情報セキュリティ政策会議　基本計画検討委員会
第１回会合議事要旨

１．日　時

平成 20 年１月 16 日（水）　13 時 00 分～15 時 00 分

２．場　所

内閣府別館会議室

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
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）
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)　内閣官房情報セキュリティセンター　センター長挨拶

(2)　委員長の選出

○　須藤委員を委員長に選出

(3)　須藤委員長挨拶

(4)　会議の公開等について

○　事務局より説明、原案のとおり了承

(5)　我が国政府の情報セキュリティ問題への取り組みについて

○　事務局より説明

(6)　「第２次情報セキュリティ基本計画」（仮称）に係る検討の視点（例）

○　事務局より説明

(7)　各委員の意見開陳

○　資料５の内容を全部議論することは大変ではないかとの認識を持っている。メリハリをつけて議論する必要がある。

○　「組み込まれない組み込みソフト」、すなわち、携帯電話などにダウンローダブルな、デバイス上で実行されるソフトが増えている。情報家電の分野でも急速に進展する可能性がある。これを考慮したとき、組み込まれたソフト、ベンダーなりサービス業者が普段は管理し、必要に応じてダウンロードして使われる「組み込まれない組み込みソフト」、そしてその間をつなぐ有線及び無線のネットワーク、この全体を考慮したときに、社会がきちんと機能して行くようなセキュリティの考え方を作る必要がある。

○　社会における情報セキュリティ問題を考えるとき、企業のサーバーなりメインフレーム上で実行されるソフトを中心に据え、そのネットワークの話をする人が多いが、組み込みソフトに関する問題は、企業側から考えていく方がコントロールしやすいと思う。携帯電話の組み込みソフトが企業側から自動的に更新されていることなどを考えると、企業側からコントロール可能であるということであり、これを踏まえながらテーマ設定していく必要があるのではないか。

○　情報セキュリティに関する業種ごとの一定のルールなりガイドラインなり規制のなかに、ソフトウェアの側面からの考え方が入っているか、疑問を持っている。今後、入れていく必要があるのではないか。

○　ソフトウェアやネットワークの品質や信頼性に関しては、規制派に近い考え方を持っている。

○　データにもあるように、ほとんどの個人は情報セキュリティ問題を余り意識していないという、乖離した状態があるのではないか。これは、役所に勤務している人にも恐らく存在し、そのため、時々ファイル交換ソフトによる情報流出が起きたりしているのではないかと思う。

○　「第１次情報セキュリティ基本計画」は、政府の政策が主に記載されているが、このような状況を考えると、政府にかなり比重があるというのは変えないといけないのではないか。インフラとして、身近な生活のなかにＩＴが入っている状況では、全体の比重を考え直さないといけないのではないかと感じている。

○　個人的に思うのは、安全も必要ではあるが、非常に不便になったとの印象を持っている。

インターネットがない時代から、情報が盗まれたり情報のネットワークが妨害されてきたことを考えると、情報伝達のネットワークを完全に守るというのは、多分無理なのではないか。

むしろ、技術を駆使し、届けるデータや情報そのものを守ることが大切であり、技術開発を進める必要があると思っており、また、利便性も確保しなければならないと思っている。

○　単に「守る」ということだけではなく、産業界において情報セキュリティに関する研究開発費が増加して研究が活気づき、日本が情報セキュリティに関する世界標準を作れるようになる基本計画になれば良いと、個人的には思っている。

○　情報セキュリティの分野においては、信頼できる統計データがないのではないかと思っている。

○　毎年、50 万人から 60 万人が大学を卒業するが、情報系の学科を卒業する人数は僅か１万人、多く見積もっても２万人しかいない状況であり、また、それ以外の学科の学生には、系統だった形で情報教育が行われていないのが現状である。

高校以下についてみても、高校では教科「情報」が出来たものの、大学入学試験に関係しないため、「情報セキュリティとは何か」というレベルの議論・授業は行われていない。中学以下については、教科自体が存在していない。

○　長期のスパンで問題を考えるのだとすると、初等中等教育のレベルから考える必要があると思っている。情報セキュリティを専門とする職業につく人のレベルを上げるためにも、全体のレベルを引き上げる必要があると思っている。

