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４回会合議事要旨

１．日　時

平成 20 年３月 19 日（火）　13 時 00 分～16 時 00 分

２．場　所

内閣府本府　地下講堂

３．出席者

【政策会議有識者構成員】

江畑　謙介	構成員	拓殖大学客員教授／軍事評論家
野原　佐和子	構成員	株式会社イプシ・マーケティング研究所代表取締役社長
前田　雅英	構成員	首都大学東京教授
村井　純	構成員	慶應義塾大学教授

（五十音順）

【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
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
神保　謙	委員	慶應義塾大学総合政策学部専任講師
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）
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) 第２次情報セキュリティ基本計画の検討範囲の設定について

○　第２次情報セキュリティ基本計画の検討の方向性に関する希望であるが、情報セキュリティ政策の様な「守り」のものは、担当者が考えれば考えるほど対策が行き過ぎてしまうと感じることがある。手取り足取りではなく、関係者一人一人が主体的かつ自主的に対策できるようにすることが重要ではないか。

○　情報セキュリティの議論をしていると、ついつい幅広い範囲の議論をしがちである。余り広がりすぎない範囲で対策をすることが重要ではないか。情報セキュリティ政策で何でも解決しようとするのは困難ではないか。

○　個人について。情報セキュリティとは、情報と情報システムの安全を考えていくことであるが、現在のように様々な社会基盤が情報システムに依存してくるような状況下では、装置に対する安心等を大きな機能システムとして考えることが重要。インターネットやデジタル化の基盤が発展してきている中で、アクセシビリティやデジタル・ディバイドの問題は、世界的にも大きな課題になっている。基盤へのインターフェイスが非常に発展してきている一方、情報弱者がシステムを使うことを考慮し、特殊なインターフェイスになっている部分でも情報セキュリティをしっかりとチェックすることが必要である。平均的なビジネスマンが情報システムを使用するようなイメージだけにとらわれていると、こうした視点が大きく漏れてくるが、人の多様性をきちんと検討しているか。各分野別の対策を縦軸だとすると、私が言っている問題は、各分野を横串でつらぬく項目であり、各分野に対してチェックを行わなければならないと思う。

→　事務局としては、論点の一つになると認識。今日の論点ではないが、政策の方向性を議論する際、議論する中身の一つになるのではないか。

○　CEPTOAR は、ある分野における対応と緊急時の対応方法に関するポータルサイトとしての役割を果たしながら情報集約点になり、必ず役に立つ情報が常に網羅されている組織であるべきだと思っているが、その認識は正しいか。また、本当にそうしたものは出来つつあるのか。作ろうという議論は続いているが、知っている限り、それがきちんと整備されているとは聞いていない。今どうなっているのか、具体的に現状並びに経過報告をしていただきたい。

→　事務局としても、CEPTOAR は情報集約センターであると認識しているが、実際に活発な情報共有が出来る段階には至っていない。これから徐々に関係者の理解を求めていく状況。

→ CEPTOAR のカスタマーについて、第一義的には重要インフラ業界の人自身である。その次は、重要インフラの他の領域の人であり、その次に国民である。現在、キャパシティの問題があり、情報の共有・提供の何れについても均一に求められていない。また、業界間の情報共有については、株主や市場に対する企業体としての活動を考慮したとき、どうしても限界がある。真摯に取り組んでいるところではあるが、ハードルは高い。業界の御理解を得つつ少しずつ進めており、後退はしていない。

○ CEPTOAR が米国の ISAC と異なることは十分承知している。また、情報共有する上でのハードルが高いことも理解できるが、情報共有が情報セキュリティ政策の核になることを考えると、最新の情報を、どの部分をどのくらいの粒度で、どの程度のリアルタイム性を持って共有できるかということがやはり重要であると考える。CEPTOAR の評価のレトリックも情報共有されるべきであり、評価を含めた現状報告を定期的にしていただく必要があるのではないか。

○ 人材の件であるが、そもそも情報セキュリティにおける高度人材の定義づけは、大変難しい問題である。情報セキュリティは非常に難しい分野であり、コンピュータサイエンスやネットワークの分野で非常に優れた人間が情報セキュリティ分野の技術者になっているという認識がある。高度な人材を育てるのはかなり難しい問題であり、人材をどのように確保するか、体系的にシステムが確立されていない場合、持続性が問題になってくる。具体的にどのような目標で何を実施するのか、ということを考える必要があるが、現在の進捗状況をうかがいたい。

→ 必要な人材の資格について、民間で体系化を図っているところ。

→ 少なくともセキュリティの人材については、元々は情報システムに関する人材もセキュリティに関与しているが、元々大学や人材育成の流れで要求していた requirement と、情報システムに携わる高度人材に求められる requirement が変わりつつあるので、この requirement の明確化とこれを社会に提示することが、現在政府側で行っていることである。

