資料２－２

情報セキュリティ政策会議　基本計画検討委員会
第３回会合議事要旨

１．日　時

平成 20 年２月 21 日（木）　16 時 00 分～19 時 00 分

２．場　所

内閣府本府　地下講堂

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
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
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）
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）
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) 基本計画策定に向けた、関係者ヒアリング①：日本商工会議所

日本商工会議所から、資料４に沿って説明がなされた後、下記内容の補足説明及び討議が行われた。

(補足説明)

○　弊社の状況を若干申し上げると、本社が大阪にあり、全国に営業所が７箇所、工場が上海を含め２箇所、配送センターが５箇所、子会社が５、６箇所あるが、日本国内は IP-VPM を使用しイントラネットで構築している。また、上海との間については、128k の専用回線をひいている。そのほか、アメリカでは１社、ヨーロッパでは８箇所ほど子会社があるが、国際通信のイントラネットとなると費用がかかるので、イントラネットは国内のみにしている。ホスト系で物流の生産管理、サーバー系で経理・営業の日報、社内メール及び文書管理をおこなっており、音声及びテレビ会議もこのイントラネットにのせている状況である。

○　経理関係については、子会社も全部一緒に行っている。それにより、費用については、通信費、コンピュータ及びサーバー端末を全部入れて年間 8,000 万円、人員は男子５名、女子３名という体制で取り組んでいる。

○　グループ内の全社を全て同じシステムで動かしており、インターネットとの窓口は、本社の一本でつないでいる。従って、何かトラブルがあれば本社で外部との回線を切れば、外部からの切断が可能になる。

○　セキュリティ関係の問題をみると、５、６年前、５月の連休に海外から日本にウイルスが大量に送られるという話があり、当時、私も担当していたので、情報システム担当部長と話をし、インターネットとの窓口を一週間ほど閉鎖し、落ち着いてから再開した経験がある。営業からは言われましたが、社長指示で閉鎖した。また、その時はインターネットとつながっている機械が少なかったので、各個人ごと、機械ごとにウイルスバスターを入れさせた。

○　３年ほど前に、インターネットにアクセスしている段階でウイルスのダウンロードを開始したことが検索している間に分かり、ケーブルを抜いて対処したことがある。これにより、かなり身近な問題であるという認識を持ち、しかもインターネットをつないでいる所が安価でウイルス対策をやるという話があったので、月 1,000 円くらいだったと思うが、そこにお願いすることになった。

○　現在はもっと安くなり、ウイルスもまず心配なく、スパムメールも除去してくれるので喜んでいたが、今年１月に USB のメモリースティックからウイルスが入り、蔓延した。これは、情報システム担当がサーバーを監視していて、判明し、２、３日かけて除去した。その際、１人でやっていたが、とても手に負えないため、５、６人を集めて対処した。このようなことがあり、USB は大変だと認識したが、これを使わないと仕事が難しいのも事実であるため、

対策を取れていない状況である。

○　話は変わるが、営業のためのシステムをシンクライアントに変えた。シンクライアントでは、サーバーにデータがあって端末にはデータが存在しない。端末を使用する度に情報をやり取りするシステムに入れ替えた。これで情報が少なくなると社内では安心しているが、社外から営業マンがPHSでアクセスすると、画面がかわるのに約20秒かかると言う問題が起きた。現在、見直しをして10秒弱ぐらいになっているが、それ以上は早くならず、通信システムを変えなければという状況になっているが、経費の問題があり、変更に至っていない。SaaSというのも通信インフラがしっかりしないとしんどいなと実感した。

○　鹿児島工場、鹿屋市の先の小さな町に工場がある。そこでのやり取りでは光ファイバーがないため、ADSLでやっている。光ファイバーを入れて欲しいが、川を３つほど越えなければならないという地形のため経費がかかり、実現していない。工場のすぐそばには、LG-WANがひかれているが、そのケーブルを少しのばしていただいて、私どものLANに入ってくれないかなと思っているが、未解決の状況である。

○　自宅では、メールとインターネット検索程度しか使わないため、ウインドウズMeを使っていたが、ウィルスバスターを入れてウイルス除去していたとき、一昨年、年末で作動しませんと言われ非常に困った。この辺りの基本OSは、2000年に買ったはずなので７～８年しか経っておらず、全然痛んでいない。にもかかわらず、費用がかかる若しくはサポートしてもらえないのが非常に困った問題であると感じる。零細企業は個人と同じレベルではないかと思うが、その意味で、巨大な出費が出ないように考えていただければ幸いである。

(質疑応答)

○　おっしゃりたい気持ちは充分理解した上で、二点指摘したい。一点目は、ITの利用の仕方に応じた対策で十分であり、全員が大げさな対策を強いられる訳ではない、つまり、パソコン単体でOAソフトを使うだけならば、特段の対策は不要であるということである。喩えると自動車の場合、ブルドーザーとかＦ１マシンを運転したいという場合は免許やスキルが必要になるが、自転車程度なら勝手に乗って良いし徒歩ならばお酒を飲んで歩いてもそんなに危険はない。これと同様に、企業がインターネットやシステムをビジネス上、重要な分野で使っていなければ特段の対策は必要ない。逆に言えば、中小であろうとインターネットを使って事業を行う企業は、これを使わない大企業よりも手厚い対応が必要になるのが当然である。その上で、それに応じて必要な情報リテラシーを向上させるという筋道ではないか。

○　二点目は、基本的な対応にはお金や人手はさほどかからない、ということである。高度な暗号化装置を入れる、ファイアーウォールを二重にするとなれば確かにお金はかかるが、定期的にウイルスソフトのバージョンアップをする、重要なデータを持ち出さないようにするなどは基本的な対応であり、特段「予算が」「教育が」といった話を強調しなくても可能では

