えなければならないところであり、事務局としては、中高がメインターゲットになると考えている。

→　ここについては、情報セキュリティ政策会議の有識者からも意見が出されていることもあり、児童と書かせていただいている。定義されてないまま児童という言葉が出されていることに問題があるのであれば、きちんと定義し整理しなければならない。他方、この議論に関しては、本当にこの政策レベルで取り扱うことであるか、文部科学省に任せてもよいのではないか、政府全体のプライオリティを考えたときにどう位置づけるかという議論があり、有識者からも意見は出されている。

○　小中高で、特に中高にフォーカスということでよいか。そうであれば、生徒、と表現すべき。小学校も含めるのであれば、児童・生徒という表現がよいのではないか。

○　教育・研究に関するコメントであるが、研究・大学機関はイメージが違う。政府機関・地方公共団体、重要インフラ、企業については、命令・指揮系統がヒエラルキーをベースとしているのに対し、大学・研究機関は、大学の先生、研究者のイメージが強く、個人の集まりという感じが強い。今の分類を見ると、ヒエラルキー系のものと完全個人のものに分けられており、その中間領域的なものとして、個人の集まりのような組織の代表として、研究機関や大学があると思っている。

○　高齢者のインターネット利用率は非常に高まっている。アメリカの例を見ても分かるように、現在60歳代が約５割だとしても、３年後、５年後はもっと高まっていくことを前提としなければならない。先ほども意見があったが、教育を受けるチャンスということでいえば、文部科学省の生涯学習という形でなんらかの手をうたなければならないのではないか。自分で主体的にやっている勤労者世帯とは違う人たちという概念で、何らかの手を打っていくことは必要であると考える。

○　施策として実現性のないもの、あまり具体化ができないものを入れることは、結果的にできなくなってしまうため、実現性のあるもの、具体化ができるものを入れていているという説明であると理解しているが、ここは基本計画の上のところ、概念の部分であるので、もっと大きく書いてもよいのではないか。そして、個別に落としていく中で、児童・生徒だとか高齢者だとかに分けていけばよいのではないか。最初から弱者を見ていないということでは、反発も出てきて、基本計画自体が視野の狭いものと見られてしまわないか。

○　成人については、自分の責任で学ぼうとするべきであって、情報セキュリティを学ぼうとすれば、民間でのパソコン教室、大学等での公開講座などへ行けばよいのではないかと考えている。対策実施主体として、特出しした場合、経費の議論、税金投入の議論が発生することを危惧している。ラディカルな意見ではあるが、人生のベテランである高齢者については、自ら取り組んで欲しいという気持ちを持っているという意見を、敢えて申し上げさせていただきたい。

○　高齢者だけを特出しする必要性が分からなくなってきている。若い人で情報セキュリティ自体を理解していない方と同等に取り扱ってもよいのではないか。児童については、自己形成ができていないということで特出ししたということは分かる。高齢者を特出ししてその先どうするかということもあるので、特出ししなくても、個人の中で情報セキュリティを理解

していない人として配慮をするのだろうなという感じはしている。

○　この議論については、別枠として後半に人材育成という話があり、その中で人材育成だけではなく、全体の教育・啓蒙という、情報セキュリティについて知らしめることを人材に絡めて書き込んだほうが具体的に分かりやすい。IT 弱者の定義については、それが年齢に関係なく存在するということを経験しており、高齢だからということは特にない。もし高齢の方になじみが薄いとすれば、IT の社会的普及が最近だからであり、そのことに触れていない方々に対し、何らかの教育というか、広く学ぶという環境は必要かと思う。他方、現在このような社会で生活をしている方々については、10 年 20 年後に高齢者となるが、特別な指導をする必要もないと考える。そのようなことを考えているようでは、とても IT 社会とは言えない。つまり、経過措置としての学ぶ場について、後ろの人材育成のところで子供たちを含めて議論し、まとめたほうが分かりやすいのではないか。

○　対策実施主体について違和感を感じるのは、政府機関・自治体、企業が基本的に人の集合体である組織であり、個人も人である反面、重要インフラはどちらかといえばハードウェア、サービスという意味ではソフトウェアであり、カテゴリーが違うものが混じっていることであった。重要インフラは企業が運営している面があり、その部分ではクロスになっているところもある。しかし、情報セキュリティという面で考えると、こういう切り出ししかないとは思っており、やや違和感はあるものの、この４領域を第１次計画でも出しているので、ここでは特に児童というものを出す必要はないのではないか。具体的内容は、後ろの方で出してくればよい。

○　１都９県の教育委員会の集まりが予定されているが、一見して情報セキュリティに関する項目はなかったと認識している。そこでは、義務教育と高等教育について話し合いがあるが、情報セキュリティに関してどのくらい関心をもっているか確認し、委員会の議論にも反映させたい。

○　児童という観点ではなく、情報弱者という形で含めた方がよいという意見に同意。高齢者は自分で対策をするべきという意見もあるかと思うが、こと IT 関係については全てがネットワークで繋がっており、弱い個人、情報セキュリティの概念が低い個人がいると、そこがセキュリティホールになって他に迷惑が及ぶ。そのような観点でみると、個人は個人でないというか、個人ではあるがその被害が他にも及んでしまうという観点で書くとよいのではないか。

○　個人をどのように考えればよいかということについて、社会全体の福祉・厚生（Welfare）を下げないためには弱者を少なくしたほうがよいということはある。それは、関係性があるからである。その点では、政策実施の合理性を担保し、政策を行う意義があるということを言った上で、情報弱者を政策の中で位置づけるべきである。

○　電子政府評価委員会では、政策効果で切っていこうとしている。ROI とか KPI の指標で日本の IT 政策の投資効果、政策効果を定量的かつサイエンティフィックにチェックしていこうということを考えている。その枠組は、今年の電子政府評価委員会の報告書で出している。