○ 人材について。午前中、IT 新改革戦略評価専門調査会が開かれて、IT 戦略本部に提出するものを委員として決議してきたが、IT 高度人材特にセキュリティに関する部分は、御指摘のとおり難しいところである。少なくとも開発する人材、高度に利用出来る人材、企業などで言えば CIO が CISO でなければならないということであろうと思うが、業務がよくわかっていて IT を上手く使いこなせるようにする教育には、かなり力を入れていかなければならない。このあたりについては、奈良先端科学技術大学院大学でやっているが、この成果がどうなるかについては注目していきたいし、NISC でも見ていっていただきたい。

○ 重要インフラ対策については、それなりの成果があったと認識している。第２次においてもそれを踏まえつつ、革命的なものよりは一歩ずつ前に出ることが重要ではないか。これから議論がよけいに拡散していくと思うので、その中で、内閣官房情報セキュリティセンターでやれることを選ぶ。姿勢として、具体的に国民が、やはり一番多い国民にとって困った問題を政府として解決するという視点が重要になってくるのではないか。

○　国民目線で行くというということは非常に重要。実際に国民が困っていることが予測されるリスクに対する対応は重要であると思う。

○　資料中「CIA（機密性・完全性・可用性）」とある。先ほどの説明では、恐らく情報に関する機密性・完全性・可用性について議論すると理解したが、それでよいか。換言すると、情報に関する機密性・完全性・可用性であるとか、BCP、あるいは公共性や市場性などの軸があるが、何を守るのかと言うことについて、私の理解は正しいか。

→　情報資産を守るという点では、御理解のとおり。ただし、情報セキュリティ政策については、マネジメントとしての機密性・完全性・可用性に限らず、BCP やプライバシーなど様々な視点がある。議論に際しては、様々な視点について考えていくべきと考えている。

○　確かに、色々な視点を考える必要があるが、検討範囲が広すぎるとぼやけてしまうという問題もある。マネジメントという言葉は機密性・完全性・可用性だけではないので、まず最初は広めに考えることとし、扱う情報なり情報資産、関連資産を守るという題目のもとで様々な要素を切っていく。恐らく重要インフラや企業など、切り方によって見え方は異なってくる。そのなかで課題が見えてくると思うが、それが今回の基本計画の政策になってくるのではないか。

→　御指摘のとおり、様々な切り口で切って課題が出てきて、それが政策になる。各論の議論を通じ、政策の範囲が決まってくると思うが、今の時点であまり抽象的に詰めても生産的ではないので、後ほど議論することとし、そのときに振り返る形で良いのではないかと考えている。

○　第１次計画の時は、情報セキュリティに関して根源的な不安があり、概観した形で政策が進められていたと思うが、現在は、根源的というよりは個別的なものが多いという印象。国民に対する計画であることを考えたとき、検討に際しては、あまり視点を絞ると国民一人一人に対し何をやる施策であるのかが判らなくなると感じている。

○　ATM の停止やコンピュータウィルスなどの細かい問題が身近に存在する一方で、政策会議が大上段に振りかぶったところだけやるというのでは、政策と国民が乖離しうまくいかないのではないか。いろいろな切り口に沿って個別の課題に対する取り組みを拾い、関係省庁がどのような手段で解決するのかというのを示すことが計画の基本ではないか。

○　議論が拡散しないよう、検討に際し視点を絞るということと、色々な切り口に沿って個別の課題を拾うことは、矛盾しないと考える。演繹と帰納は相互に重なり合いながら動くので、まとめるとしても、結局、具体の部分が出てくる。違法有害情報を例にすると、国民からすれば、ネットの安全性と言えば違法有害情報の問題を一番強く意識するということが出てくる。つまり、第２次基本計画を検討する委員会としては、第１次計画からの変更部分に関する、全体としての大きな方向性を提示することになると思うが、その時の視点として、個別の課題があり、最終的に大多数の国民にとって IT が使いやすいものにすることが必要である。機密性・完全性・可用性に限定するような形での議論には抵抗感があり、軸にするとしても、その周辺についても絡め取りながら進めてもらいたい。

○　但し、具体的な問題を全部出し、「ジクソーパズルをうまくはめ込むにはどうしたら良いか」というようなやり方だけに陥らないようにする必要がある。

○　国民目線でわかるところから入っていくと、色々なことと関係が出てくるが、その関係図を相関的にとらえなければならない。これが体系的な発想にも繋がるが、その関係図を描くことが、基本計画検討委員会の重要な任務になるのではないか。

○　経済・生活・安全保障を柱に建てるということであるが、特に安全保障と外交に関する事項について、前回外務省から「特殊な情報セキュリティについては、当該省庁が情報の性格に応じて対策をやるべきであり、全体の議論にはなじまない。」という意見があったことに若干の驚きと失望を感じている。例えば、法務省や警察庁が国際連携の中で進めている犯罪者データのネットワーク化や防衛省が日米で進めている情報の統合化という話をこの委員会で検討するのは確かに筋違いであるが、少なくとも様々な情報基盤を国際連携の中で対外的に依存しながら、様々な国民の生活や安全保障に対する情報のレベルを高めていく時代が来ているなか、例えば法務省、警察庁、外務省の情報セキュリティのレベルが十分でないと、対外的に非常に大きな迷惑をかける時代になっている。すなわち、セキュリティのレベルをどのように保つかということと、それに対する機密性の分類がしっかりされ、アクセス権限を明確に分け、情報公開制度に対する公開のレベルをどこまで定めるかということに対する国民の理解、社会的なコンセンサスを得ることは非常に重要である。これは安全保障・外交の重要な課題であり、この会議において、理念として盛り込むべき大変重要な部分であると考える。

