情報セキュリティ政策会議　基本計画検討委員会
第１１回会合議事要旨

１．日　時

平成 20 年 9 月 11 日（木）　16 時 00 分～ 19 時 10 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
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
神保　謙　委員　慶應義塾大学総合政策学部准教授
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）
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・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

⑴ 企業・個人分野での取組み状況に関する説明

○　警察庁より資料２に基づき説明がなされた。

○　総務省より資料３に基づき説明がなされた。

○　経済産業省より資料４に基づき説明がなされた。

○　文部科学省より資料５に基づき説明がなされた。

⑵ 企業・個人分野での取組み状況に関する説明についての質疑

○　新聞報道等でしか拝見していないが、先般、グルジアでの戦争状態において、インターネットにサイバー攻撃が行われ、政府機関のほとんどの政府機関のホームページが麻痺したという報道がなされた。1 年ほど前にも、エストニアでそのようなサイバー攻撃が起きたことが報道された。リアルな戦闘行為とサイバー空間での攻撃が同時に行われた事例は、これが初めてだという論調であった。警察庁でのサイバーテロ等の対策では、そういったものも念頭に置かれているか。それとも別の省庁になるのか教えて頂きたい。

⇒政府機関ホームページ等が攻撃対象となって、使えなくなってしまうといったこともサイバーテロ対策の対象として進めているところである。

○　エストニアの事例もそうであるが、今後いろいろなことが起こり得ると考えられる。事業継続性の観点からそういったことも考えておかなければならない。

○　文部科学省の方にお伺いしたい。情報モラル指導ということでカリキュラム表が出ているが、情報セキュリティは純粋な学問ではなく、技術や安全策といった内容である。中学では高校入試、高校では大学入試を目標にしており、学校側も子どもたちもその方向で動く。その中で情報セキュリティという観点を技術と捉え、カリキュラムを組むことで、どれだけ有効に子どもや生徒たちに勉強したいという意識が現れるのかという気がする。大学では情報は学問として捉えられており、技術という側面ではなく、もう少し学問という体系の中で組んだ方が、入試の科目にないため勉強しないというスタンスではなく、子ども、もしくは生徒たちがきちんと勉強していくのではないか。

⇒　ただいまのようなご意見は確かにあろうかと思うが、現状から申し上げれば、中学校では「技術・家庭」の技術分野で、新しい学習指導要領においても「情報に関する技術」と

いう内容があり、「情報通信ネットワークと情報モラル」という項目の中で行われることになっている。技術的・科学的な理解に基づく学習になるが、その上で、情報モラル、情報セキュリティに関してどういった行動をとるべきかを学ぶということになる。情報という体系の中でやるべきではないかということについては、高等学校では普通教科で「情報」がある。情報教育という全体の中で、情報モラルも位置づけられものであり、高等学校の情報科の中でも情報モラルについて体系的に学ぶということになっている。

○ 文部科学省の方にお伺いしたい。情報モラル指導モデルカリキュラムは非常にすばらしいが、例えば中学校で、このようなことに関して、年間で何時間程度教育されているか。

⇒中学校では「技術・家庭」の中で取り上げることになっているが、情報モラルカリキュラムに関しては「技術・家庭」に限らず、各教科でこのモデルを基に組んで欲しいということである。中学校では「技術・家庭」の教科があるので、この中で取り上げられることが多いと思うが、社会科や総合的な学習の中でも、情報モラルが取り上げられているという状況である。具体的に何時間かけているかについては、我々としては把握していないが、「技術・家庭」の技術分野について、年間３５コマ程度学習を行っているが、その中で具体的にどの程度割り当てられているかについては把握できていない。

○ 年間３５コマの中で、これだけの項目に割り当てられる時間は、どんなに多くても３～５時間程度だろうか。

⇒具体的な時間についてこうだということは難しい。３５コマの中でいろいろな学習がある。

○ これだけの内容があればすばらしいということになるが、実態として時間を使っていなければ、結局は絵に描いた餅になってしまうことを心配している。そうであれば、肝心な部分を数項目でよいので、きちんと教える方が効果が出るのではないか。

○ 先ほど警察庁の方から、安全確保に向けた取組みの中で、いろいろと教育も行っているとのことであったが、警察庁が文部科学省と連携して行うといったケースはあるのか。

⇒警察庁としても、学生、保護者に対する広報は必要であると考えており、文部科学省とも連携をとりつつ、進めているところである。現場レベルでは、学校で行う研修・講習会において、都道府県警察の警察官が講師としてサイバー犯罪等についてお話をさせて頂いている。

○　親としての経験から述べると、現状はパワーポイントやエクセルの使い方についての学習に時間が割かれており、情報モラルに時間を割いているという認識はなかった。実際に学ぶ方からのスタンスから言えば、面白くあるべきだと思う。モラルという形で、「あんなこと、こんなことをしてはだめだ」と言われても子どもたちとしては面白くない。算数や国語などのおもしろい科目があればそちらへ興味を惹かれる。モラルという観点だけではなく、情報を学問として捉えて教育カリキュラムを組めば、技術的な行動だけではなく、セキュリティを守るためにこんなに数学の要素が使えるということを教えられれば、もっと子どもたちの興味を惹くのではないか。

⇒「技術・家庭」でパワーポイントやエクセル等のソフトの操作を行う授業を行うケースも無くはないと思われるが、今回の新しい指導要領の中では、コンピュータや情報機器については、小学校の段階で基本的な操作を身につけるとしている。「技術・家庭」における情報モラルを含めその上で時間を割いて学習できるよう、指導要領を改訂したところである。

⇒面白い授業をという観点については、先生方もいろいろと工夫をされている。一方的に、これは悪い・あれは悪いというのではなく、何故こういうことをしてはいけないのか、何に問題があるのかを考えさせる活動を重視していきたいと考えており、新しい学習指導要領の中で、そのようなこともしっかりと行っていきたい。