その観点からすれば、個人への政策、予算投入がサイエンティフィックに合理性を持つか否かは定量化にかかってくる。インデックス、インディケーターを明確にし、先程委員がおっしゃった方面に予算を投入していくことが社会にとって明らかに良いということを証明するロジックと数式を必要とする。これはEUの政策の投資のやり方でもあり、アメリカ・オーストラリアのやり方である。日本の場合、どちらかといえば法規の枠組みの観念が出て、サイエンティフィック、インディペンディングな観点からの政策評価を行っていない。ここにアメリカ、EUとの違いがある。少し踏み込み、こういった定量化指標を使った方がよいのではないか、もちろん、法規は法規で意味があるので、並行してあってよい。可視化できないと、比較してこれが優れている、優れていないということが言えない。居合わせた人の多数派の意見だから決定したというケースが多い。効果があるのであれば、違和感があっても児童という言葉を使えは良く、情報弱者を救った方が政策効果が現れるのであれば救った方が良く、高齢者も政策効果が上手く示せるのであれば、取り組めばよい。その辺りをロジカルに委員会で議論するのもよいのではないか。

○　情報弱者というか情報無責任者、ボットやSQLインジェクションを埋め込まれていたサーバ等を別に直さなくてもよいという人が多数いる。ウィルスに感染しても直す気がなく、何か影響があるのかという人もいる。こういう人が、ボット・DDoSの発射台になる、偽サーバに仕立てられ、DNS ポイゾニングでオンラインバンクに見立てられるなどして、無責任でいる。そういう情報無責任者にちゃんと直せという強制力が今はない、そういうものを出口としてもっていくというのはどうだろうか。

→　個別のところで議論させていただきたい。

○　対策実施主体について、「主体内（個人等）に加えて主体間…」という部分は、重点施策なりに展開することを想定されているのか。どういう形で検討しようということなのか。

→　個々の集合体か個人かは別にして、現在の実施主体の観点は、政府も重要インフラも企業も個々の実施主体として捉えており、主体ＡとＢが協調して対策を行う観点がない。それについて検討することは必要か、というのがこの部分の問いかけである。中小企業や児童をどう扱うかは主体の細分化であり、後で出てきてもよい話ではあるが、「主体間」をどう扱うかという意味では枠組みなので、特出しをさせていただいている。

○　政府機関対策中、統一基準では、政府が行う外部発注・アウトソーシングは、発注するときの要件だけで書いているが、もう少し上手い枠組でやりたいと事務局では考えている。

○　重要インフラについては、専門委員会を経てではあるが、所管法と原課がどこであるかを見つつ、対象企業（一部対象企業と言わせてもらえていない分野もあるが）及び対象者を決めて政策展開している。その対象はユーザ企業、ユーザ的な主体であり、ITセキュリティのことを考えると、IT サプライヤーとの関係をどのように考えるかは論点として出ているが、具体的に施策の中でどうするかについては、なかなか言えていない。今から３、４ヶ月の期間をかけて検討せざるを得ないと事務局では考えている。

○　普通の企業については、経済産業省ではモデル契約書という形で外注先との関係の議論は

しているが、対等性がどうあるのか、管理義務はどちらに置くかなどの議論に入って行く必要があると考えており、単にガイドラインを示すだけではどうにもならないと事務局では考えている。

○　主体間に関しては、ここでは規範性と示しているが、いろいろな形、法律をつくる考え方、そうではないもっとソフトなやり方があるのかもしれない。第１次計画に沿う取組みの中で、対象としている部分と周縁のジョイントの部分について政策展開をしていかなければ、実効性が確保しにくいのではないかと考えている。事務局としては、ひも付けをする具体的な政策があると考えている。

○　従来の分類では、政府機関と地方公共団体を一括りで分類しているが、主体を分ける、記述を分けることも必要ではないかと考える。また、大学についても政府機関に近いところで行っているが、実情はかなり色合いが違うと感じており、政府機関をもう少しわけるのであれば、大学も特出しで出てくるのではないか。地方公共団体についても政府機関とは異なってくると思われる。

→　提言の中でどのように書くかは、委員の意見に従うところであるが、地方公共団体については、行政機関という役割と重要インフラとしての役割があり、２つの領域にブリッジしている。総務省とも話をしたが、政府として地方公共団体に指示出来る立場にはなく、これをどうするかという課題がある。地方公共団体をまとめて書いたほうが見通しがよくなるのではないか、という考えもあるが、注文に見えてしまうのではないかというトレードオフに悩んでいる。

→　政府からすると大学は独立行政法人等という位置づけであり、現業をもっているものについては、現場毎に需要や必要なものが異なるので、理性的に考え、必要な対策をきちんとやり、主管官庁にきちんと示しなさいという以上のことは踏み込んでいない。事務局としては、それ以上踏み込めないという印象を持っている。また、大学には国立と私学等があり、いろいろと議論もあり、言及していない。

○　セキュリティマネジメントは、指揮命令系統がどうなっているかということからはじまるが、私学系は格別、大学法人・研究機関等は指揮命令系統がない。そこで作り方が変わる。政府統一基準をきめ細かくする、企業のように大学法人の対策をきめ細かくやればよいのかもしれない。主体として完全にわけろという無理をいうつもりはないが、対策的には少し考慮したほうがよういのではないかと、現場では感じる。

○　対策支援主体、促進する主体として、第１次計画ではメディアや教育機関が書かれているが、ここでは書かれていない。これは、ここでフォーカスするのはここに書かれているものだけで、それ以外は検討しないということなのか。

→　検討しないとう言うわけではなく、暗黙の了解で入っているという認識であった。明示すべきであった。

○　教育機関というものも促進主体としては入ってくるということか。

→　教育機関・メディアなど、従来から入っているものは入れているつもりであった。ここ

での教育機関の位置づけは、教育することにより実施主体の理解解決を促進する主体であり、対策を実施する主体ではない。

○　プログラマ等がセキュリティを考慮するために共通言語を作る必要があるのではという話は、ここに特出ししてもよい。対策実施主体の主体間の記述において、協力体制、役割若しくはコミュニケーションをどう取るかということを付け加え、そういったものをやっていくとすれば、主体間のジョイントの部分として、プログラマ等云々の共通言語を作るといった話は整理できるのではないかと考える。

→　このパートでは、標準化団体、法律に基づく標準等の役割をフォーカスするべきではないかということで書いている。IT ベンダが関係する標準化のプロセスに関わる人たち、あるいは団体、組織、フレームワーク等があるのではないかということで書いている。

○　ここでは共通言語の方策を進める組織というか、主体を考えるということか。

→　組織論をやる訳ではなく、現実にそういう取組みに関わっている人々がおり、セキュアな、あるいはセキュリティの機能が高い、その機能を確認し得るシステムデザイン、システムインプリメンテーションは、標準化のプロセスでやられている。そういう方々にどのような働きかけと政策展開をしていくかということが、この支援主体というところで浮き彫りになるのではないかという趣旨で、ここに入れている。