　→　第１次情報セキュリティ基本計画において、安全保障と危機管理の点については、理念だけは書いたものの十分に書ききれなかったため、事務局として後悔していた。第１次基本計画策定の時には、安全保障領域の情報システム、情報ネットワークあるいは情報資産の価値の認定等が希薄だったという事情もある。現在は状況が変わっているので、本日ではないにせよ、しっかり議論がなされることを期待したい。

○　外務省の意見については、外交秘密の保秘の問題と情報セキュリティ対策の問題を混同しているという印象。いささか筋違いではないかと思う。

○　個別のテーマで問題点があるなか、これを抽出し、絡まっているところを整理して示せればよいが、おそらく上手く行かないのではないか。世の中は意外と繋がっていない。例えば、数年前にWinny騒ぎがあり公用パソコンを導入したものの、データを自宅に持ち帰れるのでイージス艦情報の漏えいが発生したという話があるが、個別の部署がネットやパソコンを利用したときの危険をいかに予測し対処するかということを個別的に、かなりきめ細かく拾う必要があるのではないか。この計画の段階でどこまで言うかは調整が必要であるが、かなり目配りをしないと、理念的であるだけにおかしな方向に行くこともあり得る。理念も重要だが、バランスが重要であることを指摘しておきたい。

　→　防衛省の例について、事務局から若干説明させていただくと、公用パソコン導入後の情報流出は、公用パソコンを導入する前の段階で持ち出されていた情報。現在は各個人の自宅まで行ってチェックしている。この問題は、情報に対する意識や相互に教えあっ

て知識を深める、自宅に情報を持ち帰って仕事や勉強をする等の風潮がITの時代に合わなくなったというところに大きな問題がある。また、持っていないと言われれば、それ以上踏み込んで調査することは出来ない。色々なレベルの個人の意識の問題、組織風土の問題、制度の問題等いろいろな要素が入っているが、我々としても取り組んで行きたいと考えている。

○　議論の視点を絞るか否かについては、以前から申し上げているとおり、議論にメリハリをつけ、重要性に応じて議論する必要があると考えている。

○　国民目線に立って身近な問題を抽出し列挙すること自体は良いかもしれないが、個別テーマをそのまま並記することには反対だ。この委員会では、「一般国民には分からないが、実は国民の生命・安全・財産に深く関わっている重要インフラや政府の対策がどうなっているか」、あるいは、「大規模な事件・事故が発生した際にどう対処するのか」を取り上げることの方が、重要度が高いのではないか。すなわち、議論の中核には、「本当は重要だが総体的に脆弱なもの」を見極めたうえで据えることが適当と考える。そして、今までの議論を見る限り、最優先は政府機関ではないかと思える。政府機関の対応が現在どうなっていて、それをどのように改善するのか、という辺りを中心に議論した方が良いのではないか。

○　計画を策定していくなかで事務局がやらなければいけない作業は、問題点を抽出した後、それを直接内閣官房が各府省庁と行うか、外に任せるか、当面手をつけないことにするか、振り分けることである。事務局としては、この優先順位付けに議論が収れんしていけば良いと考えている。そこには、市場性に任せればよいものもあれば、公的対応が必要な部分もある。また、国民から見たときに対応しなければならない部分もあれば、産業界から見たときに対応しなければならない部分もある。このように多様な観点があり、それについての整理整頓を今の段階でできると、今後の議論が発散しなくて良いと考えている。

○　情報セキュリティについては要望が高く、議論しようと思えば何でも議論出来るが、リソースの問題やフォーマリティの問題があり、やりきれない。

○　大枠の議論については、一旦ここで切り上げ、以後の議論において適宜関係づけて議論することとする。

⑵　「確保するべきセキュリティの検討」について

○　切り口はいろいろあるが、具体的な対策が進んでいない状況では、「機密性・完全性・可用性」という基本に尽きるのではないかと思う。また、可用性の発展したものが事業継続計画であると考えれば、議論を展開し易い。

○　最初に御説明のあった政府機関の評価内容を見ていると、機密性の面ばかりに取り組んでいる印象がある。他方、これまでの議論では、可用性の方が重要であると指摘する声が多い。また、金融機関を例に、実際に日々発生しているシステム上の問題を分類すれば、イメージ的には機密性・完全性・可用性は１：１：８くらいで、８割程度が可用性に関する事項とみられる。そうした構造が他の機関でも同様とすれば、可用性や事業継続に関する問題を議論の中核に据えるべきではないかと認識している。質問になるが、政府機関においては、可用

性よりも機密性の方が重要との判断に基づいた調査結果なのか。

→　機密性が一番取り組みやすいため、機密性から取り組んでいる。可用性の重要性は認識しているが、予算編成の問題と直面する。可用性のマネジメント、業務継続計画については、出来ていないことも多く、また、予算制度上の問題もある。必要性は認識しているが、予算獲得に結びつけるには至っていない。

