情報セキュリティ政策会議　基本計画検討委員会
第14回会合議事要旨

１．日　時

平成20年11月5日（水）　16時00分～ 18時40分

２．場　所

内閣府本府　地下１階講堂

３．出席者

【委　員】

有賀　貞一　委員	株式会社ミスミグループ本社代表取締役副社長
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	大成ロテック株式会社常勤監査役
重木　昭信　委員	株式会社ＮＴＴデータ代表取締役副社長執行役員
下村　正洋　委員	ＮＰＯ日本ネットワークセキュリティ協会事務局長
須藤　修　委員	東京大学大学院情報学環・学際情報学府教授
高橋　伸子　委員	生活経済ジャーナリスト
富永　新　委員	日本銀行金融機構局参事役
中尾　康二　委員	テレコム・アイザック推進会議委員（KDDI株式会社情報セキュリティフェロー）
満塩　尚史　委員	環境省情報化統括責任者（ＣＩＯ）補佐官 （各府省情報化統括責任者(CIO)補佐官等連絡会議情報セキュリティワーキンググループリーダー）
宮地　充子　委員	北陸先端科学技術大学院大学情報科学研究科教授・附属図書館長
三輪　信雄　委員	綜合警備保障株式会社参与
和貝　享介　委員	監査法人トーマツ

（五十音順）

【政　府】

内閣官房情報セキュリティセンター
警察庁
総務省
経済産業省
防衛省

４．議事概要

(1) 情報セキュリティ技術戦略の推進について

○　以前の議論で政府における積極的な利用というものがあった。開発したものを市場に出していくことは大変であり、洗練されたところまでもっていくには、時間がかかる。日米を比較すると、米国は市場が１０倍近くあり、製品が出来上がるスピード、市場側の許容性、まあまあでもＯＫといったところがある。日本は、完璧でなければ誰も買わないといった市場性がある。日本では育ちにくい土壌がある。政府がなるべく活用すればという考えがあったが、政府が活用して、それがまあまあの製品、未成熟な製品というわけにも行かないだろう。それを担保しながらも、セキュリティがまあまあなところへ二重化して入れる、テスト的に入れるなど、テストを図りつつ利用するような仕組みがなければ、開発だけを行っても、普及、洗練される、アジアの中での競争力のようなものにはならないと考える。

○　国が率先してこのような取り組みを進めていくことはよいが、日本に閉じたものになってしまう。国際標準に打って出ていき、日本製が主流を占めていくようなところと連携していかなければ、今までの日本の技術開発が世界標準にならなかったという同じ轍を踏むのではないか。是非、そういった戦略を持つということを盛り込んでいただきたい。具体的には、こういった研究開発から出てきたプロトコルなどを早い内から国際の場に持っていき主導していくということである。

○　日本企業、製品が海外に出て行きやすいサポートを、国際摩擦にならない範囲で行うことが必要ではないか。米国やヨーロッパへ、ベンチャー企業の製品、大企業の製品が進出できるようなサポート体制を作っていくということが盛り込まれているよいのではないか。

○　標準化について、この前のＷＴＳＡに参加し、いろいろと感じたところがある。随分前の標準化というものは、標準化の方向性や方式が出来上がって、「ふーん」と言う人と、実際に使う人と両方あり、「ふーん」と置いておく人たちが多かった。標準にすることと、国や地域のいろいろな活動を連携させ、ビジネス等の展開を図る人たちが増えてきていると感じる。ある良いこと、開発物を生成して日本で活用するということが国際的に上手く展開できるような仕組みが一つのキーワードになるのではないか。国際連携のところに書かれるとインパクトがあるかもしれない。標準化は技術のフォーマット、メカニズムを決めるということだけではなくなってきている。コラボレーションということが重要になってくる。先の委員の意見はよく理解できる。

○　技術戦略推進の方向性はよいと思う。進める主体はこのＮＩＳＣになるのか。どこが行うのかがよく分からない。

⇒技術戦略の推進に限るものではないが、この計画は政府の計画になる。もちろん政府が環境を作り、他の主体に何かしていただくという期待の部分もあるが、基本的には政府ということになる。

○　具体的な話については、主体を明確にしておかなければ、結局はなかなか進まないということになる。それぞれ個別に決めていくことになるとは思うが、どこがプランし、進めるかということを明確にできるとよいのではないか。そうすれば、必ず成果は出てくる。

⇒基本計画にはそこまで記述しないが、基本計画を受けて年次計画を作ろうとしている。今までの第１次情報セキュリティ基本計画では、セキュアジャパンを作成している。そこでは、誰が、いつまでに、何をするかを記載している。

○　先の委員のご意見にあった政府が積極的に活用していくことについて、テストベッドということが重要になると考える。まだ、改良を加える余地があるものにも、手を出さなくてはならなくなるかもしれない。それはグランドチャレンジ型の研究開発に関係するのではないかと思うが、そこへテストベッド等も絡めていければよいと個人的には思う。そこまで、踏み込まなければ、市場での普及は図れない。

○　あるべき姿として、設計段階からセキュリティを作り込む開発手法の普及と定着とあるが、これは是非お願いしたい。これは合理的なアプローチの一つであると思っている。具体的な取組みの方向性を見ると、このことに対応する記述が薄いと感じる。開発手法は開発されているというスタンスかもしれないが、記述が弱いと感じている。作り込む開発手法の開発自身があるべきだと思う。それが、開発プロセスとなり、ＩＴリスクの形式的な表記方式や定量的な評価方式をどのように使っていくかを開発しなければならないと思っている。具体的な取り組むべき方向性へ入れていただきたい。

○　“ＩＴリスク”とあるが、リスクの前に“ＩＴ”とあるのは、特にＩＴを取り上げたいということか。また、テストベッドという表現で、例示のあるマルウェアのデータベース、ウイルス実証実験のテストベッドは、今もないことはなく、ＮＩＣＴでもかなりやらており、作りが非常にセンシティブで、大変なものである。ＩＰｖ６のテストベッド環境をつくるなどもう少し入りやすいものがよいのではないか。これを挙げられている根拠はあるのか。