○　先の委員と同じ認識である。昨年、学術俯瞰講義で情報について講義を行う際に、本部から分かり易くということを言われたが、学生も分かりきったことでは、「またか」ということになってしまう。若干高度でも、「なんだろうこれは」といった探究心を起こすものも入れた方が、おそらく面白がると思う。情報学、情報科学とはなんだろうという興味を喚起することなどにも留意して頂くことも重要である。

○　これは各々の学年の、各々のカテゴリーにおいて習得しているべきレンジ、知識の単位、能力の単位を示しているのであり、そのインプリメンテーションは各自自由だということか。それを面白くしていくということは、将来の授業での実現、インプリメンテーションに掛かってくるということでよろしいか。

⇒小学校の早い段階から情報モラルについて指導していくことが必要であるが、発達段階ごとの指導するレベルについてまとめたものはこれまでなかった。情報モラルについては早急に取り組むべき課題であるとのご指摘を踏まえ、このような表を作らせて頂いた。今回の学習指導要領の解説でも書かせていただいており、こうしたものも踏まえ、体系的に、各学校、教育委員会の指導計画の中にきちんと書き込んで頂きたいと考えている。

○　本当に教育を行っているのかということをお伺いしたい。「技術・家庭」において、パソコン教育の一環のような形で行って、本当に効果が出ているか。社会科等、他の違う科目で行うなども含めて検討すべきであると思う。

○　日本のように、高度なメール機能やインターネット・アクセス機能をもった携帯電話を子供に与える国は他にない。そこから現れる大きな問題がある。そのような問題に関して、平均年齢５０歳を超えるような教員で成っている学校ではピンと来ていないのではないか。本当にそのようなところでカバーしきれるのかということを、真剣にお考えになっているのかということを申し上げたい。

⇒教員のＩＣＴ活用指導力の向上ということで、その中で情報モラルの指導力も含めて向上を図っている。具体的には実態調査を行い、その結果によっては教育委員会の研修等もあるので、そういったツールを使いながら指導力向上を図っていきたい。

○　実態として、学校の先生方は教えることが非常に多く、情報や金融についての学習は、掛け声だけで、現実には行われていないという実態もあると承知している。先ほどの資料５の１１頁に、「地域・家庭における情報モラル教育の充実」ということで、地域で取組むという項目が挙げられている。ご説明では、地域の取組み、社会教育などは、大人だけが対象との感じを受けた。学校カリキュラムの時間数でできないとすれば、教育委員会は学校教育、社会教育の両方に係っているのだから、地域社会等で取組んでいくことができるはずである。何か取組みが行われているのかお伺いしたい。

⇒保護者等への啓発については、子どもに大きな影響を及ぼす立場ということで、取組みを進めているところである。現在は、総務省と連携し e-ネットキャラバンをはじめとして、啓発講座を学校、公民館等を利用して開催している。そこで、インターネット等の危険性についての啓発を行っている。そのような取組みを更に発展させるために、地域における取組みの充実ということで予算要求させて頂いている。実施に当たっては、学校現場との連携も視野に入れつつ取組みたいと考えている。

○　その地域での取組みというのは、大人だけを対象とする生涯学習政策局の取組みか、または、子どもも巻き込んだ親子の講座という形で行っているのかということをお伺いしたい。

⇒ 生涯学習政策局としては、大人のみが対象ということではなく、子どもからということで取組んでいる。保護者に焦点を当てつつ、その先には、保護者の方を通じた子どもへの啓発ということも視野に入れて行っている。

○　「保護者の方を通じて」という表現をされては、一緒にやられているかどうかが分からない。金融に関する学習の例では、授業の中で取り上げられないということで、親子一緒にした講座が様々なところで展開しつつある。親も子も同じ時間の中で、一緒に学ぶことが効果的だということもある。そのような取組みが実際に行われている、または推進しようとしているのかを伺いたい。

⇒ 現状では、親子一緒に学んで頂くということが、結果としては行われている。また、保護者の方だけにというもの、教師の方にというものなど、いろいろなケースがある。今回の事業では、基本的には保護者の方を対象としているが、実施に当たっては子どもと参加されるパターン、先生方も参加されるパターンがあると考える。

○　実際に推進しようとしているのかということをお伺いしたかった。文部科学省はカリキュラムを作る、予算を確保するだけではなく、現場で進んでいるかについてチェックしているのか、ということをお伺いしたい。どこかでやっていますという例を挙げて頂くだけではなく、ベストプラクティスがあれば、それを核にして様々な取組みを広げて頂くことが重要だと思う。

⇒　現状については、今年度で地域での取組み事例等を調査しているところである。そういった事例を収集・分析し、課題等を踏まえて改善していきたいと考えている。

○　資料５の１１頁の「学校における情報モラルの充実」の１項目に「情報モラル専門員派遣」とあるが、この専門員はどのような能力、資格のある方達で、どのようなことをされるのか。人数や規模についてどの程度を考えられているか。

⇒　脅威等については新しい手口を使って行われるということから、そのようなことについて技術的・専門的視野をもっている、生徒に対するそういった指導のできる能力をもっている方々を想定している。それを２１地域ということで、各地域に対応付けるということを行っていきたいと考えている。

○　総務省にお伺いしたい。技術面でＩＰｖ６への移行を重点に書かれているが、ＩＰｖ６へ移行してもセキュリティの問題は解決せず、むしろ拡散するのではないかというのが私の考えである。資料３の４頁にある情報セキュリティ政策はあまり根本的な打ち手にならないのではないか。インターネットの大きな問題は匿名性から出ており、極端なことを言えば、匿名性を排除するネットワークを作ってもよい。技術的に匿名であるネットワークと、匿名ではないネットワークが並存するような研究など、セキュリティのレベルが上がるような研究について、具体的なお考えがあるのかお伺いしたい。