→　中央防災会議が出している業務継続計画に関するガイドラインに従い、必要なシステムについてはバックアップがなされているという例はあるが、過剰投資の面もあり、一定の統一的な方針を示す必要性は感じている。

→　なお、今回の計画は、政府機関対策だけではなく、社会全体を対象としている。政府機関対策に関しては、可用性が重要であるが、社会全体でも可用性が一番重要という訳ではないことに留意する必要がある。

○　機密性・完全性・可用性については、守るべき対象が何かにより、どれに重点を置くかの答えが違ってくる。例えば、情報そのものを守る時には、漏れては絶対にいけない以上、可用性より機密性を重視することになる。他方、システムそのものを考えた場合、システムの属性により異なるが、機密性より可用性に重点が置かれるものもある。この辺りを分類しないと議論しにくくなり、あるいは議論が発散する。まずは守るべき対象について、情報資産そのものか情報システムか、いくつか類型化したうえで、どのような脅威から守るのかということを具体化し議論していかないと、具体的な対策を考えにくいのではないか。

○　情報資産を守るのが目的で、情報システムはその手段であると位置づけてしまうと、専ら、情報資産の機密性・可用性を情報システムの側で分担することになり、結果、どれだけやっても可用性を担保出来ないのではないか、という意味のない議論になってしまうのではないか。

○　機密性・完全性・可用性の重点配分については、分野や分類により変わってくるという意見に同意。とすれば、この議論については、後ほど戻ってくることになると考えている。先ほど、「情報資産の機密性・完全性・可用性か、情報システムか、マネジメントか」という指摘があったが、それぞれで異なってくると思うので、基本的には「仮置き」で次に進めていただきたい。そうしないと、何のための基本計画かわからなくなってくる。

○　これは細かい議論になったときに取り上げてもらえばと思うが、切り口という点では、機密性・完全性・可用性というのはOECDにおけるセキュリティの定義であると思うが、その他にもいくつかの定義がある。様々な側面で様々な対象に関わるような形で取り上げてもらえればと。

○　これは整理学の話であるが、一つの情報セキュリティを確保する時の情報セキュリティの特徴で分類する方法があり、公開性の議論などもそのマトリックスに含めることが出来る。しかし、機密性・完全性・可用性（CIA）とは別の切り口があったときには、それは同じ軸に並べるべきではないと考える。「何に対するCIAプラスαか」という構造で整理すべきではないか。

○　情報セキュリティだけを見ていると、狭い範囲の議論に深入りすることになる。情報セキ

ュリティはリスクマネジメントの中の一つの要素であり、リスクマネジメントとしてどういうリスクレベルがあるのか、リスクコントロールをどのようにしていけばよいか、という観点から見ていく方が整理しやすいのではないか。

○　第１次情報セキュリティ基本計画では、「安全・安心」が目的・目標になっている。恐らく、この時には安全・安心への危機感があり、目的・目標が設定されたと認識しているが、対策が進められているなか、この目的・目標でよいのかと考えている。それぞれの分野によって違うのかもしれないが、個人は格別、企業については「安全・安心」だけでセキュリティを語られると、自ら動く「動機付け」にならないのではないか。例えば、可用性を高めることによる効率性の確保、信頼性を保つことによる社会責任の達成など、もう少し具体的な部分まで明らかにするのが良いと考える。それによって、機密性・完全性・可用性のバランスも変わってくるのではないか。

○　貴重な意見が多数出た。この論点については、事務局とも検討し、改めて提案したい。

⑶　「他分野との関係」について

○　違法有害情報対策については、直接は関係ない部分も多いかとは思うが、関係する部分もある。ここで言う「他分野」の一つに入るのではないか。目配りはしたということを明確にする観点からも、「他分野」の一つに列挙した方がよい。

⑷　「政策推進にあたっての基本的スタンス」について

○　第１次基本計画では、セキュリティに対する国のスタンスは「守り」であったと思うが、もっと「攻め」のスタンス、対策を行うことにより国が豊かになる、他の国と比較してより優位になるという視点が必要ではないか。具体的には、IT の利用・活用の基盤となる機器の開発が考えられる。現在は、ほとんど海外製品である。海外製品の利活用は安全保障とも関係すると思うが、本当に安全か。

○　情報セキュリティというのは、基本的に、豊かでないと対策を取れない。将来的にどうなるかは不明であるが、現実問題として、企業を見てみると、大きな会社やコストがいくらかかっても良いとされる分野の対策は進んでいる反面、競争にさらされているところは厳しい。我が国は豊かにならなければいけないという発想が根底には必要であり、その上での計画作りが必要である。

○　経済・生活・安保という視点に加えて、「個人の意識改革」という視点を入れる必要があるのではないか。IT がこれだけ身の回りにあり、国民生活と密着しているなか、自然災害同様、自助が共助や公助より先にくるという領域に入りつつあると考えている。国の政策で「国民の意識改革」を据えることについては、いろいろな意見があるかもしれないが、視点として無視出来ないのではないかと考えている。