ないか。喩えて言えば、家の火の元を点検してから出かける、帰宅したらドアの内鍵を閉めるなど、常識的にお金をかけずにできるような話が沢山あると思う。家が大きかろうが中小・零細であろうが、必要なことはやらねばならないという点は動かしようがないので、それに応じて対策を実施すれば良いと思う。

○　莫大なお金がかかるようなセキュリティ対策は元々現実的ではない。費用対効果が見合わなければ採用できない、という方向で話を進めれば、中小企業の悩みのかなりの部分が解決するのではないか。

○　極めて多重階層の労働集約型産業に従事し、中小、零細といわれている多くの企業に支えられている立場からすれば、本日の話は、非常に身につまされ、共感出来た。

○　セキュリティを考えるときには、市場の変化、マネージメントとコントロール、技術やスキル等いくつかの切り口で考える必要があると考えているが、今日の話は、かなりの部分、技術的な所で解決しようとする、だからお金がかかる、という話に重点が置かれていたように思う。先ほど別の委員からあったように、身の丈のセキュリティ、最適な取組みがあると思うので、それを捕捉したうえで、機密情報取扱いのルール、仕事用のパソコンにWinnyはじめP2Pを使う環境をつくらないなどの取組みをやっていく必要があるのではないか。

○　地方の建設業を見ると、老夫婦２人（社長と副社長）で電子商取引のための講習を受けに来られていたり、作業所一つにインターネットにつながるパソコン１台を設置すること自体が目標になっているという実態もある。地方に関しては、まさに支援策をやると同時に、必ずしもツール本体ではなく、その前の段階、管理の仕方であるとか、そういうことをきちんと理解していただく取り組みも大事であると思う、上手く指導する仕組みが余り無いが。

○　技術の問題に関しては、ソフトの品質が悪いがためにいろいろなトラブルを起こし、解決が困難なケースが多いという問題があると思う。セキュリティ対策ソフトでさえ、パターンファイルの事故を起こし業務障害を起こす。原因を特定するまでに半日を要する場合もある。そういう状態の中、中小企業に安心してパソコンを活用してもらうには、別の観点から解決を考えていく必要があるのではないかと思う。

○　資料の３頁目に、「取引先への過度な情報セキュリティ対策の強要」と言う文言があるが、「過度な」とはどういう事か、例示があれば教えていただきたい。また、情報セキュリティの向上は、中小企業、零細企業にとって競争力の向上になるのかどうかをどう思っておられるのか。第三に、中小企業側で考えた時に大企業からの情報をどう守るかという事を主眼に言われてると思うが、逆に中小企業の情報が大企業のほうに漏洩している、利用されているという事もあるのではないかと想像しており、この点、御意見を伺いたい。

→　「過度な」の例であるが、自分の身の丈に応じた情報セキュリティ対策を認識していたとしても、実際に大企業と取引する時には大企業のレベルに合わせないといけないため、

この時に「過度な」という感じになるのではないかと思う。また、大企業が開発したセキュリティツールを使用させ、その際に１回１回使用料とって、開発費を回収出来るようにするところが実際にある。また、複数の企業との取引をするためには、単一のセキュリティシステムではなく、各企業毎のセキュリティシステムを導入しなければならない等、コスト増もある。

→　セキュリティの向上と、企業の競争力の向上は、並行ではないのではないかという感じがしている。

→　大企業が中小企業のあらゆる情報を吸い上げてしまうというのは、情報では余り無いのではないか。技術のノウハウならばあり得るが。

○　感覚的な話であるが、セキュリティは、どちらかといえば、みんな頑張らないと大変だが、何もなければコストゼロなのに、というのが感覚としてある。一般の方もそういう認識をしているのではと思う。

○　中小企業が大企業との取引において、いろいろと負担を感じているという点についてであるが、当社の例を述べると、電子商取引を行う中で、たしかに、取引量の大きい会社さんからは使用料を取る場合があるが、比較的小さい規模の会社さんとは、そういう規制をかけない仕組みでやっている。また、普通の家庭に入れている環境、その程度の環境を作ること以外は求めないようにしている。

○　建設業の作業所というのは、非常に通信環境の悪いところに設けなければいけない場合があり、残念ながら日本の隅々まで良い通信環境が整っていないため、64k で充分動くような通信設備の作り方をしている。限られた環境でも動くように作れる技術力について、きちんと考えて欲しい。

○　現実、小さい会社をみていると、小さいところに対してはより厳しい要求がなされ、大きな力がある所にはそこそこの要求にしかなってないというのが、実際の日本の商取引の中では行われてる感じがしており、これが変わっていければと感じている。

⑵ 基本計画策定に向けた、関係者ヒアリング②：消費者団体

主婦連・東京地婦連・消団連・日本消費生活アドバイザー・コンサルタント協会（ＮＡＣＳ）から、資料５に沿って説明がなされた後、下記内容の討議が行われた。

○　個人情報に関する相談件数について、の数年の変化のデータをいただきたい。例えば、2005 年及び 2007 年はどういう傾向になっているのか。

→　2006 年が一番新しい情報であるが、傾向は毎年余り変わっていない。

○　資料５の一番最後に「監視社会」、「管理社会」と書かれている。これに少し関係するが、現在のインターネットというものは、ある程度匿名性があると思うのだが、この今のインタ

ーネットをどのように評価するか。匿名性がありすぎるのではないかとか、感想で構わないので、意見を聞きたい。

→　情報発信の場面では、どこの誰が出してるかが明らかであったほうが良いと思うが、電子商取引の議論では、セキュリティが確保され個人情報が漏れないようなものでないと安心しないのではと思う。