⇒この例は、技術戦略専門委員会で例として挙げられたものである。扱いは難しい面もあり、例として適切か考えなければならない。ＩＴリスクについては、ＩＴを付すことにより、範囲を狭めようというものではない。情報セキュリティに関わるリスクということでＩＴを付したが、表現が適切でなければ考えさせていただきたい。

○　ＩＴリスクは、ＩＳＯ１５４０８のようなシステムのセキュリティ、脆弱性のようなものに思えてしまう。今述べられたようなことであれば、セキュリティリスク或いは単にリスクとされても問題ない。

○　今頂いた意見については、事務局で整理の上、盛り込めるものについては盛り込ませていただきたい。まだ、御意見ある方は、事務局へメール等でお寄せいただきたい。

(2) 情報セキュリティ人材の育成・確保について

○　政府機関における人材の確保ということで挙げられているが、政府機関だけではなく、情報セキュリティに関わる業務に携わる人物は、ある程度資格を持っていなければならないというようにしていかなければ、必要性も生じてこないのではないか。

⇒３年間の期間で実現できるかは分からないが、政府がある程度の資格、能力を求めることにより、米国などではそのようだが、民間の方に普及していくのではないかと考えている。政府が一定の能力を要求すれば、ＩＴベンダー等の民間企業もそのような能力が必要になってくる。そういった染み出し効果を狙っている。また、世の中全体としても、業務と資格・教育制度がしっかりと対応するものが作れればよいということで記述している部分もある。

○　今のままでは、資格を持っている人、持っていない人も業務に携われるようになっている。資格を持っていなければ携われない、資格を持っていれば何級以上になれるなどといったことが必要ではないか。

⇒ここでは、そこまで資格によって政府組織に規制をかけるというイメージではない。そこまで行くことは硬直的で、政府組織や民間でも自主的に資格をとる、そのようにしたいという制度を作っていきたいということである。

○　まずは政府からということもあるだろうが、民間についても具体的な取組みの記述があってもよいのではないか。政府機関の取組みをみていると、まだ取組み初めという印象がある。まずは検証をして、というレベルだと思っている。このような話では、インセンテ

ィブはあるのかということになってくると思う。組織の義務としてやらなければならないということにはなるかと思うが、インセンティブについての話が見えてこない。民間で言えば、キャリアアップのプロセスがきちんと見えるということになる。難しいということは、重々承知しているがインセンティブという視点が欲しい。

○　セキュリティ資格と業務の結合の推進については、明示や明確化によって、情報セキュリティ資格者が何をやる人か、どういうことをできる人かということが分かるということだと思うが、人材を増やしていくというイメージ、奨励していくということを考えるのであれば、インセンティブ的なものを考えなければならないと思う。

○　ここでいうインセンティブとは、具体的には金銭的なものか、プロモーション的なものか。

○　民間では、金銭的なものとプロモーションだと思う。基本計画にどこまで書けるかということはあるが、具体的にはやった方がよい。

○　あるべき姿は２０１２年、３年後を想定しているのか。

⇒基本的には次期の基本計画が終わる、２０１１年の後、その辺りを考えている。

○　そう考えると、姿として“環境整備が行われ始めている”などの書きぶりだが、スピードが遅すぎるという印象である。政府機関としてはいろいろな事情があり、この程度のタイムラグはあるかとは思うが、現場としてはこれでは遅いのではないかと感じる。

○　人材育成に関しては、民間に対する支援策がいるだろう。支援策については、もっと具体的なものを考えていくべきだろう。例えば、企業が資格取得を推進していくための費用の助成などである。

⇒人材に関する委員会でも議論があったが、法律による必置資格などは、規制の一環にもなるのでやりにくいという議論もあった。失業者対策等では、失業者に対して、再雇用機会を得るための教育に関してはお金が出すといったものはある。セキュリティに関しては難しい部分があるのではないか。政府で資格を活用するということはあるかもしれないが、民間で資格を持った人がいなければダメだというのは規制論になる。この国の政策を見たときに、今、必置資格というものは人の生命に関わるような分野に多く、また必置資格は減る方向にあるのではないか。

○　政府が、調達側、買う側としてそれはできるが、民間へ危険物取扱責任者のような形でやるのは反対である。一義的には決められない。日本のＩＴセキュリティ、ＩＴ技術者のレベルを上げていくための支援策は必要である。教育の支援といったものがあってもよいのではないか。

○　人を育てるのはよいが、各省庁に何年も情報セキュリティを行う人が必要との議論があったが、本当にそういった形が成立するのかということが素朴な疑問としてある。また、各省庁に、これだけ資格がある人を雇って行けるのかということも、不可解な感じがする。霞ヶ関のビルなども、財務省の管財局がまとめて作るなど、政府内でアウトソーシングのようなことがしっかり行われている。何年も同じところに情報セキュリティを行う人材を確保することは、効率が悪く、各省庁でバラバラに行い、金も掛かり、どのように処遇してよいか分からない人材が増えるのではないか。天下りのような、腐敗や不健全の温床になりそうなシステムは根本から考え直す必要もあるのではないか。

⇒今までの流れからすると、政府はあまりにも情報セキュリティについて知らない人ばかりであり、知識のレベルがまだ低いというのが皆さんの見解である。外部の人材の活用も含めて、やらなければならない。一つのシステムを作る際の発注にあたり、全く能力のないまま発注をしては、相手の言うままになり、高いシステムを作ることになる。あるいは、作る側が善意で作ろうとしても、やりたいことが分からず作れないということがある。政府の人材の能力を高めなければならないというのは、我々の希望認識である。外部の人材に頼れるところがあれば、是非頼ってアウトソーシングをしたいということはあるが、全てアウトソーシングを行って業務が回るかといえば、回らない。もう少し能力のある人材が政府の普通の、それは任期付でもよいかもしれないが、公務員としているということが重要である。