○　重要な視点であり、工夫して言及すべきであると考える。

○　経済・生活・安保という切り口は、「状況」若しくは「活動」に主眼をおいたものであるが、政策推進にあたっての基本的スタンスを考えるうえでは「誰が」という視点、確保するべき情報セキュリティの享有主体という切り口も一方で存在する。具体的には「国」「社会」「個

人」など。この切り口に「活動」を組み合わせるという複層的なスタンスが必要ではないか。

→　第１次情報セキュリティ基本計画では、この基本的な３つの理念に対し、実施主体である４つの主体を掛けて執筆した。

○　経済を重視しなくてはいけないとの意見があったが、情報セキュリティというのは、IT の有効利用を推進するための守る技術ではないか。とすれば、経済・生活・安保という側面で分けられないのではないかと感じている。

→　資料の図では「経済」「生活」「安保」を縦に並べているが、実際には「市場性」という軸が存在し、市場性で語ることが出来る「経済」及びそれと表裏一体の「生活」と、公的対応しか考えられない「安保」という分け方を行った。

○　製品を製作する際、情報セキュリティは儲けられない、儲からないという位置づけであり、多くの力をセキュリティには割けないというスタンスではないか。とすれば、経済だけを見ていても情報セキュリティは確保されないのではないか、市場原理では進まないのではないかと感じている。

→　第１次情報セキュリティ基本計画を策定した際は、情報セキュリティに対して責任を負う主体が過度の責任を負っていないか、国の責任を過度に期待しすぎていないか、という認識があり、官と民との間の役割分担を明確にしたいという考えがあった。その背景の一つには「小さな政府」という考え方があり、市場が設定出来る所は市場に任す方が良いのではないかと考えた。その状況については見直す必要があるかもしれないが、少なくとも当時はそう考えていた。

○　セキュリティ政策の推進に際してのコスト負担を社会で共有できるか、経済的に成り立つ基盤をつくっていく上で、出来ることが何かあるか、民間がやるべきことはあるのか、などを議論していくことが必要であると思う。経済的なレトリックの中でも、コスト負担を盛り込みつつどうやって成長していくか、官、民の役割を織り込んだ形で、基盤を作っていく必要があり、逆に官、民の役割を炙りだしていくことも求められる。経済を度外視したセキュリティ政策は、基本的にあり得ないのではないかと考えている。

○　第１次情報セキュリティ基本計画は、豊かな経済社会生活を守るという側面が前面に出ているが、文化を高め海外に発信する情報自身とその発信の仕組みを守る情報セキュリティ、よりよいものを創造するための情報セキュリティ、という視点を何らかの形で入れられないか。

○　第１次情報セキュリティ基本計画を策定する際、「日本は経済大国で成長する。」、「システムは高信頼である。」、「国民は、トラブルを許容しない頑固者である。」、「政府は間違いを認めない頑固者である。」という考えが土台として存在した。第２次においては、一定のリスク・障害を社会的に許容し一定の被害者が出るかもしれないが、それでも全体として上手く進んでいるならよしとするか、第１次と同じ土台に立つか、選択することが必要であり、事務局として御意見を伺いたいと考えている。

→　無謬性原則を貫くか否かは、次のテーマとも関係してくるので、あわせて議論する。

⑸ 「重点を置く対策段階」について

○　無謬性の議論は、おそらく、事に応じて速やかに対応出来る等の柔軟性が計画にあるかという議論と関連する。ある種の事故調査委員会を作れという議論もあったが、トラブルなどが発生したとき、その対応についてセキュリティ政策会議の専門部会のような組織が意見を言えるようなシステムを盛り込むのであれば、ミスも存在するが速やかに対応できる体制もある、というかたちで盛り込めるのではないか。

○　１次情報セキュリティ基本計画は、いわばみんなで夢や理想を語った「きれいな絵葉書」の様なものであると感じているが、第２次計画を作る意味があるとすれば、「リアルな生写真」になるのではないか。内容面でも「綺麗事はやめて、本音で語る」ということでどうか。例えば重要インフラでは、相当のコストを掛けて障害を起こさないように努力しているが、どれだけ頑張っても障害はゼロにならない。その現実を直視し、一定のリスクは許容した上で対策を考慮する事にした方が、第１次情報セキュリティ基本計画との対称性も明確化できる。ここまで率直な姿勢に転換することには疑問を提起する人がいるかもしれないが、ここは現実に沿った対応が大切ではないか。

→　これを進める場合、説明責任、透明性、コンセンサス形成の仕方などについて、今まで以上に機能を高める必要がある。そのため、これを推進する枠組みについて、今の政府の構造から更に踏み込んで行く必要がある。これについては、事業者も傍観者ではいられなくなるが、御意見を伺いたい。

○　情報セキュリティにかかる費用は、最終的には利用者である国民に、税負担の概念に近いような形式で負担していただくしかないのではないか。セキュアなシステムを無料で享受することは、そう主張する人も多いだろうが、資本主義経済の中では現実性を持たないのではないか。