→　普通に意見を表明する場合は、匿名性で良い部分もあると思う。ただし、それが犯罪に関わったりした場合、それでもその人を特定できないという現状は、もう少し改善出来ないかと思う、例えば、プロバイダーとの契約などの認証などがもう少し進んでおいて、被害者にとっては人物が特定され、明らかにされるべきと私は思っている。

○　説明資料の最後のページに、「安全対策は、基本的にはITを提供する『企業の責務』として計られるべきではないか。」とある。自分も消費者の立場として、何割かはそうだろうと思うが、「基本は『ITを利用する側の責務』として計るべきでないか」との見方もある。

○　インターネットのように責任者や総括者が存在しない場合、誰に責任を持っていくのか、解決が不可能である。提供者側はできる範囲で最大の努力はするが、使う側が適切に使わなかったときまで責任を持たせるのは公平ではないし、合理的ではない、という考え方がある。自己責任原則が最初に来ないと、モラルハザードに陥り、いつまで経っても企業と消費者の適切・健全な関係が構築できない悪循環を懸念する意見もある、ということも申し上げておきたい。

○　先ほどの相談件数で、架空請求を含めて2004年から2006年のところで相談件数が大幅に減少しているが、それに対する原因・理由については想定しているところがあるのか。

→　マスコミを通じ、警察、総務省、消費生活センター等の広報・啓発を、複数回するという形でキャンペーンをはっていただいた効果として、減ってきているという状況である。

○　適切な情報提供の仕組みがなっていないのではというお話があった。この難しいところは、インターネットの仕組み自体を我々は便利に使っているが、そこにできあがったものが常にあって、安全検査をして国が薬のように３年間の検査をして初めて使える仕組みではなくて、皆が実行して進んでいくという仕組みである。何が問題になるかというと、実は小・中学生すらも便利に使っておりどんどん変わる。これに対して、後追いで教育しようという時に文科省で指導要領を決めている間に、必ずギャップが出て遅れる。そういう意味では、逆に消費生活センターなどで活動してる皆さんが、「草の根」といったらおかしいが、皆がうまく情報をシェアしながら相互に知識を増やしていく仕組みを作る仕掛けが必要だと思うが、これについてのアイデアを持っていたら、紹介いただきたい。

→　市民講座などでウイルス対策とか架空請求・不当請求の対策の話になると、受講希望者の倍率が高い。また、パソコンの使い勝手やソフトを使いこなすという講座も人気が高い。ただし、自治体の予算に限りがあるので、年数回しかできない。また、被害発生時には、

注意喚起をネットに流させていただくが、それにお気づきになるのは、日頃ネットを利用している方たちであり、そういう知識がない方もたくさんいる状況である。

→　地方に行くと、消費者相談の予算等もほとんどないため、データ自体を相談の窓口で調べることすらできないのが実情。そういう面も含め、対策をたてていただきたいと考えている。

○　インターネットは非常に便利であるが、自分が通信している相手が誰かすらよく分からない、場合によっては、自分の意図と全く違うところに繋がっていてもそれがわからない、という事態がある。他方、セキュリティは自己責任、使う人で勝手にやってくださいというところがあり、甚だ不親切であるが、安価と利便性が故に自主的にはこれを使わないと仕事も全然進まなくなったし、インターネットを使わないことには必要とされる基本的な情報すら得られない状況である。そこで、リテラシー教育でカバーしようとしているが、自分の親の世代のことなどを考えると、80 歳のおじいちゃんおばあちゃんにインターネットの安全性について説明し十分なリテラシーを確保するのは難しいと思われる。他方、IT ベンダーに安全性を全部保証させることも困難であると思う。どういう方法によって安全性を確保するか、国民的に議論する問題だと思うが、お考えを聞きたい。

→　個人的意見であるが、例えば省エネ例をみると、切替スイッチがついていても出荷時設定がオフになっており、自分でオンにする設定になっている。インターネットのセキュリティに関しても、パソコンにしても携帯電話にしても、セキュリティの部分について、あらかじめ自分自身で設定している利用者は少なく、何かトラブルがあった時に初めてセキュリティの設定がどうだったか教えられ、設定するのが実態。未成年者の携帯電話には原則フィルタリングを設定することが始まったのもひとつの動きだと思うが、メーカーとして、最低限の情報セキュリティに関しては基本的な設定でカバーできるのではないかと思っている。

○　資料の最後に書かれている、「安全対策は基本的には IT を提供する企業の責務として計られるべきでないか」という意見は、その通りだと思う。自己責任原則は分かるが、自己責任原則というのは、きちんと消費者の知る権利や、教育を受ける権利というのが満たされた上で出てくる原則であり、消費者基本法にもあるが、事業者の責務を果たした上でというのが基本だと思う。

○　資料中、７頁目に、「利用する側のレベルに見合った情報提供・教育・リテラシーが、十分になされているとはいえない」と書いてあり、その次に「情報提供には、携帯ショップ等、地域に身近な場をもっと活用していくとよいのではないか。」と書いてある。子供たちに関しては、学校教育はじめいろいろな場があるが、社会人に対する教育の場として、担い手は誰がよいのか。事業者がやるのか、事業者の場を利用しつつも公正中立な人たちがよいのか、担い手についてどのように考えるか。

→　携帯ショップは一例であるが、身近な携帯ショップなどに場を作り、その携帯キャリアだけが情報提供するということを我々は考えているわけではない。携帯にしろパソコンにしろ、身近な相談ができる場所、自分のノートパソコンを持って行って相談できるような場所が必要だと考えている。