○　政府内のアウトソーシングということでは、霞ヶ関の建物についても政府内でアウトソーシングを行っており、政府内の適切な部署が所轄官庁と協議して作っていく。ＩＴだけが違う方式を取らなければならないかという、説得力がまずない。各省庁がそれだけの人材を抱え込んでやることが、効率的だとは思わない。ＩＴセキュリティ部門に１０年も、２０年もいて、役所の中のもの全てに詳しくなるという話があったが、役所の方に伺っても、１０年役所にいたとしても、他の部署のことは何も分からない。政府内でアウトソーシングを行うという体制にし、一箇所に相当優秀な人を集めて、一定レベルをクリアしているかチェックする、アウトソーシング的なコンサルティングを行い、しっかり発注ができるという仕組みを考えなければならない。各省庁がバラバラに人材を確保するというパターンで行くと、第１次と変わらない結果になるのではないか。

⇒国土交通省が官庁営繕で省庁の建物を作っており、ＩＴについてもそのような形で調達する、政府内で他の部署にアウトソーシングするというご趣旨だと理解する。ＩＴは、業務フローとの関係が強く、個別性が高いと言われている。パッケージ化や共通化ができないかという話もあり、人事、会計などある程度共通的なものは政府共通的に行うということで、ＩＴ室の方で、そういった合理化を進めているところである。それ以外の個別部分は外に切り出しにくいところがある。とは言え、役人がプログラムを書くわけではなく、ＩＴベンダー等の外部に委託することになるため、委託は行い、アウトソーシングについてはＳａａＳなど行えるものは行っていく。魂を売ってはいけないという議論が過去にあったが、分かる人間がいなければ、仕様書など細かく書けないため、そこは内部で確保しなければならない。

○　純粋に技術的なことを分かっている、或いは業務を分かっているアウトソーサーの２種類がある。業務系のことはＣＩＯというよりは、ＣＩＳＯといった役割になる。その辺の職務のあり方も今後考えていかなければならない。ＣＩＯの役割は調達仕様書の作成や、日本はそこまでの権限は与えられていないが予算も扱う。

○　政府機関や各省庁は、企業に喩えるならば、大企業や重要企業のように、それぞれが相当重要なことを行っており、情報もかなり重要なものを抱えている。そのような前提に立てば、「重要な業務・システム等のコアの部分は自分で面倒を見る」というスタンスに立つのが適切である。このような委員会ができ議論しているのも、政府機関の情報セキュリティやＩＴが重要であるとの前提に立っているからではないか。一方でコアでない、非重要な、誰でもでき、共通化できるようなものは、どこかがまとめて面倒を見ることがあってもよいと思う。霞ヶ関のビル工事とＩＴを一緒に論じていただきたくない。ＩＴはそれぞれの省庁毎に独自性というものがなければならないはずである。仮にビルのように共通化してしまえるということなら、「省庁を再編・統合してしまえばよい」といった議論にまで飛んでしまうのではないか。

○　人材について、人を雇ってくる或いは資格といったものと、外部委託で仕事をやってもらうという形を考えられているが、民間では出向という形があるのではないか。セキュリティ技術に関する知識や経験をもった企業に人を出し、自分で手を動かしてやるということがあれば技術的なものは比較的短期間に習得できると考える。例えば、ある期間、人を出し、戻ってきて、政府機関の中でそれを活かせば、実質的なことはできるのではないか。

○　脅威に対抗しようとすれば、かなり高度な人材がいる。これを各部門、各組織でそろえようとすれば、かなり大変だという議論になる。技術的には脅威をアイソレートし、サービスモデル化して提供するような仕組みをつくることも、グランドチャレンジである。イ

ンターネット環境で晒されている諸々の脅威があり、システムを作り込む際の脆弱性の問題がある。後者は難しい部分があるが、前者について何とかアイソレートし、それを防ぐためのサービスメニューを作ることは、進んでいるようで意外と進んでいない。そういうものをしっかり育て、そこでの人材はそれぞれで一生懸命育てるというより、そういったサービスを使うという方向にもっていくということは、技術のチャレンジと人材の育成が両方相俟って、いろいろなことができる。システムの脆弱性については、そういう人材を育成する必要があるが、システム構築のアウトソースも含め外出しできないか。我々が考える以上に、サービス、アウトソース化、メニュー化は急速に進むのではないかと考える。それらに対しいろいろと配慮した方向にしておかなければならない。

○　姿としては、米国のように何人も資格者を持っているというよりは、人材教育を始めましたという状況ではないかと正直思っている。情報セキュリティポリシーのガイドラインを作った際は、全く進まなかったが、統一基準を作ることで進んだということもある。ある程度やり方を示し、“やりなさい”と強く求めることは良かったのではないかと思っている。ＮＩＳＣなどの一箇所の中央が、教育モデルの課題等、情報セキュリティ確保に関して各省に対して支援をするということは強く出してもよいのではないか。

○　現場にいる方々は、セキュリティの考え方を整理し、判断するということはやられていると思うが、専門知識をアップデートすることがかなり大変である。各個人でアップデートしてくださいということは大変なので、中央の支援などの役割分担はあるのではないかと思う。継続教育的なものについて、中央で何ができるのかという取組みもあってよいのではないか。

○　ＮＩＳＣの役割をもう少し明確にするということか。

○　人材確保に関するＮＩＳＣの役割を明確にということである。

○　量的な問題も考えなければならない。１，０００人の人を確保するのであれば、自前の教育体制や体系をとり得るが、地方に行けば自前の完結的な体制はとれない。情報セキュリティ人材ということだけで議論しても、ＩＴ人材の一部として存在するもの、或いは業務も含めた包括的なものを想定してもよいが、政府全体としてＩＴ人材がどれくらいあり、情報セキュリティ人材はそのうち何%を想定するのかといったものがなければ、結論を出しにくいのではないか。米国では、万単位のＩＴ人材がある中で、かなりのセキュリティ人材を割り振ることができると思うが、日本の、特に中央省庁の現状では、ＩＴ人材が限定的であり、ＩＴ人材をどのように確保するかが課題になっている中で、情報セキュリティ専門家を確保するのはかなり難しいのではないか。そこで、姿において“動きが開始さ