○　情報セキュリティ対策について、政府において現在出来ていること、出来ていないこと、これから出来ること、出来ないことをきちんと切り分けて国民に説明すれば、完璧に安全であるということに固執しなくても良いのではないか。

○　各個人や組織などは一定程度リスクを保有しながら活動していく、と規定するのが良いと個人的には思っているが、社会的には難しいのではないかと感じている。先ほど、経済・生活・安保とは別に「個人の意識改革」という話があったが、個人に責任をどこまで取ってもらうかというのも、一定程度お願いしなければならないのではないか。

○　企業の中での個人の位置づけ・役割が変わってきているのではないか。最終的には組織としてセキュリティを守っているが、活動は個人で行っており、組織の中において各個人が一定程度の責任を果たしている。日本の文化的には、個人と組織の関係性が若干不明確であったが、これを明確にする必要があるのではないか。個人的には、この部分の整理に踏み込みたいと考えており、意識改革が必要であると考えている。

○　基本的スタンスに書かれている３つの事項は、何れもITが主語である。しかし、これまでの議論を聞く限り、情報セキュリティの主役は情報技術から情報人材や個人の意識という部分にふくらんでいる。第１次ではITを強調したが、今後の基本スタンスを考えるにあたって

は、IT 以外の部分について議論するべき時期に来ているのではないか。

○　第１次情報セキュリティ基本計画の下で取り組んでいることは、そんなに無駄なことではないと思っている。有効性があって良いものは継続して実施すれば良く、不足しているものは不足していると評価すればよい。

○　第２次計画においては、「何か起きたときにどう対応するのか」ということに重点をおく必要がある。事業継続計画を策定できなければ、いくら啓発・教育活動をしていたとしても、トラブル発生時には対応出来なくなる。また、トラブル発生時の対応を重視した場合、プライバシーの問題などは犠牲にならざるを得ないが、やむを得ないと考えている。そして、そのような議論も含めて議論を展開していかないと一般人にはわからないと思われるので、ある程度計画に書き込むべきであると考えている。

→　事業継続計画の策定について、これを推奨するガイドラインが中央防災会議から出ているが、現実にこれを策定している企業は、東証一部上場の 14%に留まっている。これは、コストを許容し得なくなっているのか、あるいは許容しようとしないからではないかと見ているが、事業継続計画の策定を可能にするコスト許容度が我が国の企業にあるのかは、是非お伺いしたい。

○　事業継続計画を策定するコストの許容については、状況が急速に変わってくると認識している。一つの動きはコンプライアンス強化であり、単純なトラブルで社長が辞める時代になっているため、投資せざるを得ない状況になっている。すなわち、大きなトラブルを起こしたときに情報セキュリティ部門なりソフトウェアのバグの責任で片づけるのではなく、会社全体の責任であるということがかなり明快になってきているため、設備・ソフト・ネットワークなど、それを支える要員を含めてどの程度まで対策を実施しておけば社会的に許容されるかというのをかなり真剣に考えており、外部監査人等からもかなり厳しく指摘される要因になっていると認識している。現在は金融機関を除き、余り本気でやっていないが、今後は自分の業種の社会的責任に応じてやらざるを得なくなるのではないか。

○　取り組む企業が増加すればコストは下がるのではないか。

○　コスト負担の議論に関連して。企業は、強制されてやらざるを得なくなったら対策に取り組むことになるが、その際、人件費を抑制する形で予算を捻出することになる。結局、どのような形式を取るとしても、国民に何らかの形でコスト負担をお願いすることになるのであり、BCP を含め要求する情報セキュリティの質をどこに持って行くかによって、コストに関係なく対策のレベルは決まってくるのではないか。

○　トラブル発生時の対応に関する議論を追求していくと、例えば通信回線網や電力網に障害が発生した場合に事業所管省庁が統括して対応すれば何とかなるというものではない以上、内閣官房情報セキュリティセンターの権限と機能の議論をやらざるを得ないのではないか。

○　無謬性を強調すると、トラブルが発生しないことを前提に仕組みを考えてしまうので、思考停止状態に陥ってしまい、問題が発生した時の対策を考えられなくなる。どのようなリスクが発生するかという評価を専門家として行ったうえで対策を立てる、その際、予見可能性の高いリスクに対して対策を打っていない場合は社会的責任を求められる一方、予見可能性

の低いリスクについては、社会もこれを許容し、発生しても社会的混乱が起きない仕組みを構築しなければならないのではないか。できるだけ欠陥のないようには頑張ってはいるものの、これを全くゼロにするのは難しいのではないかと思っているので、問題が発生したときの社会的対応力を作る必要があるのではないか。

○　重点を置く段階については、もちろん準備段階についても従来どおり考える必要があるが、いくら対策をしてもリスクが残る以上、それに対応する対応段階や復帰段階のことを真剣に考えないと社会的責任を果たせないのではないか、従って対応段階や復帰段階にウェイトを置いて考えるべきである、という意見が多い。また、「政策推進にあたっての基本的スタンス」についても様々な意見が出たが、対応段階から議論を遡及した方が結論を出しやすいかもしれない。この方針に基づき、もう一度、次回あたりに議論を詰めていただきたいと考えている。