○　資料中、８頁目に「被害救済の現場では、手探り状態で対応している現状であり、専門の一元的な相談窓口、原因究明機関、紛争処理機関等が必要である。」とあるが、一般的な被害救済窓口として「国民生活センター」や「消費生活センター」などたくさんあるなか、ICTの部分に関しては、現在なかなか対応出来ていない実情なので、このように提案されたのだと認識している。この窓口・機関等については、現在いろいろと設置されている窓口の強化という形態で対応できるのか、あるいは ICT、セキュリティに対しては専門の窓口・機関が必要であるとお考えなのか。

→　相談窓口の件は、現時点で考えがまとまっているわけではないが、情報家電を例にすると、冷蔵庫が壊れたのか、冷蔵庫に繋がってるネットの部分の通信が壊れたのか、適切な故障箇所を自分で見つけるのは非常に難しい。どこか一箇所に行けば、そこできちんと調べていただき、原因も説明していただき、紛争処理もしていただける場があればと考えている。

○　いわゆるユビキタス社会で生活していると、今までにない、学ぶべき知識や制度がどうしても必要になると思うが、資料にあがっている最近の事例を読ませていただくと、IT に対する警戒心がもの凄く欠けているという印象を持つ。このことについて、どのように見ておられるか、伺いたい。

→　大きな不安感を持っているのは事実。また、知識がなく、横文字とか専門用語で説明されても理解できないので、イメージで意識を維持しているところがある、そのため、より具体的な実態の状況、ウイルスに感染したパソコンを見せて、「こう言うのが症状です」と言うのが一番、皆さんに理解していただきやすい。専門用語ではなく、普段使ってる日常用語で説明し、危険性とかが理解できれば、今抱いてる不安は減るのではないかと思う。

○　残念ながら、ネット社会は性善説が採りにくい所がある。リスクがたくさんある事をどんどん啓発する為、情報セキュリティのコミュニティ活動を民間として始めているが、こういった活動を大きく盛り上げ、ネット環境の把握に取り組むべきと考える。

○　実際に代理店として、携帯ショップを運営しているが、お客様からどのようなクレームなり相談事があって、それにどう答えていこうかという検討は、正直あまりした事はなく、代理店はメーカーに情報を出し、メーカーが基本的に啓蒙していく課題かと考えていたので、非常に新鮮な意見として聞く事ができた。

○　企業が情報セキュリティ対策をして、それにより売り上げが伸びるかという論点があるが、

消費者の立場として、例えばインターネット取引などでセキュリティ対策を充分やってプライバシーを保護するとか、セキュリティ対策を講じていますという公表をしている企業とそうでない企業と、消費者が取引をしようとした場合、どちらと取引をされたいと思うのか、あるいは、そういう対策を取った企業のほうが、消費者としては取引をするのだろうか。

→　セキュリティについては当然、それの対策がとられているということが大切であるということを、案内している。基本的に、セキュリティが整備されていないというのは怖いことであると。現実的にも、消費者がリスクをかぶるので、対策がされている方を消費者は、選択する傾向にある。

○　既に主婦連の有志の方が、携帯電話の使い方とかセキュリティなどを一般にレクチャーして歩いていたり、老テク研究会の方がNTTドコモさんと提携し、各地で携帯やパソコンの使い方、セキュリティを講習して歩いている。そういう方々の層をもっと厚くする必要が、今後あると思う。また、企業の協力が必要であり、企業はそういう活動を、政策的に支援しても良いのではないかと思う。

○　私が関係している研究で、ブログとSNSの分析があるが、実は、自ら進んで皆様個人情報を一生懸命提供し、悪意のある人に簡単にわかるようにしている、という問題点があると感じている。個人情報を守れと言う一方で、自ら一生懸命重要な情報を出しているという状況である。既にブログは1,400万あるし、mixiに登録している人も1,000万人いる。この中で、悪意のある人が、自分で簡単なプログラムをつくるか、もしくは分析ソフト（安価なもの）を入手すると、簡単に、家族構成の中の機密、機微のある情報、電話番号などがとかわかる状況になっており、今後、政策的に重要になってくるのかなと思う。但し、自発的に情報提供なさっている方を「やめろ」とはできないので、注意喚起する対応と、事後的に紛争になる際に上手く紛争処理をできる機構が必要ではないか。

⑶ 基本計画策定に向けた、関係者ヒアリング③：政府機関（国土交通省）

国土交通省から、資料６－１に沿って説明がなされた後、下記内容の討議が行われた。

○　説明をいただき、非常に苦労されていることは感じた。意見１と４はおおむね理解、特に４（非常時における予算・契約の弾力化）は早く真面目に考える必要があるのではないかと思うが、意見２と３については、違和感を感じる。「組織形態が階層的であり作業に時間的な猶予をいただきたい。」と言われると、国民の立場からは、組織のあり方を見直すのが先決ではないか、民間はやっているし税金をそういう事で使われたら困ると思ってしまう。また、意見３（評価を開示すると複数の階層から圧力がかかり、隠蔽・改竄にも繋がりかねない）は、心情が分からない訳ではないが、「そういう組織であることを反省し、重大な決意を持って来年からは生まれ変わりますから、今年だけは勘弁願いたい。」とでも言われない限り、本末が転倒している感が否めない。

→　御指摘を受けることは覚悟の上で書かせていただいた。確かに、組織自体が変わらなけ

ればいけない、そういう転機にあるというのは理解しているが、やはりITの進展速度と役所機構の変化の速度がリンクしていないのではないかと感じている。例えば、人事でもITに詳しい人間が適性に応じて人事がなされるようになってきたのかというと、ようやくそのような動きが若干見られつつあるものの、他方、本当に適性があるのかと人間が我々担当者の世界でも動いてるのが実態である。これについては、政府全体の動きの中で、もう少し推進力がかかって行かないと変わらないのではないかと危惧しながら書かせていただいた。