○　先ほど議論があった、児童への目配りということも不要ではないか。極端な話、被害を受けたものが辛い思いをすればよいわけで、そのようなアメ・ムチがなければ対策は進まないと思っている。その辺りは、メリハリをつけてまとめる必要があるのではないかと思う。

○　「枠組み」に関する記述は、立体的にしないと単純な感じを受ける。やりたいこと、やるべきことは挙げられているが、実際にその実効をどう担保するかが重要である。規制論者であるから法律を作るべきと述べている。ガイドライン、規範、共通言語を作っても、やらなくても済む場合はやらない、やらないほうが楽である。例えば、ボットに感染しても、自分が被害にあわなければよい、何もやらなくてもよいということになる。第１次情報セキュリティ基本計画では、問題点を提起し、状況を理解させるための努力をした。今回、状況を把握したとかやっているが、問題点を解決しようとする段階で同じような議論をしても仕方がないという気がしている。もう少し踏み込んで、法律を作って全部取り締まれとは言わないが、共通言語をもってというところまで言うのであれば、セキュアなシステムを作るための仕組みをどうやって作るかということを提起しなければならない。

→　法律のような作業コストが大きくてオペレーションがしにくい道具は、最低限しか使うべきではないと思っている。そのための代替手段、具体的に実効性の高い手段というのは、今のところ見つかっていない。それに対して何ができるかについて、チャンスがどこにあるかは分かってきてはいるが、具体的にどうするかは全然見えていない。いくつかの可能性に対してマルチビッドしている状況が、第２次情報セキュリティ基本計画ができるサイクルの第一ステップではないかと思う。強い規制に入っていくことは、強く意識していない。規制が入ると社会コストが上がると同時に、マーケットが非常に弱くなる。情報セキ

ュリティ単体で、マーケットが許容しうるレベルかということには悩んでいる。マーケットが元気で右肩上がりであればやるべきであると考えるが、日本のITマーケットは世界と異なりフラットかマイナスである。そのことを考えると、こんなにフラジャイルなマーケットを抱えているところで規制をやらなければならないのかということはある。全体のトーンとしては、個人としては強くは書いていない。但し、第１次提言は基本計画検討委員会の提言であり、事務局との綿密な打ち合わせは必要かもしれないが、委員のみなさんがそうすべきだというのであれば、書くのかなと事務局では考えている。

○　マーケットのインセンティブを重視したやり方をどうやって作っていくかというのが、この委員会の事務局の基本線だと思われるところ、その効果が不確定であり、コストがかかるかもしれないが、作ってそれで強引に進めるということも選択してあり得るということも、検討しても良いのかもしれない。次回の委員会までに各委員の意見を伺いに行くということなので、そのときにおっしゃっていただいてもよいと、委員長としては考えている。

○　既存のガイドライン・基準の例示にあるように、この手のものがたくさん決まっており、これにより徐々に改善しているとは思われるが、本当に皆が幸せになったのかのだろうかと感じている。こういったものを事業者に決めろといえば、決まってくるが、これにより本当に遵守されているか、レベルが上がったのか、やった人やらない人のメリット・デメリットが出ているのか、こうしたことを具体的に出すような枠組を作っていかなければ、やりっぱなしになってしまう。極端な話、５年後に同じような会議をやっても、結局同じことだったということになりかねない。実効性を担保できる枠組なり、仕組みなりを組み込んでいかなければならない。その一つとして、私は法律があると思っている。

○　法律制定は非常に作業コストがかかる、ということは疑問を持っている。鍵を閉めずに家を出て、泥棒に入られましたといっても自慢にはならないのと同様に、ウィルスに感染したということをある意味自慢することはおかしい。そういったプリミティブなレベルにある者は、社会的な規範やルール、場合によっては法的な処置も含めて担保していかないと、社会が上手く動かないのではないか。そういう枠組全体を第２次情報セキュリティ計画に全部入れるわけには行かないと思うが、何らかの雰囲気を入れておかなければ、第２次情報セキュリティ基本計画を作る意味合いが薄れてくるのではないか。

○　委員の意見に賛成であり、法律の制定が非常に作業コストがかかる作業であるとは思わない。ただし、法律でできる部分とできない部分、やっていい部分とやってはいけない部分がある。ここは、その細かいところを議論すべき場ではないが、方向性としてそういうこともあるということは、第２次情報セキュリティ基本計画で是非入れていただきたい。具体的に何をするかは、この場で議論すべきことではないと考える。

○　法律に盛り込むかどうかという議論もあるが、実務的な問題として、情報セキュリティの脅威は次から次に現れるものである。とすれば、脅威を想定できる範囲内でしか法律化できない、ガイドラインを作れないという状況では、法が想定していないことがたくさん生じることにより、なかなか追いつかなくなってしまう事態がこれまでも出現しているのではない

か。

○ 「プログラマ等がセキュアなシステムを確実に提供できるようにすべく…」という箇所は、非常に具体的なことが書かれており、非常に違和感を覚える。問題の本質は、仕様書を書く発注者側が共通言語をもって対話できないことにあるのではなく、どこの水準まで情報セキュリティを担保するかを決めれば、サプライヤーとしてそれほど間違えることはない。どこまで実施すべきかの社会的合意や、どこまで規範性をもってそれを定められるかについては様々意見があると思うが、どこまで実施すべきかということが決断されない、発注者側の責任としてそのガバナンスをしていないことが問題の本質であり、共通言語を作っても問題が解決するわけではないのではないか。異論があるわけではないが、この部分はここで書く程のことではないのではないか。

○ 今の委員の意見と思いは同じであると考える。NIST 等で設定している、社会通念上これくらいのシステムを作ればセキュアであると相互にいえるような基準を作って欲しい。それが共通言語の範疇に入るものだと認識しており、「共通言語」という言葉でも良いのかなと思ってはいた。今の委員の意見によると、範疇に入らないということだとは思うが、思いとしては同じである。明日になると違う情報セキュリティ上のリスクが出現し、それを今日想定していなかったとして全部サプライヤーに責任を負わせるというのは問題であり、基準・スタンダードが必要ではないかと思っている。それが共通言語の範疇と考えている。