⇒　資料５の９頁【参考５】に記載しているが、ＩＰｖ６が抱える脆弱性があり、実環境でどのような課題があるか抽出することも一つの課題であると考えている。ＩＰｖ６への移行にあたって、ＩＰｖ４と並存する期間があるため、ネットワークを上手く動かしていく上での課題もあり、検証していく必要があると考えている。そのために、移行シナリオを検討する、プロトタイプのシステムを構築し、データを解析した上での課題抽出を行っていきたい。

○　ここで書かれているＮＧＮはＮＴＴのＮＧＮということか。ＮＧＮはｖ６とコンフリクトを起こすというような問題もあるようだが、ここに書かれている課題を是正して、セキュアにしていかなければ、本当の意味でのネクスト・ジェネレーション・ネットワークにならないのではないかと思っている。その辺はきちんとやる必要があるのではないか。

⇒　ＮＧＮは今年３月にリリースされたが、必ずしも完全ではないということもあるので、そういったところは修正していってもらうということが必要ではないかと考える。

○　セキュアなネットワークを作るということで、昨年の１１月に新世代ネットワーク推進フォーラムが立ち上がり、ＮＩＣＴで研究開発に着手しているが、これとＩＰｖ６の関係はどうなっているのか。フューチャーインターネットで全く新たなプロトコルを作ろうというものであるが、ＩＰｖ６との関係がよくわからない。

⇒　新世代ネットワークの検討は、全く新しい転送原理について、１０年くらい先を見越したもので、ＩＰｖ６との関係はない。

○　文部科学省に対してであるが、アンケートのとり方に関して、教育委員会から件数を上げて頂くだけではなく、文部科学省の方からアウトカムが何であったか、どのような指標を採って欲しいかということを明示しておかなければ、中身についての検討・分析を行うためのアンケートにならない。戦略的に考えたアンケート等を、文部科学省から教育委員会にお願いして頂くということがよいのではないか。それを行わなければ、エビデンスに基づく次の政策立案ができないということになる。

○　政策展開を促していくために、今どのようになっているかを見るアンケートを採る際に、直ぐに返して頂くのではなく、３ヶ月、６ヶ月といった期間をとり、その間に改善をしたものを返して頂くということもある。それにより、進めなければならないということで取り組んで頂けることもある。その辺りも工夫して頂けるとよい。

○　委員の方で伺っておきたいことがあるという方がいらっしゃれば、事務局へメール等でお寄せ頂き、各省庁へ聞いて頂くということにしたい。

（3）企業・個人分野

主体間の類型に応じた共通理解のあり方、信頼関係の構築について

コスト・利便性の関係、コストからメリットへの転換

○　ＩＴの力を活用して世の中どんどん便利になっているが、様々な主体がシームレスに繋がりエンドツーエンドで様々なものが処理される結果、見境なく「何でも繋げば良い」という方向に行き過ぎているのではないかという問題意識がある。リスクが顕現化した際の対応力とのバランスにおいて、どこかに分断した避難エリアというようなものを作っておかなければ、リスクが溢れ出してしまう惧れがあるのではないか。その辺のリーゾナブルな関係性についても、何がしか主旨が反映できると良い。

○　ＡＳＰ、ＳａａＳのように企業が持っている情報をＩＴベンダに預けてしまうということを想定すれば、契約で担保するということになるかもしれないが、ＩＴベンダがシステムを提供し、それを利用し、情報資産はそれぞれの企業が自分の責任で守るという現実から考えれば、主体間でのモデル取引・契約書で縛ることは難しい。どのような情報セキュリティレベルのシステムにするかという仕様を発注者側が明示することで、守らなければならいということになるのではないか。同様にＳＬＡガイドライン、格付け等についても、個人情報を念頭に置くのか、その企業にとって価値の高い情報を念頭に置くのかによって、主体として情報を、どの程度守るべきかについてガイドラインを示すことは有り得る。どのような情報を預けるかにより、提供側はレベルを変えることになり、会社によって格付けするわけではない。もう少し詰めたセキュリティレベルを明確化しなければ、このような議論は難しいのではないか。

⇒　契約の書き方について、いくつか問題点が指摘されているところであり、また情報処理の実態自体も変化してきており、その辺りをどのように考えていくかは難しいところである。サービス提供者の格付け、レベルという議論の前に、契約当事者間の実効的な評価をどうするか、モデル取引・契約書も浸透して行かないことをどうするかも難しいところである。ガイドライン間の整合性の課題などもあり、ガイドラインを中心とした施策の進め方でよいのか、この先ガイドライン以外でもレバレッジを効かせられるものがないか、考えるところである。

○ 企業が持っている情報資産を守らなければならないという点は、我々も真剣になって考えている。個人情報保護等について、法律で定められる管理のあり方などについては、ある程度ガイドライン等が示される必要がある。顧客から預かった情報を適切に管理しているかにつ

いては、法律やガイドライン等を作るべき問題か、あるいは自主性により競争原理の中で、取組まれていくことがよいかは、よく考えるべきである。全てがガバナンスを効かせるためのガイドラインを整備すべきということは、企業の意欲を削ぐ可能性もあり、広く網をかけない方がよいのではないか。

○　個々の企業の取組みについては、今の委員の意見でよいかもしれないが、繋いだ場合どうするかということは重要である。ＩＳＭＳに関して技術に関する記述がないわけではないが、ガイドラインやルールでは技術に関する記述がほとんどない。セキュアなコーディングを行う、例えばＳＱＬの脆弱性についてはチェックするソフトウェアがあり、そのチェックをかけているかといった、技術についてのガイドラインやルールはあるようでない。このようなものを決めることは難しいだろうが、決めていこうといった動きは必要である。

○　先の委員の意見にあった「何でも繋げばよいというわけではない」という主旨のご発言に関連して、例えば、２０年くらい前に作ったアセンブラにパッチを当てて、コントローラのソフトを直して、クレジットカードの処理を繋ごうなどということではトラブルは起こってしまう。古いソフトだと調べればわかるようなものは繋がないといったことを、具体的に個別に行っていく必要があるのではないか。