○　所管業界で情報セキュリティ上の問題が発生した場合、業界の担当者を呼んで指導し、調査結果を出させて公表する側の官庁の意見として、いかがなものかという印象を持った。自分のところが規制しているレベルは、最低限自分のところでクリアしていかなければいけないのではないか。

○　意見３で「問題は公表しないでくれ」と言われているが、もし改革をしたいのであれば、むしろ洗いざらい公開し、実態を明らかにし、変えるための圧力を得ないと、省内に意見が浸透しないのではないか。意見３は、むしろ、「国交省の中の情報セキュリティについてもっと公開するように会議からしっかりと指導してほしい。」と書くべきではないかと思った。

○　重要インフラのかなりの部分に関与されている立場から、本業に関してどのように御意見を持たれているのかについて、御意見をいただきたいと思った。何らかの重要インフラに関わるような、本業で諸々の大きな問題を抱えた時にどうするべきかという、何らかの方針はあるが。

→　重要インフラに関しては、電子マネーの世界と重要インフラの世界がリンクする形になってきており、将来的にどう発展しどういうリスクを負っていくのか、ということに関心を持っている。注意深く勉強していかなければいけないとの認識の下、現在、検討しているところである。

○　お話を聞いていて、たぶんITの活用の仕方と組織構造が著しく乖離しているのではないかと感じた。企業はそういう所の構造をできるだけ緩和し、ITの利活用ができるモデルに変えている。時間がかかっても結構なので変革をお願いしたいと思う。

○　「人事の異動が早すぎて育成ができない」というのは、そういう中での制度の改革が必要ではないかというように思うが、ITリテラシーやセキュリティリテラシーを浸透させる最初の時期に有効だった方法としては、困っている人達をサポートするチームを常駐させていた。初歩的なところを今更という気もするが、ひとつの手段として有効な方法かもしれない。

○　防災の監視などにもIT技術が使われたり、飛行機の例ですとこの間システムの故障で飛ばなくなったりとか、または交通機関の自動改札がうまく行かないために大混乱が起きたとか、交通に対してのIT技術や情報セキュリティの重要性がどんどん増えてきていると思うが、重

要インフラを守る立場としての見解を伺いたい。

→　重要インフラの関係の取り組みが深いところまでいっていない、という実態であるが、重要インフラ専門委員会に鉄道・航空・物流の３分野が参加するほか、それぞれを所管している原局に協力しながら連携を深めていきたいと考えている。

○　コンピュータセキュリティ担当として苦労されているのだろうなと拝見させていただいている。昨年、NISC の人材育成・資格制度体系化の委員会に私も参加し、そこで申し上げたことに近いが、特に幹部に対し、リスクマネジメント、リスク感覚を教育すべきという話をさせていただいた。現在、国交省の中で、コンピュータに限らず、リスクマネジメントの感覚的な教育はやられているのか。その反応はどうか。

→　いつから始まったかは把握していないが、幹部に対するリスクマネジメント研修が行われているのは事実である。だいたい課長職以上が受講し、１回で全員やる事は難しいので、ローテーションで実施している。反応までは承知していないが、機会があれば別の機会に御報告させていただきたい。

○　ちょっと不安になったというのが、率直な感想である。現在、行政評価局のほうで政策評価委員会委員もさせていただいており、各省庁にヒアリングをやらせていただいているが、「評価・公表手法の改善を求める」は問題。政策の評価は、メリハリをつけて、PDCA をちゃんとまわしていただくということにつきる。まさに情報通信、テクノロジーをうまく活用して業務改善をしていただかなければいけない。そういう視点で動いていないのか、率直におうかがいしたい。

→　「評価・公表手法の改善」については、いろいろな御意見をいただく事を覚悟の上、敢えて書かせていただいた。我々としても、現場に対してプレッシャーをかけてきているというのが実態であり、現場はかなり大変なんだという泣き言も聞かされたが、やるという意欲については、かなり必死になってやっている。ただ、サーバーを管理しているチームのほうから、国交省の名前が良い意味で出ようが悪い意味で出ようが、名前が出ると、攻撃めいたものも含め、訳の分からないアクセスが急増する、という指摘を受けた。すなわち、IT に関しては、IT が非常に優れていると公表されても、非常に劣っていると公表されても、いずれにせよ攻撃が増えるということを管理しているチームから聞いておりましたので、公表に関し意見提出させていただいた。

○　電子マネーと重要インフラのリンクについては、検討していかなければ、という事ではなく、すでにトラブルが起きている以上、責任感を持ってやっていただかなければいけない。多分やってらっしゃる事とは思っているが。

→　個別の航空や鉄道などの取組みについて。鉄道については、JR など関係団体が集まって問題点を洗い出しており、業務改善対策というのをメーカーと摺り合わせていると聞いている。業を所管する鉄道局のほうで取り組んでいる。航空局でも同様に、先日もレーダー

のダウンの話がありましたが、今まさに原因究明作業をやっている所である。

(4) 基本計画策定に向けた、関係者ヒアリング③：政府機関（外務省）

外務省から、資料６－２に沿って説明がなされた後、下記内容の討議が行われた。

○　自らの対策の遅れについて、公表しないことが国益であるというのは、余りにも戦前のはなしを聞いているような印象。むしろやるべきことは、セキュリティホールを埋めることにより、国益をそれによって守ることではないのか。