○ この部分では、二つの要素があると考えている。一つはソフトウェアの品質・信頼性に絡むところであり、それを担保する、責任を持つという仕組みが、今の IT サービスの中では欠落しているという問題がある。もう一つは、共通言語というのは合意形成の手段のことだと思うが、容易に合意形成ができる手段、モデル契約書であったり、FNCP をベースに双方が発注過程を含めてプロセス管理をするというのも合意形成のところであろうかと思うが、何らかの形で容易に合意形成できる仕組みや、でき上がったソフトを担保するような明確な仕組みなどはいるのではないかと思っている。情報セキュリティに絡むことだけではなく、品質担保や責任をとってきちんとやれる仕組みがないだけに、いつもこのところが問題になるような気がする。建築の分野では、建築士という個人の責任おいて構造設計に責任を持つことにより担保する仕組みがあるが、それに類似するものがあってもよいのではないかと思っている。こういうものが無いことによって生じる問題が、トラブルになっている。ただし、責任体制を明確にしたからといって何か解決するという短絡的なものではなく、エンジニア全体のレベルを上げないと駄目だとは思うが、共通言語だけをもっても解決はしない。合意形成は重要であり、何らかの枠組がいるかということは感じている。先ほど指摘があった部分は、今回資料に追加された記述であるが、今までの流れからすると、ここだけ具体性があり、書き方の馴染みがないかなということは感じている。

○ この部分については、色々と議論はあろうかとは思うが、委員長としては、事務局に意見をまとめていただきたいと考えている。

○ 「枠組み設定と推進体制」は極めて重要な部分であるが、現段階ではいろいろなレベルの

ことを必ずしも論理的な構成を考えないまま書いたという、若干つらい内容に止まっていると感じる。今後、文章にするときに上手く整理されるよう期待したい。

○　物事の順番として、先ずは推進体制強化の必要性を冒頭に掲げ、その具体的な解として米国のNISTのような組織体を作るということを持ってくる整理が普通。すなわち、ポイントは「NISTのようなものを作る気があるか」を主軸に据えて議論することにある。これらの点は、上記の枠組設定の議論とも絡んで、「どういう主体や機関がどういう立場・役割で参画し、全体としてどう構成するか」という絵を1枚描けば、かなりクリアになる筈である。この間、「他分野との連携について」は、後順位に回せば良い。

○　「委託・アウトソーシングを進めることが重要ではないか」という部分は、私の主張とは逆で（他の委員からの意見であれば残しても良いが）、むしろ、委託が進み過ぎた弊害があると感じている。本気で推進体制を強化するのであれば、今のご時勢から逆行する話ではあるが、「真に重要なシステムの主導権は元の機関に復帰させる」、「任せ切ってはいけない」ということを前提に、「IT ベンダの役割は何であるか」を明確にしてはどうか。この点は、特に政府機関を念頭に、従前から申し上げている。行き過ぎた委託・アウトソーシング、全て丸投げが多いという現状を考慮したとき、本件は重要な論点である。

○　この部分の議論については、議論をクリアにするために、NISTに類似するようなものが必要かどうか、あるとしたらどうしたらよいか、いらないとしたらどうしたらよいか、という進め方がよいのではないか。

○　委託・アウトソーシングについて。文書の文脈からいくと、合理的な情報セキュリティ対策というのは、自分でやるのは大変であり、アウトソースしてもいいのではないかという意味と認識している。たしかに、IT ベンダに丸投げしているからそもそも問題だというのは、あると思う。ただ、一方で情報セキュリティ業界に身をおいている者からすれば、不十分な情報セキュリティ対策の結果として問題が生じている、にもかかわらず対策した気になっている、そういう事例も把握しており、情報セキュリティ業界の役割もあると考える。

○　情報セキュリティ対策そのものが進化しておらず、全てパーフェクトにやらなければならない、PDCAからやりましょうという論調があるが、そればかり言うべきではないと思う。「枠組み設定」の部分で言及されている中小企業について、その対策が進まないのは、モチベーションが無いこともあるが、人も金も物もないのでモチベーションだけをつけてもできないのが事実である。業界として、安くて簡単で効果的なものを考案して提供する必要がある。情報セキュリティ対策のある部分の委託・アウトソースはやってもよいのではないかと思っている。

○　政府機関を見て特に思うことは、対策を実施することはアウトソースしてもよいと思っているが、何をやらなければいけないかと考えるとこまでも人任せにしているところがある。先に委員が言われたことだと思うが、そこは自分できちんと持つべき。アウトソーシングを進めなさい、止めなさいという議論は乱暴。実施段階の話と、頭をつかうところは自ら持たなければならないということとは、分けて考えなければならない。アウトソーシング自体は

進めてもよいと思うが、考えるところまでを捨ててはいけないと思っている。

○　特に政府機関もそうであるが、企業についても、情報セキュリティについてはアウトソーシングが進んでいるという感がある。何故かと考えると、情報セキュリティについては、スペシャリティが少し必要なところがある。システムであれば、自分の業務についてアウトソースするだけなので、自分のところで何をやるか、何をアウトソースするか分かっている。しかし、情報セキュリティについては、０からの丸投げになっているので、企業においても、情報セキュリティについては自分で考えるところを持たなければならないということで、議論を分けていただきたい。

○　推進体制の強化は必要であり、NIST のようなものがいるというのは同感。しかし、この文章を読んで、公的機関として政府調達における技術評価も実施とあるが、“も”と書いてあり、NIST の役割が明確に書かれておらず、どこまでやるか分からない。また、「社会全体における情報セキュリティに係るリスクを把握する機関」とあるが、どこまで踏み込むのかという疑問もあり、あまりよろしくないのではと感じる。文書だけをみれば、把握するためにはこういうセンサーがいる、こういうシステムがいるという話になると、どこまで行くか分からない。善意でみればそう解釈はしないが、単にリスクをどう評価するなどの分析だけであればよいかも知れない。

○　機能するか確認を行う体制とあるが、これは政府調達のシステムだけに対してかということを確認したい。仮にそうであるならば、それが明確になるように書き直す必要がある。

○　NIST のようなものについて、私のイメージと事務局のイメージが違う可能性がある。NIST のようなものと言ったときに、フレーバーとして出ていないのが、海外に対して日本の基準を外からの基準に対して主張していく、そのための基礎研究をしていくことであり、そういったことも必要ではないか。そういうことも進めていただきたいという気持ちもあり、NIST のような機関を作っていくというのは賛成である。