れている”、“生じている”といった引けた表現になっているのではないか。量的にどれくらい確保するのかを明らかにしなければ、議論はできないのではないかと思う。

○　ユーザーレベルのセキュリティ人材、プロフェッショナルレベルでのセキュリティ人材があると思うが、政府の中で必要なのはユーザーレベルのセキュリティ人材だと思う。どの程度の能力ももった人が必要かということは見えにくい。プロフェッショナルレベルのセキュリティ人材は、アウトソースに頼らざるを得ない。現実的に高度なレベルで活動している人は、多くの団体の中で、使命感に燃えながら個人的に活動している人が目立ち、そういった人たちの評価と処遇が描きにくく、育成がうまくいかない。ユーザーレベルの人材が備えるべき知識を明確にしながら、その層を厚くすることに特化してしまうと、後にその人々の処遇を含め難しくなる。そういった特定のレベルの層を厚くすることと、プロフェッショナルレベルを組織化して育成していく手立ての両方が必要ではないかと感じる。

○　資格は一つの目安であり、ベースラインである。アウトソーシングとして求められるものは高度な技術や最新の情報、民間で実際にこういったことが起こっているという情報であると思う。そのような専門的分野は細分化されており、高度なものであり、資格というものは合わないのではないか。ウイルスに詳しい人、ハッカー攻撃に詳しい人、Ｌｉｎｕｘのオープンソースに詳しい人、データベースに詳しい人など資格では無理がある。セキュリティはキャリアがものを言う。その人が積んできたキャリア、スキルのレベルを定量化して表現できる業務スキルシートのようなものがない。この人は凄い、この人は有名という表現でしか、世の中通用していない。キャリアがどのような事象に対応しているか、キャリアとレベルの定量化した共通言語として、業務スキルシートが書けるようなものがあれば、その人たちが試験を受けるための試験勉強をするようなこともなくなり、より現実的になる。

○　資格も含めて、今委員がおっしゃったことは、抜本的に考え直し、キャリアやスキルをマトリックスで定量化、可視化していくことを考えてはどうかということだと思う。資格はあってもよいが、あまりこれに重きを置いたものは、間違った方向に行くのではないかとう御見解かと思うが、おそらくそうだと思う。今述べていただいた点も、かなり考えていかなければならない。

○　他の委員から出た意見で、量的な予測、どのような組織体制になるか、to/be モデルについて言及されていた。これを何年後のモデルとするか、例えば１０年後として、次の３年間でどこまでいくか、人員の必要性を含め量的な推計を立てていくことが必要になるのかもしれない。これまで、重要な点をいろいろと述べていただいた。この辺りも事務局で整

理しなければならない。

○　まだ御意見がおありだろうと思うが、事務局へメール等でお寄せいただきたい。

(3)国際連携・協調の推進について

○　“アジア地域等における脅威とその所在を把握し、具体的な脅威に対する対策を積極的に協調して行う”といった一文がなければ、セキュリティの計画としては重要な部分が抜けている感じがある。遠慮することなく、地域にとって脅威になることは、一丸となって取り組むということがあってもよいのではないか。警察庁や防衛省、或いは安全保障に携わる機関との連携を深めて対応するということを入れておくべきではないか。

⇒資料に示している“アジアにおける共同の脅威動向の把握機能創設の支援”等、そういったことも念頭に置いており、最終的に文章としてどこまで書くかについては検討させていただきたい。

○　文章としてはこのようなことでも良いと思うが、基本計画の内容が、年次毎の具体的なアクションにどのようにブレイクダウンされるのか、そのイメージがつかみにくい。Ｇ８やＡＰＥＣなど、ハイレベルな国・政府の連携を考慮し、標準化なども視野に入れた計画だと私は捉えている。アジアパシフィックの通信事業に関するＡＰＰなど、そういったところも視野に入れておっしゃっているのか、次のステップに行く際の具体的なところのイメージが持ちにくい。落とし込むところで、具体的に考えるということでもよいかも知れないが、３年後にここまで到達するのは難しいのではないか。

⇒姿については、ここに書かれている方向性を全てやった上で、そのようになるかどうかは分からない理想形ということで書いている。バイとマルチの両方の場があるが、ＰＯＣ機能として、日本のベストプラクティス、海外の状況については積極的に発信していくということを、今いろいろな会合があるが、引き続き行ってまいりたい。バックグラウンドとしては、国内の体制をしっかりとし、関係省庁と協力して、日本として取り組んでいくことが必要だと考えている。アジア関係については、主としてＡＳＥＡＮ諸国を考えている。日本企業がかなり海外に出て行く、サプライチェーンなどグローバルになっているが、やはりアジアが多いということがあり、ＡＳＥＡＮを中心として、議論していきたい。情報セキュリティ文化、国際的な政策のハーモナイゼーションという観点では、欧米も含め議論しなければならない。今あるＧ８やＡＰＥＣ，ＯＥＣＤなど、高いレベルで合意を得られるような活動をしっかり行いたいというイメージである。

○　“情報セキュリティに関するアジアの玄関としての地位を確立する”という一つの姿があるが、私の経験からくる感覚では、協調・連携を行う場合には、日本からの発信が非常に重要である。それはいろいろな方がやられており、情報セキュリティに関して、日本はかなりアジアの中で先進国と思われている。しかし、それをまとめて引っ張っていくとなると、一つの団体を推進する、或いはＰＯＣを連携させるなど、強い力が必要になってくる。そういった力をどのように落とし込んで実現していくのかというメッセージがなんとなく感じられない。

⇒オペレーショナルな取組みでは、例えばＣＳＩＲＴやＡＰＣＥＲＴでは、日本も提案をし、それをオーソライズしている。個別のミッションに関しては、そういった活動をしている。スタンダードについては、特にアジアスタンダードというわけではないので、これはグローバルに行う。ＬＥ（Low Enforcement）については、いろいろな枠組みがあり、ＬＥはＬＥで頑張ってもらう。政策のレイヤーで、どのように連携させ、引っ張っていくかということが残されている。第１次計画の際にも、いろいろと行っているが、アジア各国のハイレベルなオフィサーが集まる場を提案しており、そこをコアにして、ドライブを掛け、前に進めて行こうとしている。総務、経産とも連携し、そこは現実的に動いて行こうとしている。相手もあることなので、国際部分としては書きづらいこともあるが、落とし込みと、具体的にやることのイメージとしては、そういったものがある。