→　国民、国家の利益を確保する観点から、限られた予算的資源の中でできる限りのことをやっているが、一生懸命やっても処理しきれない所は出てくる。特に、外務省は在外公館を抱えているが、在外公館については、いろいろな環境あるいは現地情勢などがあり、ネットの接続環境も異なる。そのようななかで情報セキュリティ対策に取り組むことの困難さと実際の取り組みを理解いただきたい。公表出来るところは当然公表するが、他方、外務省として個別の状況について公表することは、いろいろな攻撃の原因となり、かつ、諸外国にとって日本の外務省は信用出来ないということにもなりうるということも、理解していただきたい。

○　先ほどの国土交通省もそうだが、実務担当者の苦渋の告白という印象。実際、システム担当者は、やっている仕事が大変な割に評価をなかなか受けられない、ステータスが低いと聞いている。

○　CIO 補佐官の立場から言わせていただくと、省庁でも官房長とかトップの方を CIO に任命し、CIO 補佐官というアドバイザーをつけて IT マネジメントをやりましょうという体制になったが、ステータスとかキャリアには繋がっていない。

○　評価結果の公表の件は、私も気にはなっている。私は、基本的に公表すべきだという意見であるので、公表したくないという意見には、身につまされながらも若干引っかかっている。しかし、いろいろな角度から、いろいろな視点で、純粋なセキュリティとかリスクマネジメントの視点以外の視点でプレッシャーがかかっているのだろうなと言うことは感じている。今回の意見を聞いて、国土交通省及び外務省でもそうなのだなと感じた。

○　予算の件については、かなり難しいと思っている。これは結局、予算の柔軟性と透明性を確保する、この二点のせめぎ合いをどうするかということで、要は柔軟に策定してしまうと、透明性が見えなくなるので、そこのバランスをどうとるかということが問題である。例えば、情報セキュリティの投資効果が明確に表現出来るのであれば、かなり可能であるが、実際には、説明出来る方が少ないという現状である。

○　２年で人事が変わるというのも、人事の透明性と経験を積ませることとのせめぎ合いのところであり、どのようなバランスにするかということは、正直、私としても答が欲しい。

○　国益を損ねるかもしれないが、この種の検査結果は、どんどん公表すべきであると思う。また、次のステップとして、極端なことを言えば、システムに登載されているソフトェアのレベルも評価し、公表すべきであると思う。確かに瞬間的なリスクはあがるかと思うが、現在の実態として、相当いい加減なソフトが作られている可能性もあり、これは、公に出して透明性を高め、第三者の目で評価をしないと、絶対改善されないと思う。サーバーと電子メール、ウェブサーバというレベルではなく、登載されているソフトウェアのレベルを全部洗い直し、公表すべき。

○　前の会社で十数年官公庁営業をやっていた経験から言わせていただくと、官公庁の調達は大手メーカーへの「丸投げ」に近く、自ら仕様書を書けるレベルになっていない。そういうこと自体、調べてきちんと発表してただきたい。予算の問題以前に、はるかに大きな問題が潜んでおり、実際には非常に安いコストで更新したり、メンテナンスできるシステムを、丸投げしているが故に、コストが高くなっているという例がたくさんある。この手のことを全部、透明性をもって発表する必要があると思う。特にセキュリティの部分、セキュリティのコア部分については、かなりきちんとしたアーキテクチャーデザインがない限り、やはり問題をどんどん起こすので、業務用システムにおけるセキュリティ部分のコア部分のレベルも含め、きちんとした調査と発表をやるべきだと思う。

→　調達の件について。少なくとも当省においては、そのようなことはない。昔から、当省においては仕様書を自ら書ける技術者を育てている。また、最近は各府省庁とも、CIO 補佐官によってきちんとチェックされていると聞いている。さらに、分離調達のガイドラインもできているという状況下である。特にここ１、２年は、各府省庁とも自ら仕様書を書き下しており、大手メーカーに「丸投げ」という状態ではないと認識している。

○　資料の１（２）、カウンターインテリジェンスとの関係について。意見はわかるが、問題は、どこからどこまでがカウンターインテリジェンスの観点から機微のものであるか、グレーゾーンがどのくらいあるかというのが明確でないことである。機微な部分については、アンタッチャブルだとおもうが、どこからどこまで区分けするか、どこからどこがグレーゾーンかということについては、NISC と議論した方が良いと思う。全ての外務省の情報はさわってはいけないというのは、国民に説明出来ないと思うので、その点は考慮していただきたいと思う。

⑸ 自由討議

本日のヒアリングの内容などを踏まえ、自由討議を行った。

○　本日の話を聞いて、金融機関にもなお課題はあるが、比較するとまともに取り組み、対策が相当進んでいるように感じた。政府機関は、かなり対策が遅れており、意識は低く、甘えている。このような状況が明確となったので、敢えて申し上げると、本日の議事は内閣官房長官からの厳重注意を付した上で公表するか、マスメディアに大きく取り上げてもらう位の

ショック療法が必要なのではないか。中小企業とか個人とかの話をする前に、政府機関を立て直す必要がある。このままだと、「まずは政府機関対策が急務であり、重要インフラなどの対策は自ら推進しているので、政府は関与せず放っといてくれ」ということになりかねない。

○　IT の責任は基本的に提供者・消費者のどちらにあるかという議論があった。通常の製造物の場合は企業と消費者で情報の非対称性があるので、事業者の責務を強調することがもっともだと思うが、インターネットの場合、情報の真偽はさておき、その殆どは各所に開示されており、情報の非対称性が限りなくないと思われる点、一般の消費者保護議論とは差異が存在する。敢えて申し上げると、「多少痛い目にあって学ぶことが必要悪として仕方がない」面もあるのではないかと思う。消費者保護の精神は理解した上で、自ら学ばない人までが完全にセキュアなサービスを求めることには無理がある点を、改めて主張しておきたい。