⇒　下請け企業と元請けの関係においての個人情報保護、特許情報等に関して、瑕疵条項で青天井に書かれるケースもあり、契約書のテンプレート等で是正していこうという動きもある。下請け代金の適正請求、支払いに関して、下請けした側が業務遂行に必要な費用の応分負担をどのように考えるかといった法律はある。現実には、そのようなところに商慣行が上塗りされ、力関係の中で適正化されないといった課題がある。中小企業は元請が変わる度に、セキュリティに関するリクワイヤメントが変わり、その度に無駄な設備投資が二重、三重と行われるといった課題がある。約９５％が中小企業であるという日本の現状を考えた場合、今のやり方で本当にうまくいくのか考えると、多くの悩ましい問題がある。大企業のロジックで、企業間のことは企業間でということでよいということは、全体最適に向かう一歩としてそれでよいのかということを、３年間の取組みの中で強く疑問に思う。

○　下請けでセキュアドなコードが書ける企業がどれだけあるだろうか。まわりの事務処理だけを固めても、きちんとしたことはできない。

⇒　そうであれば、発注側が適切な納品検査を行っているのかという議論にまでなってしまう。今の問題は、中小がしっかりしておらず、大企業はしっかりしているということではない。商社化している企業と、実行的な仕事をしている中小企業という構造がこれまで考えられてこなかったということである。ＩＴゼネコンとよく言われるが、発注書を書くためだけに大企業の

社員がいて、コードを書く、オペレーションを行うのは中小の下請けであり、情報セキュリティに問題でトラブルが起これば、瑕疵条項でバッサリ切られる。産業施策を含めて、これで強くなっていくのかということを考えたとき、何かやらなければということを、この３年間で感じている。

○　議論がずれいるのではないかと感じる。テストデータ等で例外的な場合もあるが、ＩＴベンダはシステム開発契約の中では、極力情報は預からない。セキュアなシステムを作る責任は、契約ではなく、どの程度セキュアなものを作るかの仕様書によって仕事がなされる。仕様書として、どの程度セキュアなものにするか示されなければ、ＩＴベンダ側も契約では受けられない。ここでの議論は、企業の有する情報資産を、どのように情報セキュリティガバナンスで守るのかということである。ＩＴベンダが情報資産を預かり、代わりに管理することはない。

⇒　三つの異なる課題があるということで整理させて頂きたい。一つは、情報の受け渡しに関して、通常の企業同士であれば市場原理が働き、規制やガイドラインは必要なく、下請け元請けの関係で市場の失敗が生じる場合には、何らかの是正が必要ではないかという議論、第二には、システムを開発する企業とシステムを発注する企業の関係で、要件を定める仕様書が明確にならなければならないという議論、第三として、情報セキュリティに関する格付けや要件等は企業に対してではなく、どのようなものに使うかといったサービス毎に考えなければならないという議論ということで事務局として咀嚼したい。

○　情報セキュリティガバナンスは重要であるが、人事、財務、資材調達の中でどれだけ影響力を持つかについては、業界、ＩＴベンダやユーザ企業によって異なるというのがこれまでの議論のポイントかと思う。情報セキュリティガバナンスはどの企業でも行われることであるが、やり方、度合いはビジネスモデルごとに類型ができるとよい。施策という観点では、情報セキュリティガバナンスは進めるにしても、進め方の中で企業経営との関わりを、この次の数年間で整理して頂きたい。その中で、今の議論であるＩＴベンダについて、どこまでやればよいか、自己のセキュリティ、システムを作る際のセキュリティをどのように分けて考えるかなど、結果としてそれがレベルになってくるのではないか。

○　法律は究極的なガイドラインであり、法律であればみな認知する。ガイドラインについては、作成段階で皆が納得いくレベル感になっているかということと、それを理解してもらい、どのように普及させればよいかということになる。先ほど、下請け元請けの話、技術でセキュリティの向上が図れないという話もあったが、個別の技術に関しては業界で整理しながら普及・啓発を行っていくしかない。普及・啓発の仕方を効率的に考えなければならない。

○　企業のＩＳＭＳでは、企業の資産に対してリスクの算定を行い、どのような対策を行うかを決め、ステートメントに記述し、具体的にその対策が機能しているかを評価し、機能していなければ直していくというＰＤＣＡを回していくというものである。国際的にもガイドラインではなく、ＩＳＯ／ＩＥＣ２７００１として基準化されている。それを推進する中での経営層の考え方がＩＳＭＳの中に十分に入っておらず、簡略化されている。具体的に経営層が何をやらなければならないかを書き下そうというアプローチが採られている。また、企業が外部リソースと連携をとりつつビジネスを進めていく中で、実際に発注を行う際の役割分担、あり方、信頼関係を整理しなければならないという議論が開始されている。標準化の世界でも、ここでの議論は非常に重要なこととして、議論が開始されている。そこで、出てくるものは、おそらくガイドラインである。ガイドラインの乱発は避けた方がよく、ＩＳＭＳのような国際的基準、国内の基準、ガイドラインは書けるところ、書けないところがある。書けるところというのは、皆がそのガイドラインを参照して役に立てるものである。具体的に書いたとしても、使う環境が違うことなどにより、役立たない場合には盛り込めない。例えば、ＩＳＯでは具体的な暗号の使い方、鍵の管理の仕方が議論されたが、企業によって異なるため盛り込むことは止め、全て外出しにした。技術は具体的に実装して評価しなければならず、詳細な技術ガイドラインは必要であるが、国の施策の中で行うことには疑問がある。脆弱性やリスクは時系列で変化しておいる。それらをアップデートする機構があればよいが、難しいとすれば、ガバナンスの推進を含めたアウトソースのあり方を整理するという施策が盛り込まれるべきということが、基本計画の一つのメッセージとなるのではないか。詳細を含めることは、別のステージで議論すべきである。バージョンによって異なるウィンドウズの話を本当にするのか、ＵＮＩＸの話をするのかでいろいろと変わってくる。必要ないというわけではないが、そのような整理でよいのではないか。ガイドラインを作る際にも、同様の内容を、別のシナリオでガイドライン化するのはよくない。筋の通った１本のガイドラインがあればよい。