○　復旧段階・対応段階について議論する際、個人情報保護法などの既存の法規を大前提として議論をすると、身動きが取れなくなるようなこともあり得る。議論に際しては、既存の法規についても相対化して考えてよいのではないかと考えており、引き続き、その方針で積極的に御意見をいただきたい。

⑹　「対策の実施における国内地域性」及び「政策方針」について

○　そもそも、地域との格差問題は社会全体に共通の問題であり、IT はむしろ都市と地域の格差を埋める存在であることを考えると、地域性をここで論点に挙げることには違和感を感じる。「コンサルタントの数が少ない」などの話は全ての産業について言える話であり、この分野に限ったことではない。弱い地域がセキュリティホールになるという考え方もあるが、それを言い出すと議論の対象が世界中に広まってしまい、結局、日本国内での地域問題だけを取り上げる意味がなくなるような気がする。

○　地域性の議論については、情報セキュリティをどういう視点で見るのか、という問題と関連するのではないか。例えば、情報セキュリティは豊かな者だけが守られれば良い、というものであれば、格差の問題を取り上げる必要はないが、情報セキュリティは生活の基本であり、いわば権利の様なものであると考えるのであれば、国は最低限のガイドラインを提示し、それが出来ないところを支援する事が必要ではないかと考える。

○　地域性の観点の存在は理解するが、権利の様なものであると言われても、やはりこの場で地域性の観点を考慮することの重要性が理解できない。

○　全体のリスクマネジメントの中で情報セキュリティ対策が負担とならないようにする必要がある。情報セキュリティのレベルは、コンプライアンスに基づく強制と、安全と信頼による市場の自由競争に基づく経済的な発展分によるコスト負担という総体的なバランスがないとレベルが上がらない。そう考えると、地方部は圧倒的に弱い。市場の力も弱く、コンプライアンスに基づく強制で負担が発生した際に、負担分を軽減するだけの利益を上げることも難しい。コストをリカバーする全体的なメカニズムを考えていく必要がある。

○　情報セキュリティ対策を実施する企業に関与してきたが、コストの議論については、これ

まで出てきた意見に同意。今後、やる気もお金もない者に対しどうやって対策を強いるかという問題があるが、他方、情報セキュリティを進めたため、直接のコスト負担だけではなく、パソコン使用方法の制限に伴う知的生産性の低下も発生しており、競争力強化の面で懸念している。また、海外技術の使用は、非常にコストが高く、対応段階や復帰段階の強化もコストを高くする要因になる。コストの問題、知的生産性低下の問題を解決するような情報セキュリティ対策のやり方を検討する必要がある。そうしないと、弱者対策の問題やコスト負担の問題は、結論の出ない議論に陥る可能性がある。

○　都市と地方の差は、様々な面で存在すると考えられるが、特に情報セキュリティに関して見ると、意識や人材に差があると感じている。企業でも東京にある本店と地方にある支店で違いがある。そして、これまでに発生したやや大きなインシデントは、比較的地方の方から発生する。そのため、不足している部分、意識啓発や人材育成を支援する仕組みを作ることが重要であると認識している。セキュリティレベルについては、都市部と地方部では同じであるべきだが、それを実行するに当たっては、都市部と地方部の差がどうしても発生するため、それをどのように補うかという配慮は必要である。

○　電子自治体の推進に 10 年ほど携わっているが、地方の自治体はどうしても財源が乏しいという現実があり、ASP と SaaS の活用が推進されている。そうすることで都市部と地域の格差、コストの問題の解決を進めなければならない。また、先ほど権利という話があったが、そうであるならば、等しく情報が提供されない社会であってはならず、その基盤を作るという意味でも考えられるのではないか。そして、そのような観点からソリューションを考えていただくと、良い結論が出るのではないかと考えている。重要性が理解出来ないという意見もあったが、この問題は重要な問題として、議論を積極的に継続していきたい。

⑺　「対策実施主体、問題の理解・解決促進主体」及び「具体的政策・対策」について

○　先ほど、コスト負担に加えて知的生産性の低下が発生しているとの指摘があったが、重要な指摘である。SaaS などでシステムのアーキテクチャーを決めてしまうことが結果として生産性の創造的発展の障害になることもありうる。

○　強制的にものごとを決めつけてレベルを上げていく方法は、政策的に十分あり得る方法であるが、そうするとリソースコストの負担が大きくなる。これを軽減できるきちんとした対策主体がこの国には十分に存在するのだろうか。仮に十分には存在しないとすれば、それを議論しなければならない。例えば、米国では NIST のように、政府調達物資に関する一定の基準を決定し、運用段階でのインターオペラビリティのチェックに代表される様々なテストを実施するというような仕組みが整備されることにより、コスト増が押さえられている。同様な体制が我が国にあるか。行政のシステム、政府システムに対して同様の事を実施する体制はあるか。いくつかの国では、政府の関連組織として政府調達基準をチェックする仕組みがあり、このような事が担保されているが、これは、コストを下げる事にも通じる。恐らく民間には存在するだろうが、対策実施主体という視点から鑑みれば、これをどのように盛り込んでいくかが大変重要である。