○　「我が国全体を視野に入れて情報セキュリティ政策・対策を推進する機関について」という部分を読んだ場合、では NISC は違うのかという感じがする。今、NISC が持っているミッション・機能で、もう少しやらなければならないことがあれば、その機能を充実させていけば良い。そのモデルが NIST にあるのであれば、それを全部まねるのではなく、日本の国内事情をかんがみて、必要な機能を充実させれば良いのではないかと考える。

○　アウトソーシングについては推進派である。サービスがきちんとしてくれば、アウトソーシングは大いにすべきと思っている。大事なところは、先に指摘があったように、自分たちが考えるべきところは率先してやった上で、自分たちの事業、活動のコアになっている部分を見極めて出せばよいと考えている。社内では「魂は売らないアウトソーシング」と呼んでおり、魂は売ってはいけない、そこだけは自分でやれと。これは、それ以外のところは積極的にアウトソーシングをしようということである。その方が全体として、自前主義でやるよりははるかに品質が上がり、コストも抑えられる。使い方さえ間違えなければ良いのではないかと思っている。

○　委託・アウトソーシングをやるかどうかということは、ここで議論すべき問題の本質ではないような気がする。ポリシーがないことには、委託しようがしまいが進まないことに変わりはなく、それを形成する必要性が高い。最低限どこまでやるべきか考えたときに、ガイドラインが良いのか法律が良いのか迷うが、その解決策としてNISTのような組織があって、その時々の状況に応じ「ここまでやればよいのではないか」ということを専門的な観点から助言してくれる、あるいは指揮するという役割を果たすことにおいては、一つの解決策ではないか。今の日本には、そういう役割を専門的な立場から果たすという組織がない。その意味でも、NISTのようなものに何を期待するかということは、明確にしておかなければならない。規範性に代わるものとして、オーソライズを与えてくれるものとしてNISTのようなものがあるのならば、一つの解決策になるのではないか。そのような、ポリシーの形成や社会的合意を作ることに最重点をおくべきであり、委託・アウトソーシングによっては対策が進まないと考える。それは手段であり、中小企業向けに配慮しなければならいということはどこかで述べられなければならないが、問題の本質ではないと考える。

○　確かに本質議論とはズレるかもしれないが、アウトソーシングを敢えて持ち出したのは、政府機関や金融機関をはじめとする重要インフラは、理念的な整理は別にして、実際問題として考えたとき、アウトソーシング先であるＩＴベンダーが実務面での主役になるという現実が存在するからである。

○　アウトソーシングが手段に過ぎないという考え方自体は、他の委員と同意見だが、そういう意味でも、自分の企業が拠って立つ重要業務については、少なくとも主導権を持った方が良い。もちろん、狭義の情報セキュリティに関する技術面など非常にスペシャルな部分について、専門家を上手に活用することは、当然重要と整理できる。

○　体制については、従来の体制は残しつつも、中小企業から地方自治体までいろんなところが対策を推進するためには、自力でできないところもあるので、これをサポートするための体制が一定程度必要である、ということが前提としてある。環境をつくることが重要であるが、自立的にできるわけでもない。どういう業界・会社、どういう技術水準をもったものに委託するかということも含め、その場のいろいろな難しい問題があるので、政府が発注する場合や企業が発注する場合も含めて、政府内にそれを評価し、アドバイスする体制が要るのではないか。その際、参考とする機関がNISTである、ということがこの資料に書きたいことであったと解釈すれば、この書き方では大いに誤解がある。順序が逆のような気がする。委託する・しないは本人の勝手であり、業界によっては外部に委託されては困るものもあることを考えると、言及することはいけない。これを進めることが重要ではないかと書いて、損害が出た場合に国に責任をとってくれという話にもなる。

○　推進体制について記述されているとは認識していない。NISC自体の機能をどこまで強化する必要があるか、どういう機能を付け加えるべきなのか、自前の組織を増やすのか外部に依存するのかということは、書きにくいとは思われるが、はっきりさせないといけないのではないかと思う。NISTの基本的な機能は、ここに書かれているようなことではないのではない

か。JIS をどのように解釈するかという問題も含めて、規則・ルール・ガイドライン等の設定の仕方についてかなり問題になっているが、昔と違い、中身を定義するのではなく外見を定義するという標準がどんどん出てきている。特に情報セキュリティに関してどうするかという話は、別途考えなければならないので理解はできるが、このような書き方にはならないのではないか。

○ NISC の機能強化は、明らかに必要であると思う。重要インフラ等を統括するにしても、全ての情報が集まっているわけではなく、指揮命令がきちんとできるかは疑問なところがある。素直に問題点、改善点を指摘する必要がある。

○ 実施主体が４つあるが、それぞれについて情報セキュリティ機能、レベルを上げるためにはどのような体制が必要か、これは重点施策で書くのかも知れないが、ある一定の概論はまとめておく必要があるのではないか。

○ 社会として、これくらいやっておけばサプライヤー及び発注者の両方が納得できる機能である、というようなことを決めるところが欲しい。そういう意味では、日本で唯一やっているところは CRYPTREC ではないかと思っている。CRYPTREC が決めたものであれば、本質的には問題があり議論はいろいろあるのかもしれないが、納得感はある。良い悪いは議論があるかもしれないが、発注する側もサプライヤー側も、このアルゴリズムで行きましょうということはできる。そういったイメージの組織体制は強く欲しいとは思っている。それをどこにつくるかは、書き振りとしては NIST とか具体的になっているが、そういったものが欲しいというイメージである。

○ 対策実施主体として政府機関についての体制の強化は、これは NISC のことを示唆しているのか、政府機関の対策を厳しくするための体制の強化ということか確認をしたい。

○ 「まずは政府機関が率先垂範し、背中を見せることが重要である」という意見を出した。政府機関の対策充実度の実態がいまひとつ定かでない中で、中小企業や個人に何かやれというのは、無理なのではないかと書いた。そういう意味では、「体制の強化」は NISC や政府機関が主眼ということになろう。

○ 現状の NISC と、NIST など理想的な組織の間で、どこに差分（GAP）があるのか、何が◎で、どこが△、×なのかといったことを整理して提示し、×や△のところは、税金使ってもやる必要があるのか、余計なお世話だから現状程度やっていれば十分かを、個別に議論してもらう必要がある。