○　主体や主体間の情報セキュリティについて書かれているが、情報そのものに対してどうすべきかという視点も重要である。対策を行う側にとっても分かりやすい。このような情報をもらった場合はここまでの対策、そのような情報を扱う企業であれば、ここまでの対策ということが分かってくる。そのようなことが出てくる施策を打つことが重要ではないか。そのようなやり方もあるのではないか。

○　重要な意見と受け止めて、事務局の方で検討するということにさせて頂きたい。ごもっともなご意見であり、これらを施策的にどのように取りまとめるか、もう少しお時間を頂きたい。

（３）企業・個人分野

「事故前提社会への対応力強化」との関係～緊急対応・事業継続性確保等について
企業規模と情報資産活用度に基づく整理、中小企業に適した施策について
海外企業が日本の個人情報、企業機密情報を保有するケースへの対応について

○　中小企業に関する論点で、「企業規模に加えて、情報資産活用度、活用する情報の重要性という観点にも配慮しつつ、適正な対策が推進されるべき」とあるが、書かれている順番が逆だと感じる。一番な大事なのは情報の重要性、情報資産活用度として、それを扱う量や頻度、そして、最後に規模が来るのではないか。インターネット自体で生きている企業は、規模が小さくても手厚い対策が必要であろうし、人命に関わるようなことを扱う企業は、零細であろうが手厚い対策が必要である。逆に、何万人が働いている企業であっても、ＩＴとの関係が間接的であったり、希薄な企業は基礎的な対策をとれば良いといった筋道を明らかにすれば、よりクリアになる。「中小企業だから人も金も足りなくて可哀想」と言うのは、ムードとしては分かりやすいが、あまり論理的ではない。文章には拘らないが、そのような整理をした方が良い。

○　事故前提社会に関して、事故があるのですぐに対応でき、事業継続ができるという論調だと思うが、ＩＴに関しては、火災や地震による倒壊とは異なり、分からないうちに被害が広がる、進行していくということが特徴としてある。緊急対応の前に、積極的に早期発見する仕組み、予兆を発見する仕組みが必要である。ＩＴに関する事故では、誰かに迷惑をかけることになるので、事故後の説明責任も果たさなければならない。そのためには、どのようことが起こり、どのような被害が起こったかを説明するための記録が保存されている必要がある。そのことを明記しなければ、事故が起これば早急に復旧すればよいということに偏ってしまうのではないか。

○　私が仕事で関係する企業では、災害や不正アクセスが発生した場合に、どのような状態になるのかが分からないというところが多い。このようなことが起こった場合、ここまではできる、そこまではできないということを明らかにするべきである。これは経済産業省の情報セキュリティ報告書に書かれるようなことだろうが、「事故前提社会への対応力強化」ということを強く打ち出すのであれば、ここを切り出し、企業も強制ではないが推進していく、事故が発生した場合に、ここまではできる、ここはできないということをディスクローズする仕組みがあってよいのではないか。一般企業のセキュリティコンサルティングを行う際、ＩＳＭＳを取得する場合と、ＢＣＰを策定する場合の作業は同等に大変なことである。事故の場合は、ストーリーから作成する必要があり、何が起こるか分からない。その意味でも、ディスクローズして、ここまではできるということが必要である。

○　海外企業が日本の個人情報、機密情報を保有するケースに関しての意見であるが、最近は

ＩＴの開発をオフショアで行う場合だけではなく、企業の人事業務、総務業務などを人件費の安いアジアで行うということが盛んに進められていると理解している。その場合、企業内の社員の個人情報が海外に出ることになり、日本の法律が及ばないところに出ている可能性もある。現実が先行している中で、そのような問題に対してどのように考えるかについては、早めに整理しておく必要がある。採りうる対策事例の提示といったことではなく、もっと強力な仕掛けがいるのではないか。

○　コストと利便性のバランス、メリットへの転換ということに関して、どのレベルで、何ができていればよいのかという共通認識がなされていない。経営事項として企業が情報セキュリティを取り上げるところは少ない。ＣＳＲはかなり共通認識されているが、その中に情報セキュリティが位置づけられているかといえば、経営者の関心が寄せられているとは言えない。経営層が情報セキュリティに関して正しく理解し、経営事項、リスク管理事項として位置づけなければ、何をどうすればよいかということが個別にバラバラになってしまう。何らかの形で、情報セキュリティについて分かりやすい指標があるとよい。元々、情報システム化する前であれば、企業では営業秘密管理規定、文書管理規定があり、そこで情報資産の取り扱いの規範等があった。その延長にあって然るべきだが、情報システムが絡むと経営者の関心が薄まる傾向にある。そこが確立しなければ、全体のビジョンが明確にならない。

○　重要インフラではＣＥＰＴＯＡＲ（セプター）等の取組みで、いろいろと進んできている。重要インフラではない企業との差が開く、ある意味で不公平になっているのではないか。極端なことを言えば、重要インフラ周辺の企業は何もしなくてもよいのかということになる。各企業のレベルに応じてであるが、ディザスターリカバリー、ＢＣＰの一環として情報セキュリティの課題にしっかりと取組むということを推進することが必要ではないか。ＢＣＰ策定の作業は大変であり、その意味でも、そのことに取組むことの示唆はいるのではないか。現状、目安がなく、自らが一定のガイドラインを決めて行うしかない。一般の企業のＣＩＯやＣＩＳＯが簡単に決められるとは思えず、何らかのガイドラインが必要である。