→　そのような主体は存在せず、大変大きな問題であると認識している。これの大きな問題は、暗号の危胎化に対応する際、どこに危胎化が存在するか、どう評価するか、どう入れ替えを行うか、これらに関するアームが存在しないことである。これを今から考えないといけない。統一的な標準の設定と確認、調達に関して決定する組織が、今のところは存在しない。今後、これを作るかどうかということで、セキュリティ・ベースド・デザインなどを検討しているが、現在、指摘のあったような仕掛け、米国の NIST の様な組織は存在しない。

→　政府調達に関連し、具体的なディテールまで入ったガイドラインをつくり、調達の統制をしていく存在があるかというと、現実には存在しない。

○　米国の NIST の様な組織の形成を促すようなことまで第２次の基本計画に書き込むか否かは、重要な論点になるが、今の話を聞く限り、書き込まないとセキュリティは確保出来ないのではないか。

○　今の議論に関連して。例えば政府機関に関しては、セキュリティポリシーが示されているが、具体的にどうすれば良いのかということで右往左往している。というのも、具体的な製品のスペックやテストが見あたらないため。その意味では、NIST もそうだが、FIPS なども必要であると思う。米国基準の民間企業では既に FIPS を使い始めているが、日本政府では逆にそれが使えない。その意味においても、是非推進して欲しい。

○　若干議論がもどってしまうが、今の議論に関連する話として、第１次情報セキュリティ基本計画はフレームを策定するものであると認識しているが、第２次計画はそれを具体化するものであるという認識を、基本スタンスとして持っていて欲しい。

→　関係づけて書ければと考えている。

○　対策実施主体について、企業を「中小企業」と「大企業」にするという考え方がある。最近まではこのように考えていたが、無理ではないかと感じ始めている。というのも、中小企業をひとまとめにして対策実施主体とすることは、イメージできない。恐らく、情報資産の種類によって対策が決まるのではないか。

○　対策実施主体について、第１次情報セキュリティ基本計画では、直接的な作用が行えるかどうかという観点で、計画の対象となる分野を切り分けている。政府は可能であり、重要インフラは所管法の中身と CSR の観点から部分的に可能である。他方、企業あるいは個人については、なかなか手が届かないという認識を持っている。仮にこれを別の観点で切り分けるとすると、コスト低減をするためのエンフォースをアシストすることが、この計画で可能か問題になってくるのではないか。

○　例えば地方公共団体を見ると、東京都のような大きなものから村役場まで存在し、大企業と中小企業の問題と同じような事が言われている。業種・業態といった具体的中身にもう一歩踏み込めば、どのような対策が可能かといった議論に、もう少し踏み込めるのではないか。例えば、小規模でもセンシティブな情報を扱っている業種、e-コマースサイトなどを扱っている企業と金型を作成している企業とでは、情報セキュリティ対策は全く異なるはずである。

→　情報資産の特性と企業規模でマトリックス表を作成したら良いのではないかという御

意見であると認識した。検討する。

○　取組みが進む主体と遅れがちな主体との格差があるという話があるが、遅れがちな主体について分析を進めていただき、それに応じた分類をしていただく必要があるのではないか。

⑻ 大括りの検討項目（“大括り項目”）の設定について

○　重点政策を検討するに際しては、「レベル分けに応じた対策」が重要な論点になると思われるが、経験上、細かいレベル分けまで決めようとすると、答えの出ない議論をすることになる。また、先ほど「手取り足取りではなく、主体的に対策できるようにすることが重要」との指摘があった通り、モラル・ハザードを起こしたりイノベーションの芽を摘まないよう気をつけることが大事である。したがって、政策の検討に際しては、細かいレベル分け毎に決めていくのは困難であることを踏まえ、先ずは考え方を指し示すのが良い。基準を作る場合には、理想的な「先進対策レベル」と、最低限実施すべき事項である「超ミニマムスタンダード」を決めることまでは何とか可能としても、その中間のレベル分けは、やめた方がよい。そうしないと、技術水準や社会環境が変化する中で、何年間も通用する内容にならない。

○　先日、暗号の関係の ISO の会議があったが、暗号のアルゴリズムについて提案する際、米国は AES を提案し、他の国は他の方式を提案するが、日本は多くの暗号を推奨暗号としている。また、暗号の製品を買う場合、日本の製品ではなく、世界的に広まっていて安い AES の製品を買って使っているところが多い。これは、日本の標準を決めるところがないためであるが、そのような共通の課題、分野ごとに分かれていないような共通の課題については、どの辺りで議論することになるのか。

→　共通の話題については、恐らく、重点政策の枠組みの横断的な情報セキュリティ基盤に関する部分が関係してくると考えている。具体的には、技術戦略の部分で吸収していくことになるのではないか。また、第１次情報セキュリティ基本計画でも「特出し項目」は存在した。

⑼ その他

○　本日、調達に関する議論がなされたが、税金の使途に関する話題であるので、議論に必要なデータや諸外国の例、得失をしっかりと示した上で議論する必要があるのではないか。

⑽ 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。