○　情報システム環境について、ユーザーの立場から見ていると大変違和感を感じることが、実はたくさん存在する。

○　情報セキュリティの問題は、企業にとってかなり深刻なリスクコントロールの問題である。多くのパートナー企業との間で機密情報を含む情報をやりとりしながら仕事を進める必要があることを考えると、自社だけが情報セキュリティに関するルールなどを作ったとしても、情報セキュリティの問題に対応出来る訳ではない。

○　情報セキュリティの問題と地球温暖化の問題では、似ているところがある。どちらも、部分的な問題は露呈しており、問題意識は持っている反面、すぐには大事にならないだろうという油断がある。

この問題は、どこから手をつけて良いかが極めてわかりにくい問題であるが、結局は、みんなが意識をもって、一つ一つの取り組みを積み上げていかないと解決しないと感じている。官と民では異なるところもあるかもしれないが、共にきちんと対応していかないと、これからの情報通信社会のなかで、大変大きな問題になってしまうのではないかと感じている。

○　資料５には非常にたくさんの論点が提示されているが、これをどのように絞り、どのように焦点を当てていくかを考えながら議論して行く必要があると思っている。

○　コンピュータシステムの開発に長く関係してきた立場から見ると、単独に存在するシステムが減少し、いろいろなシステムがネットワークでつながり始めたことが最近の特徴ではないかと思っている。その結果、一つのシステムの問題がネットワークを介して非常に広い範囲に影響を与えたり、ネットワークが止まるとシステムの大事な機能がほとんど機能しなくなってしまうということも発生しているのではないかと思っている。

○　昨今、メールによる情報交換量が多くなっており、コミュニケーションの手段として、大

半の比率をインターネットに依存し始めている。これは、非常に重要な通信からどうでも良いようなものまで、ほとんど無法地帯に近いような形でいろいろ使われているが、これが一旦止まった時にどうなるか、非常に心配している。

情報を守るという論点のほかに、通信手段としてのインターネットが使えなくなったときに、どうやって通信手段、コミュニケーション手段を確保するかということは、社会として非常に重要な問題なのではないか。

○　政府機関や重要インフラなど、どんなときでも事業継続が必要なもの、通信手段を確保しなければならないものがあると考えている。被災時や有事においても通信手段を確保することは政府としての役割であり、政府として確保しなければいけないもの、あるいは法律・組織によってバックアップの手段を用意しておくべきものについて、きちんと整理し、万一の時にも機能する仕組みを作ることが必要であると思う。

○　国として公的に、どうしても社会の秩序維持・機能維持のために準備しなければいけないものの整理と、個人のレベルの情報セキュリティ教育・リテラシーの問題といった情報セキュリティの問題は、若干質の異なる問題ではないかと考えている。

○　“情報システム”のセキュリティの話と、“情報”に対するセキュリティの話を分けて議論していきたい。一緒に議論すると、何だか訳が分からなくなり、解決したような気になる。情報視点、情報目線というのか、情報資産というものに対してどう判断していくかということは、結構重要なことではないかと考える。

○　どのようにセキュリティシステムを監査していくか、保証するのかということを何年も実施してきているなかで、セキュリティマネジメントシステムが有効に働いているか、今は格付けという話もあり、監査で保証できるのかという話もある。

○　監査で保証できるかという問題で悩むのが、対象となる情報の価値をどう見るかという点。

○　情報の価値が一義的に決まれば、対策費用、対策費の効果が出てくるのではと思うが、「いや情報の価値など決められない」という話になる。価値は、人間が考えて与えているものであり、雰囲気で決まっているものかもしれない。雰囲気は流れるものであるから、フィードバックでグルグル回って、どこかで収斂していく回路がつくれれば、そういうことを軸に何か施策が出せればと感じている。

○　１万５千人以上を動員しているインターネット安全教室での報告、全国 40 ヶ所ぐらいの連絡会議での声では、1 万５千人くらいの一般の皆さんは確かに「解りました」、しかし「で、どうしたらいいのですか、で、私はできません。」という状況。そういった方々をどうやって救っていくのか、手をさしのべるのかという問題がある。