⇒　頂いたご意見について、基本計画で政府がなすべきこと、その実行可能性を考えると難しいところもある。まず、企業規模よりも情報資産の重要度、活用度が重要だというご指摘は、客観的にもご尤もである。国としては中小企業施策といった確立した分野があり、政策としては打ち出しやすいということがある。情報資産の重要度、活用度に応じた施策ということでは、どのようにその度合いを測るのかということがなければ、施策になりにくいという問題がある。

予兆を発見する仕組みに関するご意見は、何らかの形で予兆が捉えられればよいが、企業が予兆を捉える仕組みを政府がどのようにエンカレッジするかという課題がある。仕組みに関して、お知恵を頂けるとありがたい。

説明責任が重要であることは、随所で取り上げなければならないと認識している。しかし、

個人情報保護法は別として、規制がないため、記録を保存することを一般企業に強制することは難しく、取組みを促す仕組みをどのように作るかが課題である。

状況を想定し、何をどこまでできるかについて公開することについては、企業が自主的に行って頂ければよいが、基本計画で行うべきとは書くことは難しいのではないか。どのようにすれば、経営者が重要性について認識いただけるかが重要だと考える。

域外適用ができないため、海外にある情報の保護をどうするかは重要な問題であるが、すぐに答えを出すことは難しく、いろいろな観点から関係省庁とも相談して考えなければならい。

どのようにすれば経営者の関心が寄せられるかということに関しては、昨今の食の安全に関する報道等で、食品関連企業の経営者がその重要性を認識するということもある。情報セキュリティに関して経営者に重要性を理解頂くための方法についてお知恵を頂ければありがたい。

どのレベルの対策がどの程度できればよいかの共通認識に関して、そのレベルについては非常に難しい。一律に作れるかということも、過去この委員会でも議論された。例えば、政府も統一基準を策定しており、実施できていなければ、その省の責任になるが、実施して何か問題が起これば、基準を作ったＮＩＳＣの責任にもなり、基準を作ることはある種の責任転嫁にもなる。世の中で、ここまでやれば免責されるという統一的、あるいはマルチグレードな基準を作れるかは難しいところがある。はっきりとこのような基準を作るということを基本計画に書くことは難しいのではないかと感じている。いろいろと具体化する知恵を頂ければ、ありがたい。

○　経済産業省の方にお伺いしたい。いろいろな指標やガイドラインを考える際は、国際対応も重要である。ＳＯＸ法対応におけるＩＴガバナンスに関して、北米ではＣＯＢＩＴ（コビット）等の議論があり、セキュリティ政策は影響を受けると考えられる。この辺りはどのような方向でお考えになられているか。

⇒　日本企業が直接的に関係するのは、Ｊ－ＳＯＸ法（金融商品取引法）である。Ｊ－ＳＯＸに関するガイドライン、システムを構築する際のベースとなるシステム基準等、経済産業省の建付けの中で、どのような対応をすればよいかというガイダンスは昨年の春に公表している。そのような状況の中で企業が困る状況もあるので、情報資産は利活用がベースであり、どのように自分の資産を守るか、自分で価値を判断するものであるということから読み解き、一方では、預かった情報はコンプライアンスの問題として、それらをどのようにミックスし、海外も含めたグループ統制をどうすべきかについてのガイダンスを作りたいと考えている。どこまでできるかは分からないが、そのための検討会を作り、チャレンジしようということで取組んでいるところである。

○　国際的な動きや新たな金融商品取引法、アメリカのＳＯＸ法に関連して動いている基準や指標を無視した情報セキュリティに関するガイドラインや施策を作っても、意味がなくなる

可能性があり、特に企業については整合性を考えなければならない。事務局でも今後検討して頂きたい。成案まで時間があるので、今日のご議論を反映しつつ、継続して検討して頂きたい。

（4）企業・個人分野

基礎教育や生涯教育を通じた児童・生徒、社会人（高齢者を含む）への目配りについて

○　教育については門外漢であるが、先ほどの歯痒い議論を伺っていて画期的なアイデアを思いついたので、開陳したい。今や大学生のレポート作成や就職活動にはインターネットが不可欠であると理解している。この際、大学受験自体をＩＴ利用にし、アクセス制御を一段乗り越えなければ回答すらできない、二、三段乗り越えなければ、東大や早慶上智には入れない仕組みにしてしまえば、教育現場の対応は一挙に向上するのではないか。残念ながら若い人は受験に関係しなければ熱心に勉強しない。無茶な議論かもしれないが、電子政府やＩＴ立国を目指しているのであれば、それぐらい言っても良いのではないか。

○　教育に関するもう一つの視点として、情報セキュリティの教育のやり方やコンテンツを工夫をした方がよいのではないか。一般の方、大学生に話をする機会があるが、つくづく感じることは言葉が通じないということである。ＩＴ業界でも通じていない場合があり、言葉の共通性、定義を整理しておかなければ、一般の方には言葉の定義が多すぎる。また、情報セキュリティは正常系ではなく、異常系を教えなければならない。予防の対策が採られていることもあり、どのようなことが起こるのか実感がない。ウィルス対策をしなければならいことは分かるが、何が起こるかは経験もなく、ほとんど知られていない。不正アクセスで何が起こるかも分からない。「こういう対策をとりましょう」という正常系だけを教えても実感がないため、ウィルスが発生する画面等を見せるだけでもインパクトは違ってくるが、そういった動力となる経験を重視してもらう必要がある。

○　人格形成期にあり自己判断能力が不十分であると考えられる児童・生徒と、リテラシーについて支援が必要な高齢者とは、明確にトーンを分けるべきである。児童・生徒に関しては教育ということに重点を置くべきであり、高齢者では啓蒙と支援が重要になってくる。法律等でも人格形成期か否か、自己判断能力の有無は区別し得るものであると考えられ、明確に分けるべきではないか。