○　国際連携・協調のところが、個別でなかったかと思う。結構綺麗なフレームワークというか、よく見るフレームワークであり、何をコメントするかと考えた。やはり我々の第１次提言の際の「事故前提社会」への対応力強化と、合理性に裏付けられたアプローチの実現というところが見えないと思っている。よく見ると、それ自身は具体的な方向性の中のサンプルなのかコンテンツなのかというそのようなレベルなのかもしれないが、逆に言うと、情報セキュリティ文化の醸成等はひとつの柱として出ているので、もう少し「事故前提社会」の対応、情報共有の一テーマなのかもしれないが、出して貰えるとよい。また、合理性に裏付けられたアプローチは技術のところなどでは出ているが、共同研究なのかもしれないが、そのようなところでの協力関係もあるかもしれない。もう少しこういうことが出てくると今回の委員会らしいのかなと思う。

○　重要な点だと思う。オフショア等、国内との関係をどうするのかも絡んでくるため、そういった別の切り口も必要かと思う。一般論で、もう一工夫あったほうがよいのではないか。

○　他に御意見がある方は、メール等でお寄せいただきたい。

(4)犯罪の取締り及び権利利益の保護・救済について

○　二点ある。一つめは、現在の法律で十分かということである。これは、足りていないという前提で、法律を作りましょうというのではなく、実際には行為そのもの、例えばフィッシングや、情報を会社から１千万人分持ち出しても犯罪にならないなど、行為そのものを取り締まれなくとも、それ以外の何かで調べるなど、別の構成要件に該当するということがあると思う。それでカバー出来る部分はそれで良いと思うが、カバーできない場合は、行為そのものを何とかして処罰の対象とするべく、ここで法執行機関が取り締り出来るということは、法律があるということなので、そういった、法律を簡単に作るべきという訳ではないので、今の法律で十分かという検証と、必要であればどういうことが必要かという検討を、３年掛けて議論することが良いかはわからないが、少なくとも議論をこの中でしておかなければ、新しい脅威などに対応できなくなるのではないかという気がする。そのような検証と研究について是非入れて欲しい。二点目として、国民が気を付けて頑張りましょうというようになっており、国民は、年寄りも、あまりリテラシーが高くない人もＩＴを使うが、かといって全て手ぶらでノーガードでも大丈夫なようにしようとは思わないし、無理である。例えば、サービスを利用する前に、特にクレジットカードや個人情報を入力する際に、その情報が漏れた場合の被害の救済がどこまで保証されているか明示する義務を負う、また、オンラインショッピングでの買い物で、カード番号を入れる際に、このサイトでは、もし漏れた場合、悪用された場合に、きちんと補填する・しないなど、そういったことを明示する、何でも全てとは言わないが、これだけが保証されているということを明示するような共通の言葉やレベルを明らかにし、ユーザが見て、「私はこれはＯＫ」と思える、判断できる材料を提供する、サイト側にそれを義務化する、あるいはそれを奨励するようなものがあれば良いと思う。

⇒　直ぐに可能かは分からないが、少なくとも利用者が判断できるような情報を、補填の範囲に限らず、できるだけ分かるようにすることは必要だと考える。どういうことができるか、事務局で持ち帰り、関係府省と考えさせていただきたい。

○　今の委員の意見に近いが、犯罪取締りの技術水準の向上を挙げ、他方で犯罪に遭わないようにしましょうという書き方になっている。その他に、犯罪そのものを減らすような取組みを考える必要がある。犯罪を減らすには、まず何が犯罪かということを再度認識し直す必要がある。先ほど、法的な問題も含めてサイバー空間上のどのような行為が犯罪行為として取り締まるべきかということについて再度考え直す必要がある。それに対して、制度的、技術的、協力的な取組みをする必要がある。犯罪そのものを減らすことなしに、加害者、被害者にならないようにということでは、安心・安全ということにならないのではないかという気がする。犯罪そのものを減らすような制度的・技術的な取組みが必要なの

ではないかということが意見の一点目である。二点目は、権利利益の保護救済のためと書いてあり、他方、問題発生時に冷静に対処し問題解決に迅速に対処できるよう知識の普及や啓発とあるが、救済に当たらないのではないかという気がする。他に救済を考えているのかお伺いしたい。

⇒救済についてはなかなか難しいが、小額被害の問題だと裁判などにもなかなか触れられない、また、基本的に事故前提とは言え、被害に遭わないことが望ましい。技術的な対応も含め、どうしても事前に偏ってしまいがちだが、もう少し救済について方向性を出すことができるか考えさせていただきたい。

○　何が犯罪か明確にする必要があるという点について。国立国会図書館の館長も講演の中で述べられていたが、例えばデータを集めたい、集めて本人の許諾なしに公共財としてフリーに公開したい、後からこれはお金をとって見せたいという人が出てくる場合は削除する。すぐにそういったことがなければ、公開としてしまうということでよいのではないかという提案をされていた。これは、国会図書館の今後の生きる道を考えた上での御意見でもあるが、そうすると犯罪が減るということもある。これは動画配信サイト等の一貫した考えでもある。そういうことも含めてなのか、もう少し既存の犯罪の枠内でということか。

○　サイバー空間上の犯罪を考えるには、リアルとの対比で考えた方が良い。一つは物を盗めば罪だが、情報の場合は問われないというのは、色々な問題はあるものの、サイバー空間上で犯罪として扱うべきなのかどうかという議論は一つある。住居に対しての不法侵入はリアルな世界では犯罪行為と言えるが、サイバー空間上では積極的に来ることを望んでいない、パスワードなどでガードしているシステムに悪意を持って入り込み、覗いたりすることについて、これは犯罪行為なのか、また、実際には使わないがマルウェアなどを悪意をもって置く場合は犯罪に当たるのかといった議論はあまりされていない。技術的なものや教育的なものだけで頑張ることは少し無理があるのではないか。