○　この会議で、一個一個の正解を出すことはあまり望まない。正解が出てくるようなシステムを作っていく、そういう組み立てが出来れば非常に嬉しい。もし、正解を出してしまうことをやれば、統制社会とか統制強化になっていく可能性もあり、そういうのはあまりよろしくないと感じている。

○　地域社会、中小企業は非常に厳しい状況にあり、情報セキュリティのことを考えている企業は本当に少ない。地域の経済事情が非常に厳しい中で、情報セキュリティについて意識のある経営者が少ない。

○　子供たちを取り巻く情報の環境、その状況に対して、子供たちがどう対応していくのかを

議論していきたい。

○　生活経済のインフラとして情報通信は非常に重要。利便性と安全性のバランスをとっていくことが大切と思う。

○　新聞・テレビ等で生活者・消費者重視の政策が報道され、安心・安全の確保ということで「消費者庁」の構想まで各党がいろいろと取り組んでいるが、この中で情報通信という分野が出てくる比率は非常に低い。ほとんどカヤの外にあると感じる。

○　内閣府国民生活局の国民生活審議会などで消費者基本法や消費者基本計画を策定した際も情報通信は大事だということは誰も否定しないが、どのように消費者政策をやっていくのかということになると、皆何も言えなくなってしまう。隠れた消費者問題が情報通信、セキュリティ分野にはあるのではないか。

○　モバイル、ＩＰ端末、機器・サービスの問題、ＡＤＳＬ、光、ＮＧＮ等のいろいろな研究会・懇談会等があり、最近ではデジタルディバイド解消戦略会議、重要通信の高度化のあり方に関する研究会等も開かれているが、これらを全部束ねて横断的にセキュリティという角度から整理していくということが大変重要だと思う。

○　ＩＴ内部統制整備も各企業で取り組んでいるが、この中でも情報セキュリティのテーマは非常に重い。

○　メディアリテラシーの関連、消費者にどのように情報発信をしていくのかということも一緒に考えて行きたい。

○　第一次基本計画に関してはバランスが取れていると感じる。論点ペーパもこれ自体公表価値がある的確な論点が多数並んでいるが、盛り沢山過ぎるため、このままフリーディスカッションすると発散する可能性が大きい。バランスを取ること、重要事項をこの中から選抜することが大事だと思う。

○　「リスクベースドな議論」が必要。情報セキュリティの分野では、ともすれば機密性（狭義のセキュリティ）だけを議論する方がいる。「非常に危険だ」ということはいくらでも言える。全体の鳥瞰図的なことから言えば、金融機関経営の中で信用リスク等いろいろなリスクがあるが、例えばインターネットバンキングは市銀決済の中で数パーセントのシェアしかない。その部分が危険と言われても、民間経営である以上、そこにだけ多大なコストをかけることは無理がある。この辺の感覚を、バランスをもって議論したい。

○　足下の議論のなかで、「将来の可能性」を議論することも気になる。先進的な、近未来に起こり得る話を展開していくと（防衛大臣が話していた）「ＵＦＯが来て攻撃されるかも」的な話だって有り得るかもしれないが切りがない。ＩＴ障害対策のように、従前からあるが解決していない問題も目の前に山ほどあるので、どちらに力点を置くのかということをオーダーしていただければと思う。

○　第一次計画では１点だけ、不適当と思われる記述がある。「ＩＴ障害／ＩＴ利用不安を限りなくゼロにする」という、目指すことは自由だが、30 年先の夢のようなことを宣言している。システムを通常のコスト観念の下で開発・運用すれば一定の障害は絶対に起こるので、この書き方は訂正しなければＩＴ常識人はやる気が出ない。喩えれば「風邪をひく人をゼロにします」と宣言するのと同じで、「風邪やインフルエンザは避けられないが、新型インフルエンザがパンデミックになることは防ぎたい」といったメリハリをつけて表現しないと拙いので

はないか。

○政府、民間企業・個人の関係で、政府・省庁はしっかりやっていただきたいと思う。重要インフラについても、確かに重要なことをしている人は、自らしっかりする筈と言えるが、企業や個人まで「みんなしっかりしろ」というのはお節介な感じが否めない。原則は自由、市場原理に任せるという部分が当然あるべきだと思う。