○　教育、育成の際に、他の分野の専門の方を代用して教えるのではなく、急には難しいだろうが、長期的な視野で情報学のカリキュラムの中で教えることを盛り込んだ方がよいのではないか。児童・生徒と高齢者への対応は違うのではないかとの先の委員の意見に同意である。特に異なる観点は、子どもは放っておいてもインターネットを使う。モラル、あるいは安全

サイド、こういうことをしては危ないということを教えることが重要になってくる。高齢者には３パターンがあり、いわゆるデジタルディバイド、全く使えないが携帯電話は使えるという人、少しだけ使うが安全については分からないという人、我々のように使えるという人がいる。安全でないことばかりを強調してしまえば、デジタルディバイドにある人は、ますます使わない方向に向かってしまう。情報通信を使わなければ、損をしてしまう、困難が生じることもあるので、そのような観点があるとよいのではないか。

○　教育の問題では、教育する側と教育される側の問題がセットとしてある。教育する側がしっかりしなければ上手くいかない。日常生活に密着することは、本来、親が主体的に教育できなければならないが、情報セキュリティに関しては何をどうすればよいかすら分からない。日常的にインターネットを使っている子どもがはるかに長けている。携帯電話によるインターネットで、親よりも情報を持っている。そのような環境の中で、児童や生徒、理解が低い人々に分かりやすく教える人がいなければ難しいのではないか。一般家庭で親が情報セキュリティについて何か言えるかといえば、ほとんど言えない。学校の先生方も大方そうではないか。そこを変える仕組みを少しずつでも作ることを、テーマとして挙げていかなければならないのではないか。

○　住所を入力した途端に、その家の周辺が見えてしまうといった環境が今後もいろいろと出てくるのではないか。そのようなものは犯罪の冗長に結びつくのではないかという危惧を感じる。ストーカーにしろ、空き巣狙いにしろ、居ながらにして遠くの状況が分かる。ある人の住所さえ分かれば、周りの環境が分かる。このような社会環境の中で理解が低い人たちに、情報セキュリティについて分からせていくことは、非常に重要なことである。教える側の仕組みをしっかり考えなければ難しい。

○　教育ではなく、個人を守るという観点から述べたい。オークションサイトでＩＤを不正に利用され、商品を出品、落札され、月額２万６，０００円のサービス利用料を請求された経験がある。サービス利用料を払う必要はないのではないかと主張したが、契約書に自己責任との記載があるということで、紋切り型であった。同時多発的に３，０００人が同じような被害にあっており、３，０００人×２万～３万円くらいの売上高ということである。銀行等であれば認証の仕組みも強化されている。それはオンラインバンクで被害に遭えば、銀行が補償するということがあるため、一生懸命、自発的に行っている。現状は自己責任ですと紋切り型であり、そういったところへカード番号などを入力している。ログを見ると一回でログインしており、それを同時に３，０００件ログインすることは困難であり、どう見ても答えは一つである。そのことを言うと、漏洩した形跡はないということであった。それは何を調べたのかも分からない、ログが無いのかもしれない。そういった場合には、サービス利用料を免除する仕組みを具体的にすれば、そういった業者も自ら考えるようになるのではないか。

○　基礎教育や生涯教育を通じた児童・生徒、社会人（高齢者を含む）への“目配り”とあるが、目配りというレベルで行くのかという議論が必要である。児童・生徒、高齢者が論点として出てきた経緯からすれば、社会的な弱者であり、義務教育の子供たちであれば国の責任でやるべきであろうという理解している。子どもと高齢者に関しては、直ちに保護すべき対象であるということだと思う。また、子どもに関しては、長い目で教育していくべきだという観点があるのではないか。

○　先ほどの文部科学省のご説明を聞いている限りでは、あのような形で、啓発などに無駄遣いはして頂きたくない。教育は、通常の教育予算の中で行って頂ければよいが、保護や支援については、ここで皆さんと議論ができればと思っている。

○　ガバメント・ツー・コンシューマー、GtoC は難しいと思う。責任分担モデルについての総務省の勉強会等に関わったことがあるが、消費者だけの責任ではない部分がある。GtoBtoC のような形で、政府が事業者に対して、かなりのことを行使する、事業者のコンシューマーに対する責任がもう少し書かれてもよいのではないか。事業者というのは、通信事業者、端末メーカ、その他の事業者であったりするかもしれないが、そのことが書かれない限り、この個人分野は今の“ふわふわ”した感じになってしまう。

○　敢えて対策を行わない者には様々なタイプがあると考えられ、主には３つあり、一つは不精・手間隙を掛けない、二つ目は費用負担がいやだ・できない、三つ目はモラルが欠如している、というところだと思う。このような人々については、まさに BtoC の B の部分がネットワークに接続させない、端末で制限するなど、技術的な措置が取れるということが必要ではないか。

○　児童・生徒に関しては、親の教育と責任をはっきりさせなければならない。高度な機器を無防備に与えて、その影響を親が分かっていないというのでは被害を受けるのは当然である。明解な説明をし、教育をするということは、子どもよりむしろ、親に対して必要である。性犯罪や、ID の不正使用など具体例を説明することが一番よいのではないか。その部分をきれいに、曖昧模糊としてしまうので、モラル等といった話になる。現実に犯罪が起きており、その犯罪例を教育することが、自分の責任も含めて身構えるということになるのではないか。

○　高齢者に関して突き詰めれば、今年辺りからリタイアし始める人間が、何故そのようなリテラシーも持っていないのかということになるのではないか。７０、８０歳の方に、コンピュータが分からないから仕方ないと言うことはあまりないだろうが、企業の中で情報化に触れていた人間がリテラシーがないということは考えられず、自己責任ということはあると思