⇒今の法律で十分かということがあるのだと思う。マルウェアは、犯罪条約批准のための刑法改正ができると、ウイルスの作成罪、送付罪などが犯罪になり、問題は解決するのだと思う。住居侵入に対応するものについては、不正アクセス禁止法があるため、少なくともパスワードなどでセキュリティが確保されているところへ入ることは犯罪になる。最初に述べられた情報窃盗については、今、おそらくパスワードといったものを盗るといったことが問題だと思うが、情報の性格に応じ、財産的価値として著作権で保護する、或いは不十分だという議論もあるが、不正競争防止法で保護する、また個人情報保護法などもある。分析を行い、この情報はこの価値で保護するということができれば、盗んだ者を罰するような仕組みができてくるのだと思う。非常に大きな問題で、考えなければならない。

○　技術戦略の推進と犯罪の取締りの部分との関連で意見を述べたい。技術戦略の推進で描かれる姿で、利用者による情報セキュリティ対策が不要な端末や情報家電の提供とあり、技術の面では、一般の方々は安心して利用できるのだろうと読める。犯罪については、サイバー犯罪という表現をされているが、相手を特定することが難しい問題と、このようなことが起きてしまうということに関して、提供する事業者、技術の面での問題があったケースがあるのではないか。一般的な人の救済ということも書いてはあるが、利用者保護という立場に立てば、法的枠組みをしっかり作り、執行するという問題と、事前防止のための教育という問題、被害にあった場合の救済の３つがある。法的な枠組みをしっかり作るという前提での話しになるが、被害救済を考えた場合に、責任の所在がはっきりしているもの、はっきりしていないもの、はっきりしていても捕まえられないものがあり、それが利用者である程度わかるような説明、警告が必要だと思う。他の委員からも出ていたが、もう少し被害救済という立場に立てば、切り分けが必要ではないか。法整備がなされることが前提と申し上げたが、裁判や救済に関する相手は、犯罪者だけではなく、行政の不作為、不行使に及ぶ可能性もあり、この部分をもう少し整理していただければ、国民の安心感は増すのではないか。

○　長年、金融の分野で被害者保護、消費者利益の実現ということをやってきた。その際、必ずプロとアマを切り分け、プロは自分でやるべきであり、救済は必要ないが、一般の利用者については、こうしたことが必要であるという形で、プロアマ論というものを行っている。情報セキュリティについても、犯罪の部分については、そのような切り分けをした議論が必要ではないかと感じる。

⇒救済については、責任の所在の有無を含め考えさせていただきたい。プロとアマを切り分けるということは、発想としてあると思うが、何がプロで何がアマかということも含めて考えたいが、難しいところもある。

○　プロとアマの線引きであるが、事業者であるか否か、業を営んでいるか否かなど、事業者の場合には規模の問題、スキルの問題など、様々な切り口があり、金融の分野でもいろいろとやってきているところである。金融機関が投資家としてプロかと言えば、必ずしもそうではないなど、その人たちを一旦プロと分類したとしても、アマ成りをさせる可能性がどこまであるかといった議論をしている。

○　“犯罪の取締り”及び“権利利益の保護・救済”とあるが、順番が逆のような気がする。サイバー空間上で起こる様々なことに対して、リアル空間の延長線上だけで考えられるかといえばそうではない。そういったことを含めた権利利益の保護・救済、犯罪の取締りに

対する対応策と考えれば、サイバー空間上の事象をどのように捉えるかということをまとめるようなアクションが先にきた方がよいのではないかと思う。

○　デジタルは財産として規定できていない、従って刑法を認めないということもあり、サイバー空間特有のルールというものは、創造、クリエイトしていかなければならない。今後、構想するといったことがあってもよいのではないか。リアルでの対応にも準じなければならないが、それだけで終わらせてもいけないのではないかという気がする。

○　どちらかといえば、保護・救済に関する観点だが、ユーザ側も勉強しなければならない、連携をする、知識をもってくるというインセンティブがあるとよいかもしれない。ここでは被害が起これば救済しようという感じで、自分自身も頑張って勉強して行こうという感じにはなっていない。

○　具体施策は分からないが、一般の人へ向かって、全て上から下への施策を書いているように思える。個人が、事件や事故の一歩手前で悩むなど、そういったものへのアクションがとれるといったことは必要ないのだろうか。いくら啓発などをやっても、それだけでは分からないのではないか。そこからもう少し発想を進めれば、インターネットはどんどん進んでいく。例えば、地図サービスでの画像表示やプロフなど、提供する側は良かれと思ってやるが、それを悪用する側が出てくる。それは、事件、事故になっていないが、個人としては不快と思うものを吸い上げる仕組み、センサーのようなものを作らなければ、後手にまわるのではないか。ただ、過敏に反応すれば規制などにも繋がってしまうこともあり、非常に危ない。今後の基本計画の３年間で、そのようなセンシティブな問題を検討していく場、そういったものをやるべきかもしれない。

○　特に、自殺者が出るなどの韓国での出来事をどのように見るか、どのように扱うかということは重要になる。

⇒　前回、他の委員からご指摘があった犯罪として定義されているものに対して、どのように対応していくかということを、まずは書いている。その他、今の法律で足りるか、足りないかは、おそらく検討しなければならない。これは、各省庁がいろいろな形で行っているが、俯瞰的に全てが見えている訳ではなく、見えているところ、見えていないところをどのように見て行くかということはある。今、委員が述べられた犯罪の定義にはないが、インタレストの違いによって、不快に感じるものなどについては、基本的には民間で取り組んでもらいたいと思うところもある。法律は現実問題として、そのような構造になっているのではないか。安全・安心のコンテキストでそれをやっていくということはあるかもしれないが、情報セキュリティ政策と言った場合には、いろいろなことが想起される。

この会議でも、いろいろな議論があり、それは議論としては良いが、本当に情報セキュリティ政策の枠内で考えられるところなのか。個人の不快さを吸い上げる仕掛けがあり、世の中で起きていることを分かった上で政策を進めることは必要かもしれないが、それをメカニズムとしてもつことが政策なのだろうかと自問自答している。計画として示すことは、正直難しいのではないかと感じている。