○　今までいろいろな意見が表明されたが、皆視点が少しずつ違っているように感じる。一例を申し上げると、第１次基本計画の場合、第３章で「今後３年間に取り組む重点政策」と書いてあり、その第１節には「対策実施４領域における情報セキュリティ対策の強化」とあるが、IT を考えたときのセキュリティの対策であるとか、具体的に何をやらなくてはいけないかというのは、非常にわかりやすい。ところが、御意見を聞いていると、いろいろな御意見のなかに PDCA という言葉があったり、視点がいろいろと違うように思う。

○　個人的には、いろいろな領域、政府機関・重要インフラ・企業・個人といった様々な観点で、セキュリティ対策前の全体をマネジメント管理していくことについて、共通認識を持ちたいと思っている。今世の中で言われているのは、企業の資産という意味の情報、おのおのが持っている資産という意味の情報だが、その資産を如何に守るかといった観点で軸がいくつかあり、例えば、人・組織、IT システムの構築・運用、インシデント対応、継続性・BCP などがあるが、これらは、政府機関・重要インフラ、企業等で視点が異なる。これを同じ土俵のなかで議論すると、たぶんかなり脆弱性が見えてくる。その中でいろいろと考えていき、リスクを評価するというリスク分析が必要である。そうすると、セキュリティの要求事項、我々が取り組むことが明らかになり、それに従って推進することになり、具体的に対策の議論が出る。また、ここも具体的に「第１次基本計画」で書いてあるが、「横断的な情報セキュリティ基盤」というのは、おそらく個々の領域とは異なる、共通軸として持たなくてはならない基盤であり、色々あるのではないかと思われるが、そういう議論も別軸であるのではないかと思う。このようなコンセプトの共有化が、次回ぐらいに議論できれば、議論が多分かみ合ってきて、第２次基本計画が書きやすくなるのではないかと思った。

○　今の御意見は、対象をどうするか、アプローチをどうするかという重要な論点であるため、次回以降の検討に非常に重要になると思う。

○　今の御意見に同意。情報セキュリティという言葉を聞いたとき、ある方は消費者広報を思

い浮かべ、ある方は情報セキュリティで政府が公表する中身の話をし、あるいは重要インフラをどう守るかということを考える。大きく分類すると、「情報そのものを守ると言うことをどのように考えるか」と「通信手段又は重要インフラについて、有事又は非常時の時にどういう機能をたてるか」という問題に分けられるのかもしれないが。

○　先ほど「リスク」という言葉で表現したが、どういった脅威に対してどういった対策を想定するのか、個々で想定する脅威についてある程度類型化して認識を合わせ、各類型毎の脅威に対する対策について議論しないと、余りにも幅広い議論が起きて議論しにくいので、順番に論点整理して議論した方が良いのではないかと思う。

○　先ほど、リスク評価という話があったが、やはりメリハリがついた対策を推進しないと、各省庁が指摘したように、対策疲れになるだけで対応が出来ないということが起きると思うので、やはりメリハリが非常に大事だと思う。そのためには、何が重要かをきちんと分類し、リスク調査を計画的にやって行かなくてはいけない部分があるだろうと。

○　今日のヒアリングで、色々と不安があって規制をしっかりして欲しい、という議論があったが、僕は危険な兆候だと思っている。何でも規制するというのはおかしなことで、IT の発展にもならないし、社会も閉塞してしまうと思っている。私見としては、色々な問題が起き、これが社会的に重大な問題へ発展する可能性があるとき、これを速やかにキャッチし政府として必要な対策をすみやかに取れるような柔軟な体制を作ってもらいたいと考えているが、そうすると、今回の全体計画は、柔軟で機敏性を持った計画にする必要があると考えている。新たな脅威が次々と出てくると思われるが、計画に全て反映させるのは困難なので、柔軟性を持った計画、組織が柔軟に対応出来るような計画にすることが今後重要になるのではないかと思う。

○　「リスク」という言葉一つにしても、結構学問的にも違っている。経済学で「リスク」というのは「予測可能な危険性」のみを意味し、全く何が起こるかわからないものは、「リスク」とは定義しない。これは「不確実性」と定義する。他方、災害研究では、全部ひっくるめて「リスク」と定義する。

○　用語を定義し、どういう論理構造を持ってアプローチするか、法律的な責任、政府・民間企業・個人がどこまで責任を負うか、自己責任をどういう範囲でするかと言うようなことも、ある程度議論すべきではないかと思う。

○　リスクマネジメントに関する意見に同意。実は、政府でセキュリティポリシーを作りなさいといったのは５、６年くらい前、結構前からである。しかし、なかなか進まなかったと言うのが実態としてあり、昨年から政府機関統一基準という形で、具体的にこのようにしてくれと言い始め、これを公表しますという話になった。そういう意味では、リスクマネジメントの観点を忘れてはいけないと思う。

○　リスクマネジメントの観点は前提であるが、具体化の方法も具体的に考える必要があると思う。今日のヒアリングを聞いていても、具体的なところが少し見えづらくなってきているという印象。ISMS やリスクマネジメントについては書籍に書いてあるが、具体的にどうなのかということが少しわかりずらくなってきた気がするので、その辺も必要かと。

○　企業でも、対策の一つとしてセキュリティポリシーや対策基準、ガイドラインを策定するが、ユーザーが何をやれば良いのか十分理解していない。全体のルールである以上、セキュリティポリシー等の策定は必要であるが、オペレーションがものすごく大切であり、何をやればよいのかが明確になるようにしないと、なかなか実効性が出ないのではないかと感じている。