○ NISC が本音でどう思っているのか、どのような権能があれば対策が進むと考えているのかを整理し、それへの賛同があれば、第１次提言で書いてしまえば良いのではないか。しかし、重要インフラや一般国民の側からみると、そこまで期待されていないような気もする。NISC が何の権限が欲しくて、何をしたいか、そのためにはお金が足りないのか、人が足りないのか明確に主張し、それを国民的目線で審議しましょうという筋の話ではないか。

→ 体制の強化については、政府対策の推進において、府省の予算・人員を確保する必要があるというのが意図である。定量的に人員の不足は検討できていないが、政府機関の評価

でも対策不十分な項目として、教育の実施や、システム台帳の整備等が課題としてある。

→ NIST 云々については、政府がテクノロジーを分かっていないという問題や、２年に１度記憶喪失になることをどう治すかということの一つの方法であろうと考える。専門家を外から買ってくるというやり方もあるが、不幸になることも多いので、ちゃんとしたプロパーの人たちが、ちゃんとしたことをやれる組織が、何年かかるか分からないが、あって欲しいということである。

→ NIST のような体制については、テクノロジーセントリックに動き、それは政府自身のためであるが、その活動ともに社会全体にとってテクノロジーとして何が必要かということはみていかなければならない。それは決してモニタリングしようというものではない。今の状況を考え、本質的に治すための体制というのはどうあったらよいかと事務局では思っている。

→ NISC をどう強化するかについては、大変になってきている。もともとできないところに無理やり作っている。役人が「そんなことはできない」と言うところを、「いや総合調整権能の範疇である」ということで、無理やり突破してきている。NISC をどう強化するかというより、オペレーションと実際のテクノロジーの部分を考えると、各ケースの中で必要な機能をどうするかを考えなければまずいと思っている。

→ ポリシーレイヤについては、内閣官房にあることは適切だと思っており、テクノロジーセントリックなオペレーションをするという意味では、あまりにも政府は体制が貧弱であるということを痛感している。情報セキュリティ補佐官を４年間やってきた立場からすれば、「もう少し技術者がいればこんなに苦労はしなかった」とはっきり思っている。学者が５年も本格的に政府機関に入って取り組むというのは異常である。プロパーの人間がちゃんと働いて、役割を果たしていくことに対し、真面目に考えてこなかったということが問題ではないかと強く思った次第であり、その意味でここに書かれるのが一番よいかと考える。

○ ここの書きぶりは、是非変えていただきたい。今お話を伺う限りでも、各委員のイメージが全く違っている。先の意見については、途中までは賛成だが、後半はいただけない。NISC はオペレーションと言ったらよいのか、欲しいと言われるのはシンクタンクというか、そういったものか。それはNIST のようなものにあった方がよいのか。

→ NISC についてはポリシーレイヤのオペレーションである。テクノロジードライバーがきちんといれば良いということである。それは NISC にあっても良いが、今更 200 人も 400 人も絶対増やせない。

○ オペレーションをするところと、先のことを検討するところは分けておく方がよい。その方が、息の長い仕事ができる。オペレーションを失敗すれば、その部分を取り替えればよい。独法のどこかが担うという話だったかもしれないが、今はないので作るしかない。その中でやることをはっきり書いていただいた方が、議論は進むと思う。そうでなければ、評価すればよいなどの突拍子もない意見が出て、困惑する。

○　IT マネジメントに関しても同様のことがある。外部からの CIO 補佐官を各省に入れてきちんとやりましょう、というのが今のレベル。その中で悩んでいるのは、テクノロジーを理解して意思決定してもらうかということである。CIO 補佐官は意思決定者ではない。情報セキュリティの場合は、CIO 補佐官の兼務が多いが、CISO アドバイザーが各省にいる。情報セキュリティをやったことがない方もかなりいるかとは思っている。そういう意味でも、どこまでというのは難しいが、IT マネジメントと比べてもセキュリティマネジメントの方がまだ強化できていない感じはしている。強化すべき“のりしろ”は、まだあると思っている。

○　根本論として、意思決定者がテクノロジーを理解した上で、オペレーションをやっていただくということが重要である。NISC がオペレーションはできないわけで、IT の管理は各省、各省の中でも各課が行っており、そこまでは絶対に手が回っていないというのが実態だと思っている。そこを変えるのは結構大変であり、IT マネジメントをどうやって普及させるかという中でも苦労している。

○　強化の仕方はどこまでなのかについても、後の議論かもしれないが、議論すべきところである。「対策実施主体としての政府機関についての体制の強化」については、NISC 及び政府機関の両方であれば、そのように書き分けていただきたい。

○　各委員の意見を聞くと、推進体制の部分は大幅に書き換えることになるかと思う。委員長としては、さらなる議論をお願いしたい。

○　甲府市役所の例であるが、完全なアウトソーシングで、サービスを買うという形で行っている。 その代わり、インソース、インタンジブルな部分を強化しており、職員の研修にお金をかけて能力を拡大し、SLA のレイティング、点数付けができる能力をつけている。職員がウォッチしてモニタリングして評価できる。おそらく霞ヶ関でそこまでやっているところはないと思うが、そこまでやればアウトソーシングでもよい。高い能力を持っているわけだから、組立てられなくても、どう動いているか、業務との関係でどう評価するか、評価指標を持てばよく、そこは柔軟に考えればよいと思う。韓国政府も、徹底的にアウトソーシングをやったけれども、アウトソーシングの評価と同時に、インソースの評価もやったと言っている。日本はそれをやらなかったため、ブラックボックス化している。

(3)「抽象部分」総括

○　「事故前提社会」とあるが、「被害を受けた人は諦める」感が漂うかなと個人的には思う。責任をとる人がきちんと取り、対策をとる人がきちんと取り、保証する人がきちんと保証するということが対策の中に入っているかもしれないが、このままでは「諦めろ」という内容にも取られかねない。その辺をもう少し考えた方がよい。

○　キャッチコピーとしては、「おっ」と思わせて「何だろう」と惹きつけるわけだが、誤解まで行くと少し問題がある。

○　BCP があるということも含め、ここのところに一言書いておくと違ってくる。事後対策も含めてやっていることとセットにしないと、「諦めろ」の世界に聞こえてしまうのではないか