○　情報セキュリティの範疇ではないとすると、どこに受け皿があるのか。Ｗｅｂ化などの技術が進化し、一般の方々は感性として分からない。技術はどんどん変わっていくということで、マウス一つを動かし、動かしている責任をとられているかもしれない。訴えようがない。ＩＴ技術について追従できているとは思えない。基本計画で、やりなさい、やるべきだ、推進すべきだというメッセージだけでもいいのではないかと思っている。受け皿を作れというのかは分からない。

⇒　方針文書であることは事実であるが、具体的に何をやるかという３年間のプログラムを考えた場合、声を出すことは大切だという意見は分かるが、今の委員意見は、もう少しシステマティックなことを考えるということではないか。

○　疑問や不安を持った場合に、聞けるところ、対応するところといった発想、或いは人に伝えるという発想である。

⇒　コストのことを考えなければ、弁護士を使うなど様々な仕掛けはある。消費者センターに相談するということもあるが、そういったことでもないのか。概念的には分かるが、イメージとしてどのようなものか。

○　但し、危険はある。

⇒　インターネットは怖いという消費者は多数いる。怖いので携帯電話使う、メールは怖いので携帯電話からメールは外してくださいという消費者もいると伺ったことがある。それをどうやって実現するか、サービスを豊かにし、賢明になっていただくしかないのではないか。インターネットの不安感を伝える有料ダイヤルサービスを買うか、といったことしか思いつかない。安心の根本には、安全はメジャラブルであるが、安心はメジャラブルではないということがある。安心を社会的に作り出していくサービス、メカニズムとは何か、それを誰がやるのか、教育ではないやり方は何か、という疑問も広がる。

○　そこを誰かが引き取らなければ、良くないのではないか。

○　食品の安全に関する議論でも同様な議論を行っている。リスクを分析し、リスクコミュニケーションを行い、一般の人に伝える。必要なものは、規制や基準値を作って取り締まる。ＮＩＳＣにそういったシステムが本来はあるべきだと思っている。そこで、分からないとおっしゃると、自殺者が出た韓国の出来事のようなものを規制する、特定の食品を法律で規制するといった声もあり、そういったことになる。事細かな枠組みができ、基準を作ってＮＩＳＣにそれを取り締まれといった無理な話になってしまう。むしろ、それは現実的に行政レベルでリスクを分析し、それを知らせるというシステムを作ることを検討すべきではないか、ということが解決策になるのではないか。

⇒　それはやれることであり、行政がやる部分であり、そういったメカニズムはあると思っている。先の委員が述べられたものは、心の問題についてである。

○　迷惑メールのようなものもあり、抜き出して法律化すべきものはすべきである。それをしっかりできる体制を作ればよい。

⇒　それは先の委員の意見ではなく、他の委員の意見にあった、リスクをみて、法律化されているかをみて、必要であれば規制や対策をたてることを行政としてやっていくことは、政府の機能としてあるため、それをオーガナイズするという努力はできるのではないかと思っている。先の委員の意見は、そうではない漠然とした不安や、法律で取り締まるほどではないが、気持ち悪いことが起きているといったことを、行政がセンスし、それに対して何をどうすべきかを考える頭をシステマティックに持つべきだというものである。

○　それは持つべきである。食品安全委員会も十分ではないと意見も分かれているが、そういったシステムを作ってやっていけばということである。それは、行政の仕事の一つであると思う。同じかどうかはわからないが、やはりある程度世間で起きていることを敏感に先取りし、それに対して分析を加え、その時点での一定の解釈というものを、専門家の観点から分析した上で国民に伝えていく。不安はあるが漠とした不安であり、今は現実的に行政的、法律的に対処する手段がないという見解を発表することも、一つの安心を得るために国民が厳正に情報を得る手段になるのではないか。国民がそれぞれ、インターネットからわけのわからない情報を集めて、これは安全らしい、危ないらしいと判断して、ほったらかしにしておくというのは行政としては手落ちではないかという気がする。

⇒　人に害が及ぶのであればそうであるが、明らかに犯罪でもなく、サービスの一環として出しているものもあり、それがわからないから不安であるというものをどのように受け止めるのかという議論だと理解している。

○　特定少数の人物が、国や行政に対応しろと言っている訳ではなく、ある程度の数の方から、そういったトラブルやモヤモヤとしていても大丈夫なのかということについて声が上がり、それをキャッチすれば、速やかに評価し、それに対して政府が見解を出していくことは重要ではないか。そういった柔軟なシステムが必要なのではないか。これは食品安全行政などでも求められるものであり、まさに、今や世界でも体制が整備され取り組まれていることであり、ＩＴについて行っても何ら支障はなかろうという感じがする。

○　個人の分野で、個人の底上げに向けた効果的な普及・啓発活動の実現というものがあり、周知、教育、一般ユーザへのアドバイスなど、こういったレベル以上のものなのか、その中で収まる話のようなものなのかによっても違うのではないか。

○　食品を例に挙げたのは、世界では風評などインターネット上で怪しげな情報が上がれば、会議体が起きたりということがある。モヤっとした不安に対して、誰かが説明しなければならない。その場合、責任をとれる主体が説明しなければ、一般の合理的な判断には結びつかないということが、世界的な潮流になっている。食品安全委員会など、行政的手法によって、いわゆる専門家が然るべく安全評価、技術評価を行い、合理的に情報提供を行っていくアクションを起こしている。ＩＴも検証できない不安があり、政府がそういったものに対応するものを作るということも、ＩＴが合理的かつスムーズに使われる社会を築くためにも必要なのではないか。なんらおかしいことではなく、普及・啓発とは少し違うものである。

○　同様の意見である。今、消費者庁の設立に向けて議論が行われている。各省庁がきちんとやっていれば、消費者庁を作らなくても諸々の問題は解決したが、迅速に対応しないため、一つそういったところを作り各省を動かす、という流れであろう。国民生活センターを使い、被害情報や注意喚起情報をより早く出し、各省とも連携して対応するということである。消費者庁ができれば、情報セキュリティもその輪の中に入り、ＩＴが絡む消費者トラブル、危険なことについて、関係各省が対応する枠組みだろうが、ＮＩＳＣのような機関があるのであれば、情報については更に支援して調査し、分かっている情報を流していくということが求められているのではないか。黙っていて良いはずはなく、ＮＩＳＣにはＮＩＳＣの役割があるだろうと思う。