○　極めて重要なところだけ、「このように重要だから、このように関与する」という整理を是非お願いしたい。金融界、銀行等で一例を挙げれば、ＩＣカードへの一斉切り替え、すなわち「磁気カードをある日をもって全部廃止する」ような話は、政府、国が音頭を取らないと困難である。それ以外のセキュリティ対策は、各民間企業等がそれぞれの経営判断で実施し、金融庁や日銀が検査・考査等でチェックする等、相応の管理プロセスが存在する。

○　ＩＴ、とりわけ先端技術や人生は、危なさと魅力が裏腹の関係にあり、「100％安全だと言えるような人生（や技術）は面白くない」という面がある。その辺りを含め、バランスの取れた議論を切に願う。

○　ある大学病院の院長がおっしゃるには、50 歳以上の病気保有率は 70 パーセントを超え、病気に打ち克つという言葉ではなく、病気と上手く付き合わなければいけないとのこと。そういう発想で、この問題も社会システムのなかで生きている限りはどうやってリスクと上手く付き合い、対応をたてるかという観点は重要かと思う。

○　セキュリティのインシデントはゼロにはならないのではないか。多分「ある」というのを前提に、レディネス、レスポンス、リカバリーという運用のスタイルを非常に上手く連携する枠組みと実働するアイデアが是非盛り込まれると良い。重要インフラの中でセプターカウンシルが議論されているのもその一環と思うが、その一つ先を見た枠組みを是非書いておきたい。

○　リスクベース、情報資産価値という話があったが、諸官庁のシステムを如何にインフォメーション・セキュリティ、マネジメントを確保するかという観点の規準があるが、具体的にそれを測定し評価して、どうあるべきか、というところが現状弱い。この辺のアプローチをもう少しきちんとしたいという思いがある。

○　認証基盤、日本の暗号を考えるなど、何か世界をリードする基盤、メカニズムが提唱できるようなところが、非常に難しいところだが、盛り込まれると非常に良い。ＩＣカードの話があったが、そういったところの先導も基本計画の一環と考える。

○　国際連携という観点も、いろんな議論の中で結びついてくると考える。

○　部分最適か、全体最適かという点に関して。業務の内容に応じて様々なシステムの作り方、運用の仕方がある。一般的には全体最適、一様な何かがあるというような施策が一番よいだろうが、一方、実効性、如何に効果を上げていくかという場合、実際のオペレショーンを離れ、過度に一般的にすると使いにくい。いろいろな取組みの実効性を如何に確保するかという観点が重要だと感じる。

○　一切起こさないということだけ考えていると、いざ起きたときにどうするかということに、なかなか話が行かない。起こさないということを十分やった上だが、一旦起きたときにその影響を如何に限定するか、影響が及ぶ範囲を少なくするかということも極めて大事なことだと思う。