○　消費者団体の発言を擁護させていただく。資料にもあるように、消費者団体も「利用する側、提供する側ともに使い方によって、過度の監視社会・管理社会になってしまわないように」と言うことを言いたかったのだと思う。インターネットだけに特定すれば、情報の非対称性が限りなくないようにも思えるが、消費者団体からは、機器の安全性の問題やウィルス対策ソフトの問題など、幅広く色々な点が出された。消費者は、今、自分たちが手につけられない問題がたくさんあって、どうしたら良いかわからない状態にあり、そこの所は是非くみ取っていただきたいと思う。

○　ここには色々な立場の人たちが集まっている。ある程度予測可能な部分も見えない部分もあるが、それぞれが自分たちの持ち場で何ができるのか、それを考えるのが多分この場だと思う。議論を避けるのではなく、お願いするべき所はお願いし、取り組むべき所は取り組むというように、事業者なり消費者なりがきちんと表明出来たら良いと思っている。

○　これからまとめて行くに当たっての要望であるが、到達点のイメージを出していただきたい。すなわち、計画全体について、委員会で最終合意まで持って行かないといけないのか、あるいは、各委員はそれぞれの立場でものを言うだけであり、それを事務局がまとめるのか。また、到達点の一つのイメージとして、第１次基本計画があるが、第２次基本計画は、第１次基本計画の書きぶりや粒度から逸脱しても良いのか、それを踏襲すべきなのか。基本的な方針が明確でないと、議論の方向が全然わからなくなるため、思考をまとまらない状況である。

○　第１次基本計画の評価が必要ではないかと思うが、どうするのか。検討しているなか、どこで出てくるのか、あるいは出てこないのか、お聞かせいただきたい。

○　第１次基本計画の評価であるが、今、2007 年の評価をやっており、多分第４回会合には、途中段階のものをお示しすることができると思う。最終的には、GW 前くらいに世の中に公表できるよう、作業している。

○　到達点のイメージについて。第２次基本計画を決定する権限は情報セキュリティ政策会議にあるが、この委員会では、その原案についてある程度策定することを考えている。

○　第１次基本計画を逸脱して良いか否かについては、恐らく枠組みの議論を今後やることになるかと思うが、対策実施４領域及び横断４分野ということでよろしいかどうか、それ以外の枠を作るべきかどうか、その中をどうするかというのは、この場で議論し、ある程度各委員の合意を得ていく部分ではないかと思う。ただ、第１回の議論でも出ているが、抜本的に改めるということは、事実上は難しいと思う。実現可能性との兼ね合いのなかで決まっていくのではないかと思う。

○　この委員会を立ち上げる前、山口補佐官と話をしたときには、第１次基本計画を踏まえた形で、第２次基本計画はどこにウェイトを置くのかと。第１次基本計画の時は、これから高度な情報社会が始まるにあたって満たさないといけないものがあり、それは情報セキュリティの話であるが、どうそれを考え、どう実装するかということだったと思う。他方、今回の第２次基本計画の時には、情報システムはかなり社会に組み込まれた、例えばSuicaのシステムとPasmoのシステムのように非常に複雑なシステムが使われているが、その中で生活がどうなっていくか。あるいは、かなり情報システムが組み込まれた時にどう運用していくのか、というのが重要になってくる。すなわち、第１次基本計画の時から明らかにステップアップしたインフラの中で、情報セキュリティをどう考えるのかということが焦点であると、山口補佐官とのあいだでは合意をした。各委員それぞれ知見を持っているので、その知見をフル動員したいという形になっているので、よろしくお願いしたい。

○　今日も色々な意見が出たが、これだけセキュリティ対策を実施しろと言っていても、これだけ進まない部分があるというのは、やはり、言っている内容に問題があるのではないかと思う。一番の問題は、コストがかかりすぎる、手間がかかりすぎるということであると思う。確かに、情報セキュリティ対策をやるためには、リスク分析があり、脅威評価があるが、情報セキュリティ対策の手法そのものが進歩しておらず、昔から結構変わっていない。パッチ当てるなどの決まった手順があり、それをやらないといけない。そして、それを如何に浸透させるかということで、ショック療法などの話がすぐに出てくる。もっと安く、簡単にできる方法について、きちんと考えていかないといけないのではないかと思う。

○　例えば、外務省の報告にあった、いろいろな国にいろいろなシステムがあるので対策を推進するのは困難という話だが、確かに、今やれば難しいかもしれない。しかし、今からもう一度考え直し、もっとITの事情が悪いところでもセキュリティが確保出来るシステムというのを考え直せばよいのであり、今のシステムに基づいて一生懸命やること、それにお金をかけることも良いが、もっとお金がかからないで国家機密が守れるようなシステムを考える方も結構大事なではないか。

○　情報セキュリティのコストというものを大きなテーマに設定していかないと、対策疲れ、疲れるのは全然構わないのだが、人・物・金は全てコストでありこれを下げていかないと、政府としても大企業・中小企業にしても、セキュリティにお金を取られてしまうだけになる。セキュリティ自身は、収益にも国の発展にも繋がらないのではないかと思うので、時間がかかるとは思うが、もっとシームレスでコストダウンできるような仕組みをきちんと考えていかないといけないのではないかと思う。

○　次回、第４回会合で評価の大枠の結果が出てくるとのことであるが、評価の対象は、「第１次情報セキュリティ基本計画」に対してどういった評価がされているのかと言うことか、あるいは、今までで色々やった評価の最新版が出てくるのか。

○　第１次計画の個別の文言に対する評価ではなく、この計画に基づいて行った施策も含め、全体的にこれまでの取り組みはどうだったのか、その取り組みによって、対策実施４領域及び横断４分野がどのように変わってきたか、これらを説明する予定である。

⑹ 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。