○　Proactive という言葉を使ってよいか分からないが、動けるところが動くという形で、記述した方が良いだろうという意見が強かったということは言えると思う。これについては、事務局で整理していただき、各委員は極力、事務局へ御意見をメール等で送っていただきたい。

(5)重要インフラについて

○　今日の資料は、ＩＴ障害の定義に関して依然として両論併記的な書き方になっているが、「サービスレベルを維持できないようなものが障害である」ということが分かる書き方をしていただきたい。前回、交通事故死ゼロや災害犠牲者ゼロに喩える議論があったが、交通事故“死”ゼロや災害“犠牲者”ゼロの「ゼロ」は、“死”や“犠牲者”に掛かっており、対比させるのであれば、ＩＴ障害による“死亡者”がゼロということに相当する。“死亡者”的なものを喩えるのであれば、ＩＴの世界では“重要な影響が出ること”とすればよいのではないか。

○　多少蒸し返しになるかもしれないが、食品の安全と、ＩＴの進歩が激しい中での危険話を同列に喩えて、「同じレベルで対策を打つのが当然だ」とするのは、同じ意味で無理がある。生命に関わる分野とそうでない分野は違う。ＩＴの利活用で利便を得るために新しい技術進歩があり、新しいものにチャレンジすることによって得られる便益の裏にリスクがある、ということは、食品における安全性の問題とは分けて議論しなければ、「もっともなようで、もっともではない」気がする。

○　災害犠牲者ゼロや交通死亡者ゼロは、申し上げたとおりで、住民票であれば住基ネットカードなど、ＩＴは選択肢がなくなってきており、生死や人生に直結している。おもちゃとして使っているわけではなく、ゼロというのは他と比較してもなんら問題ないと思う。ＩＴは常に進化していると述べられたが、食品といったものも日々進化しており、だからこそ不安や不満がある。例えば、クローン技術を使った牛などの安全性も評価する、ＢＳＥは近年になって発生してきた感染症である。食品は何も店頭食について、安全評価をしている訳ではなく、ＩＴだけが進んでいるものではないので、幅広い観点から御議論していただく方がよいかと思う。

⇒　行動計画の本文については、今回お示ししていないが、先ほど御説明した内容で書こうとしている。目標ということについては、「ＩＴ障害は、国民生活や社会経済活動に重大な影響を与えることがない」と書こうとしている。ＩＴ障害というものを無くして行くことは、基本的な姿勢として持つべきであると、重要インフラ専門委員会の中でも議論がある。方向性としては、そういったものを書きつつ、目標ということでは先のような形で整理したいと考えている。

○　具体的な取組みの方向性の中で情報共有体制の強化とあるが、情報共有の目的は重大なシステム故障等が起きた場合の対策を実施するためか、または原因について共有し再発防止を行うためなのか。どのような観点で、何を共有するのか読み取れないので、補足をお

願いしたい。

⇒情報共有にはいくつかの側面があり、予防的なもの、何か発生した場合にそれを直ちに共有するもの、後の教訓とするものがある。教訓と予防は情報としては区別しにくい場合もあるが、再発防止のような形で共有しようというものである。速報の体制は、内閣官房と重要インフラ所管省庁、重要インフラ事業者の間のネットワークを構築しており、情報を事業者の方から所管省庁を通じて、内閣官房にいただいたり、内閣官房から必要な情報をお出しするなど枠組みがある。セプターは各分野の中で情報共有していただくが、分野を跨いだ情報共有ということで、セプター・カウンシルの設立準備会を開催しており、設立にはまだ至っていないが、本年度内の設立を目指すとしている。その中では、当面はリアルタイムというよりは、事例や参考となる情報の共有ということを想定している。様々な側面で、それぞれの体制をとりながら進めていきたいと考えている。

○　何か事故が起こった際の一次対処や事業継続を行うために、相互依存関係にあるものがリアルタイムに情報共有を行う体制と、原因などについて情報共有を行い、良いものにしていく、比較的ゆっくりとした時間軸上のものは少し異なる。情報の判断もあるということで、書いていただければと思う。

⇒その点については、行動計画の中で詳しく書いていく。

○　第１次行動計画の中で既にやっている、第２次行動計画の中では、それを改善していけば良いという雰囲気が強く感じられる。本当にそれで良いのか。ネットワーク化とテクノロジーの進展で、非常に複合的なシステムができあがっている。セプターの中だけで物事を考えても済まなくなる時代になっているはずだ。本当に、そういったことに対応できる検討がされているか。自分の業界はきちんとやっているから、他の業界のことはよくて、それなりに対応するといった雰囲気が感じられなければよい。

○　情報共有体制の強化について、具体的には、電力や通信のインパクトが一番大きいはずである。それぞれのセプターの中でしっかりやっているのであれば、共通で一番重要なものが壊れた場合にどうするのかということを、積極的に前に出して検討すべきではないか。

⇒　一点目のご指摘については、第１次行動計画では、基本的には枠組みを作るということを目指していた。例えば、安全基準や、情報共有体制、相互依存性解析、分野横断的演習の４つの柱について、プログラムとしてやろうということについては、ほぼ達成できるであろうと考える。それで十分だと考えている訳ではなく、安全基準等や情報共有体制などについて、更に進化させていくことが重要だと考えている。

相互依存性解析については、更に範囲を広げるということで名称の変更も行っている。相互依存性については、分野間の依存関係をみており、電気や通信のほか、水道についても、水が止まるとコンピュータが止まるということで指摘されている。また、データのつながりによる、相互依存関係もみている。こういった知見を、安全基準や演習の中でも活用し、一つの分野が他の分野にどのように影響するかということにも活かしていきたい。

○　まだ御意見がおありの方は、メールにて事務局へ御意見をいただきたい。

(6)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 －