と若干思う。

○　そういう声や、懸念が出るという感覚は分かる。しかし、バランスや程度問題であり、他の委員から言及があった「痛い目にあって知ることも重要」ということと、「それを言っちゃお仕舞いよ」というところの均衡の話だ。どこをベンチマークにするかということもあるが、日本はあまりにも完璧であることが社会的・国民的に期待されていることが前提で、メディアもそういう報道をする。しかし、国民全体の経済合理性から行くと、その構造自体から変革した方が良いという認識に立って、敢えて「事故前提社会」という考え方もあることに気付いてもらうことに意義がある。常識として分かっている人には、当たり前のことかもしれない。今までの物事の捉え方が偏っていたので、中立にするためには、敢えてこういう主張も盛り込むことが適当である。表現について、誤解が生じないよう工夫しても良いが、基本的な認識はそれで間違っていない筈だ。何か起こした人の責任を追及しようという動きは、既に十分やられている気がする。

○　何の事故でも、原子力でも地震等もそうだが、絶対的な安全はないことは、常々メッセージを発信してきている。起きたときの対策をしっかり取ると言うことが、本来的な筋である。対策を考える場合、コストと得られる安全水準というものを考える必要があるというのは、当然皆そう思っている。そうであるならば、「事故前提社会」というのは、政府内で流通しているキーワードではないので、敢えて使う必要があるのかということは申し上げたい。皆が共通理解として言えるような表現で、ここは書いたほうが良いのではないか。趣旨については、争うところではない。

○　この議論を講演などですると、聴講者はITベンダや自治体の方が多いので、言えば分かってもらえる。ただ、この言葉は、一般の国民の人が聞くと責任を放棄しているのではないかという変な誤解を起こす可能性があるので気をつけなければならい。

→　方針を大転換したわけではないことを、先の委員会でのご意見を踏まえ、ここには書き足している。事前の防止対策の努力はするわけだが、努力をしても100%はなくならないので、事故も起きる。事故が起きたときにどうするか、BCP、リカバリー・事後対策を考えおきましょうというメッセージを出すという趣旨である。手抜きでいつ事故が起きてもいいと考える人が出てくると困るので、その辺はケアする必要があり、書きぶりについては前後も含めて検討したい。

○　上手く説明を行い、定義をしておかないと、ここだけ捉えられると問題である。この言葉を使うかどうかも含め、事務局に検討していただきたい。コンセプトについては皆了解しているところであると、委員長として考えている。

○　この言葉は、結構キーワードとなるような気がする。ただし、解説が必要であり、事故は防げない事実はあるけれども予見や予防により健全な社会を維持する、ということをきちんと解説すれば使ってもよいのではないか。この事実をきちんと認識することは、キーワードになる。

○　「事故前提社会」という言葉を使うかはお任せするが考え方は是非入れていただきたい。

この場の人にとっては、おそらく当たり前のことであり、講演などの場では納得していただける考え方であると思うが、世の中一般の人は必ずしもそうではない。この部分は、今回の目玉になると思うので、是非お願いしたい。

(4)「重点政策」部分に関する検討論点（全般）について

○　第１次提言素案の中に、重点施策は入るのか、それを踏まえてコメントした方がよいのか。それともその後で時間がとれるのか。

→　先の委員会で、熟度に関する図を出させていただいたが、各論は熟度が低くなると考えており、例であるとか、こういう検討が必要ではないか、というレベルになってくるイメージである。

○　例示であるとか、サンプル的にこれが並ぶというイメージか。

→　第１次提言なので、全て書ききることは考えていない。今後検討が必要なことの指摘はあると思っている。

○　「第１次提言」で記述が多いのは、これまでの基本コンセプトと今日議論いただいた推進体制等のところであり、これらが厚く書かれると思う。重点施策のところは、まだ議論できると考える。

→　枠組みのところで、横断４領域を前提としているが、これが８というのであれば、今回言っておく必要がある。大括りで枠組として出した上で重点施策として考えるべきではないか、というような話は、今回書いておく方がよい。政府機関や重要インフラで、こうしろというような細かい議論は、例になってくるというイメージである。

→　今回の重点施策の大括りな枠組として、「第１次情報セキュリティ計画」で書ききれなかったものとして事後評価をどうするか、政策の事後評価、社会でおきたことの事後評価、いわゆるポスト・モーテム系のところをどうするか、他のフレームワークを含めて整理しきれていない。それはどうしたらいいか、事務局として問題意識はある。もう一つは、リスクアセスメントをどうするか、何箇所か少しだけ芽は出ているが、今のところクエスチョンマークである。それを書くかどうかは、提言案をまとめていく段階で考えていきたい。

○　電子政府の全体最適化に情報セキュリティの視点を加えて推進すべきではないか、とある。情報セキュリティは重視されていると思っているが、どのようなものが足りないのか。

→　最適化計画は、費用を含め無駄を排することが目的であり、設計段階からセキュリティを組み込んで電子政府の構築を考えるところがメインでは入っていない。今後は、IT 担当室、総務省と話をして視野に入れていただきたいということで書いている。

→　政府全体の最適化は、府省共通の規模の大きいシステム、省内の中でも大規模なシステムが対象となって進められている。個別の課が持つシステム、網から外れてしまうシステムがある。そこまで含めて考えると、小さなところでセキュリティ上の課題があるのではないか、そのようなものを今後どう捉えていくのか、次のステップで考えていくべきではないかという思いがある。

○　最適化計画との連携はしていただきたいと思っている。最適化計画は、良し悪しは別にして、設計書レベルまで定義して、それでデザインすることになっている。情報セキュリティはポリシーがあって、ではインストールしてくださいという状態なので、SBD(Security by Design)の検討を進めていただいて、実際にどうやっていくのかを共通仕様にすることで、各課のシステム等にも導入されていくかと思っている。連携なり、具体化というところで是非お願いしたい。

○　政府機関の情報セキュリティは、目標を定め対策をやってくださいということがやられていると思うが、通常の企業でいう業務監査の機能がほとんどない。業務監査が最良かということは検討の余地があるが、各省のPDCAのチェックのところが弱いと感じている。内部監査機関は評価だけではなく、組織の中でアドバイスも行う。そういったものを含めた機能があれば、もう少し機能するのではないか。各省でのチェック機能をどう考えていくかが重要である。