う。書きにくいことではあるが、ある程度のことは、書かざるを得ないのではないか。

○　利用者に対する説明がまずい、不親切なところがある。もう少しサービス提供側も、高齢者だからということではなく、技術をより使いやすくするための努力はいくらでもできるのではないか。説明をきちんと行う、利便性を高めるための努力もサービス提供側には求められる。

○　産学官関係のパートナーシッププログラムに関係して、いろいろと勉強した経験から申し上げると、高校では情報という教科があり、その教科書はよくまとまっており、よい教科書である。しかし、これは大学入試センターの科目には入っておらず、入試の対象にはなっていない。それは、基本的には誰も真面目に勉強しないということである。改善すれば状況は随分変わってくるだろうと思う。

○　情報技術で立国する、科学技術立国と言っている中で、情報を試験に入れない、情報リテラシーが足りていないなど信じがたい。

○　それは文部科学省にも申し上げており、情報処理学会等でも指摘しているが、豊富な内容でよい教科書を教えられる教師がいないということが、おそらく現実ではないか。

○　大学入試の関門として、情報、ＩＴに関する情報学でも構わないが、利用の方法、モラル、学問、これらに関して試験をするということを決めてしまえば、そこから下に向かって降りてくるのではないか。文部科学省の中で手当てできなければ、民間の事業者で手当てをするなどの必要があるのではないか。

○　情報や金融に関して、入試に入れれば高校がしっかりと取組むのではということは、過去から中教審でも議論になっている。しかし、文部科学省は学習指導要領についてのみ関心があり、大学のカリキュラムについては他人事と思っている。大学入試に入れるにはどうすればよいかは、別の場で討議しなければならないことだと感じている。今回の書きぶりで、工夫して盛り込んで頂きたい。大学入試と企業の入社試験でやることは、かなり効果的だろうと言われているが、文部科学省が動かないので他の方法を考える必要がある。

○　ゆとり教育の廃止にみられるように、他と比べて明らかに成績が悪ければ、驚いて動くということはある。ＩＴのベーシックなスキルに関する国際的な指標があれば、それを見て検討するということを書いてもよいかも知れない。

○　一番世論が動くのは、韓国や中国との比較であると思うが、日本は明らかに負けている。

指標を用いて比較すれば、これではまずいということになるのではないか。

○　これまでのご意見はまとめさせて頂き、今後の議論の俎上に載せていくこととする。まだ、ご意見がある方は、事務局までメールでお願いしたい。

（５）地方公共団体

地方公共団体の情報セキュリティ対策の推進について

地方公共団体が情報セキュリティの観点から地域で行う活動について

○　地方公共団体、対策支援主体、情報提供主体、推進体制についての討議であるが、時間も差し迫っており、対策支援主体以降の議論については、次回の委員会に回したい。

○　前回の政府機関の議論にもあった情報セキュリティ報告書を、地方公共団体についても推進して頂きたい。評価を行う必要はないが、自治体ＣＥＰＴＯＡＲ（セプター）にあるＬＡＳＤＥＣ（ラスデック）といったところで、比較が行えるポータル等があれば、いろいろと考えて、推進して頂けるのではないか。

○　今の委員の意見に同意である。政府機関についてはこれまで、いろいろな整理が行われてきており、そのような段階であるということなのかもしれない。しかし、地方公共団体については、情報セキュリティポリシーを定めて、公表してもらうことが前段としてあるのではないか。自ずから次にやるべきことを認識して頂けるのではないか。

○　情報セキュリティポリシーを持っている地方公共団体は多くなってきている。情報セキュリティ対策をどのように行っていくか、財政面で悩んでいる地方公共団体もかなり多い。

○　ここでどこまで書けるかということもあるが、人口減で予算が減っているということであれば、共同システム化、共通システム化を図り、コスト削減や運用経費削減を図るしかない。情報セキュリティポリシーも、独自のものでなく、皆同じものでよいということにもなる。その方が最低限のものを確保しつつ、コスト面でもパフォーマンスがよい。書きにくいかもしれないが、そのようなことを推奨できないか。

○　今、委員が述べられたような方向で、これまで総務省でも政策が検討されているが進んでいない。また、独自の作りこみ等があり、共同アウトソーシング等にできない環境にある自治体も多い。それによって効率化が図れるということとは別の問題で、バックハウスとフロントハウスのデータ連携できなければならないが、その目処が立たないという事情もある。いろいろあり、簡単なことではない。しかし、委員会として、そのようなことを各自治体に

言うということは、大変意義がある。

○　前回の総務省のご説明資料にあるＬＡＳＤＥＣ（ラスデック）の自治体セキュリティ支援室のようなところが、政府におけるＮＩＳＣ相当になればよいのではないか。どこまで独自性を求めるかということもあり、性格の違うところもあるが、ここが成長して頂くしかないかとは思う。

○　地方公共団体の情報セキュリティポリシーは、ガイドラインに沿って作られているだろうと思うが、それがどこにどのように公表されているかは認識が薄い。それは、先ほどのポータルサイトへ並べて頂くことがよい。そうではなくても、ディスクロージャの方法については一定のものを作ってもよいのではないか。そのような施策はなかったと思うので、ディスクロージャの方策を推していくしかないと考える。

○　経済産業省の支援でインターネット安全教室を全国で開催している。各地方の主催される主体の方々が集まり、連絡会議を開いて意見交換を行っている。各地方では、インターネット安全教室の他に、総務省・文部科学省のe-ネットキャラバン、警察庁のものがあったりする。中央から見れば、ピラミッドのように広がりがあるように思えるが、地方で情報セキュリティを担っているのは、ある限られた人々である。そこへ、全て各種教室、キャラバンが集中しており、調整ができずにバラバラで動いている。連絡会の中で各担当の方から、何とか一つに、あるいはもっと融通が利くようにできないのかという意見が出ている。効率化、整合を図って行っていくということは、是非お願いしたい。

○　まだ、ご意見がある方は、事務局までお寄せ頂きたい。

（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　－