○　この部分に関する資料の記述が、委員会初期段階のオープンクエスチョンのままになっているのは如何かと思う。各府省庁はPDCAサイクルに取り掛かったばかりで「確立したとは言えずなお課題が多い」とか、機密性を中心に始めたが「完全性・可用性の対策はこれからだ」、とかは、議論の中でクリアになってきた。重要インフラについては、「不特定多数の顧客に大きな影響を与える重要障害はゼロにする」と書くか、「迅速な復旧と再発防止策を取る」ということを中心に書くか、例示とはいえ、最初と変わらない素朴な疑問形のまま列挙せず、議論を適切に反映した形で記載して欲しい。

○　ある省庁の最適化計画に関わったが、PDCAサイクルはそれなりに考えており、セキュリティもそれなりに考えてはいる。しかし、GMPOの移行はほとんど考えていない。言っても聞いてくれない。やはり機能強化は必要である。

○　評価をするとき、情報セキュリティ対策はコストがどれくらいかかり、どれくらいのレベルが達成されるかは、なかなか説明ができていない。分かりやすい説明の仕方を出さないと、現下の状況では進まないのではないか。うちの社内でも、何故そこまでやるのか、何故そこまでお金がかかるのか、という話になる。何を達成するのにどのくらい必要かということをきちんと示す手法を見せないと、進まないのではないか。

→　情報セキュリティを全くやっていない段階で新たなことをやろうとするとコストと情報セキュリティ対策のファンクションの関係は、一瞬だけきれいに見える。しかし、システムを組み込み始めると、他の要素、教育やサプライをどうするか、システムの設計をどうするかというところに沈み込んでしまう。政府システムのことだけについて言えば、ミレニアムプロジェクトで作ったときは見えていたが、EAになっていくつか改修を始めたところで、だいぶ沈み込んでいる。政策予算は見えるが、オペレーションの予算は見えにくくなってきている。原課が握っているシステムは、全くわからない。そこを抜き出さなければ議論できないということを、各省庁とどう議論していくか、考えていかなければならないという意識は、事務局としてある。

→　「沈み込む」という表現は、情報セキュリティ対策のコストが見えない、他の予算の中に紛れ込んでしまう、トータルでシステム一本の中に情報セキュリティは組み込まれているということである。

○　先の委員の意見で、政府が見えるようにする必要があるとあったが、民間もどうしたらよいか分からないのではないか。

→　民間も同じである。アウトソーシングされれば見えるが、情報セキュリティ対策をやればやるほど、システムのファンクションとして上手くインテグレーションされコストの分離が難しくなるのが現実である。そのフェーズに入り始めている。

○　電子政府評価委員会で全府省庁の主要システムの投資コストと運営経費を析出し、分析しているが、おっしゃるように統合的なシステムが多く、見えない。どう分離して計算すればよいか、非常に困る。当初の時点で見える形でやらないと、複雑になってしまう。機能が連結しているため、どこで分離すればよいか分からない。

○　セキュリティシステムはネットワーク構成に関わっており、これだけを分離してお金を出してくれというのは難しい。ただ、どこかで説明責任を果たさなければならない、というのが先の委員意見だと思うが、そこのところは何とか手法が欲しいというのは、切実に思うところである。ROI の形ではないと思っており、どなたか研究していただければよいが、すぐに答えがでるものではないので困っている。説明責任を果たす手法を確立しなければならないことは、確かであると考える。

○　利便性にも関わる問題で、利便性なのか情報セキュリティなのか、何の意味でシステムを構築するのかが、よく分からなくなる。そのため、政策的にも進まず、民間でも悩ましい大きな要因になっている。そこを何とか重点的にやらなければならないのではないか。財政状況をはじめ、いろいろな意味で進まないのかもしれないが、複雑に絡み合っているところがネックになっていると思う。

○　システムを更新しなければリスクに晒されて失われる価値というのが、情報セキュリティの価値ということになると思う。そういう計算をして勧告を出して更新させるなど、新たな手法を言わないと、より安全になると言っても分からない。情報セキュリティというのは、失われた時の損失がどのくらいなるかというのが重要であり、それに対するコストを考えるのが情報セキュリティだと思っている。それを誰が評価するか、事故が起きたときにどういう調査をするかも含めて、きちんと評価できる組織が政府内にあって、勧告なりをできないといけない。事故調査委員会や原子力であれば安全委員会が存在するが、それに対する重点策があった方がよい。

○　ROI という言葉にこだわるわけではないが、指標をつくるということは二つあり、一つは、最初に設計段階でこれだけの合理性を持ってやるから予算執行をしましょう、と言う話。これは企業も同じ話である。もう一つは後での評価であり、ROI は定量的に測って目標を達成しましたよねと議論できるので使う、というパターンが多い。被害がこれだけ出ませんというのを考えたことはあり、最初に想定としてこれだけ危なさそうだから入れましょうという

議論はできるが、それが実際どうだったかということや被害額が予想できない。

○　一定の前提条件を置いて評価し、こういう危険性があるということを提示し、政府などがどう対応するかということを議論する材料を提供する必要があると考える。それの示し方があるのではないか。

○　一つ一つのシステムについて、効果とコストの関係で評価して決めて行く手法もあるが、大規模なシステムの場合、十分な時間と人をかければできると考える。しかし、政府の調達物品とか、提供しなければならないシステムは、小さなものが多いので、その一つ一つについて、担当者も十分育っていない状況で行うのは困難ではないか。ある程度類型化し、例えば暗号方式であれば64bit でやると危殆化、今のコンピュータの能力では64bit では不足であり128bit の暗号を使うほうが良い、ということを専門的・技術的観点から常にウォッチングして基準をメンテナンスし、アドバイスできる人が必要であると考える。そういうものがNISC やNIST のようなもので実現されるのであれば、非常に意義深いことである。法律を作っていては間に合わない。どんどん時代は変わっていくのであり、時代に追従するためには、費用と効果のバランスを考えると世の中一般的にはここまでやっておくべき、ということを表明する権威のある機関が必要なのではないかと思う。一つ一つについて議論していくのは、大変ではないかと思う。

○　今日の議論は事務局でまとめ、「第１次提言」に反映させていただきたい。どうしても言っておきたいことがある場合、事務局までメールで意見を送っていただきたい。

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 －