○　一旦起きたときにどのように復旧していくか、或いは限定的にしていくかという観点も議論したい。
○　電子政府の効率化、最適化では外部のＩＴ専門家をアドバイザーとして入れ議論を行っている。各省庁の中にはセキュリティに対する専門家も入れてセキュリティの議論も行っている状況。
○　政府機関統一基準の中で、最高情報セキュリティアドバイザーというものも定義されており、各省庁の中に外部のセキュリティアドバイザーをコンプリーティングしていくといった状況も生まれつつある。
○　政府機関統一基準が制定されて約２年経つ。政府機関のセキュリティ評価、ＮＩＳＣでの評価や自己評価等が公表され、自分たちの省庁がどういう状況にあるかといった幹部の認識、職員の方、約 80 万人が統一基準四百数十項目の同じようなポリシーをご覧になるという状況が生まれつつあり、やっとというと申し訳ないが、「気づき」が出てきたと思う。
○　政府機関の自己点検で一個一個を見ていくという中で、いろいろと具体的な課題が出てきている。具体的にはどうやっていくのか、監査体制をどうするのかといった具体的なところが今回の議論になるのではと思う。
○　いろいろな記事を見ても回避・転化という話はあるが、リスクの“保有”という言葉が消え去ってしまっている。その結果、単純に紋切り型で厳しくやるという状況が出てきている。厳しくするだけではなく、事故が起こったときのＢＣＰ的な対策を含めて考えると、代替策（アルタネーティブ）といったものを含めて考えるといった観点で見ていきたい。
○　セキュリティのいろいろな会議に出ると、大体同じ方が出ていらっしゃる。その状況が悪いというか、やはりまだ市場が狭いと実感させられる。技術論から法制度の話まで、コンサルタントが全部できないと、ほとんど仕事にならないような状況もある。法制度、ビジネス、技術の話までを全部一人でやるというのは、産業としてかなり厳しい。若干階層モデルのように出来ないかと思っている。答えは見えていないが、そういったところも少し頭に入れつつ、と思っている。
○　専門用語が解らない等で部下が何をやっているか分からない、マネジメントができていないという状況がある。政府、民間企業、大学等でもそうだが官房長・審議官級から企業でいう部長級、課長級、主任級のような階層的なものも考えなければならない。
○　日本学術会議セキュリティ・ディペンダビリティ分科会で、セキュリティとディペンダビリティがどのような形で今後発展していくべきなのかという議論がある。セキュリティは様々なインフラストラクチャーの中で使われ、かつ、それがネットワークを通して複雑に関与している状態の中で、リソースを結びつけることで良いソリューションが出る可能性もあるが、各組織が独立的に議論し、若干統一的な見解が見出せないということが問題と感じている。様々な分野の方が参加される委員会で、統一的な施策・セキュリティに関する施策という観点で議論に参加したい。
○　ＩＳＯの国際標準化の中で、セキュリティの実現のために必要な暗号、電子署名（デジタル署名）、認証等の国際規格制定、我が国の規格を国際規格にしていくという活動がある。セキュリティ対策の国際的な観点で議論に参加したい。
○　セキュリティというと暗いイメージ、病気と一緒に生きていく、病気対応する研究のよう

な感じだが、セキュリティを使うことで、新たなマーケットを創出できるという観点で、意見を述べていきたい。匿名性を保ちつつ、悪意あるユーザーを特定するといった技術もあり、守るためのセキュリティではなく、新しい市場を創出していくという観点の技術も提案していきたい。

○　e-コマース等で大規模なサイトを運営している大企業でも監視サービスへ費やす予算は少ない。（月 20 万円程度）それでも高いという意識もある。中小企業の意識としては、情報漏洩対策サービスがあったとして、支払おうという金額は更に少ない。（月 5,000～10,000 円程度）プライバシーマーク／ＩＳＭＳ取得へ向けた取組みで更に費用が必要となる中、（Ｐマーク 300 万円、ＩＳＭＳ　500 万円等）、またプライバシーマーク取得企業で、情報漏洩が発生している企業の数が５パーセントある等のデータもある中で、もっと実効性のある対策が必要なのではないか。

○　技術だけで何でもできると考える訳ではないが、情報セキュリティをやりたい中小企業向けに、情報資産の棚卸し、資産の価値を洗い出してリスク分析を行い、対策をとる（プラン・ドゥ・チェック・シーを行う）、情報セキュリティ担当委員の任命等といろいろ行なっても、答えとしてたいしたことにならないような感もある。

○　情報セキュリティの監視サービスを行っているトップシェアの企業でも抱える顧客は３百数社、全体でみても監視サービスを受けている企業は 1,000 社も無い状況。中小企業向け、大企業の下の方でも、リスク分析等よりもっと安価に、効果があるもので技術的な対策を具体的に明示し、それをマスト条件とする、そういったことを行う技術者／技術会社をインフラとして提供する必要があるのでは。

○　経済産業省が支援するセキュリティキャンプで、１０代の方にセキュリティを教える活動を４年間行ってきた。毎年、三ー四十人が育っていく中、スキルを生かせる次の進学／就職先がない状況。情報セキュリティは幅広い知識、深い知識と経験が必要で、実務を知らないと出来ない側面も当然あるが、高いモチベーションをもった若い技術者・コンサルタントが働く場所・地位等の確立が必要。また、企業あるいは官庁の中で、情報セキュリティを行う人の社会的な地位の確立、地位を見出せるような政策としての作り込みが必要と思う。

○　サイバー犯罪や情報セキュリティについての法的な観点で意見を述べていきたい。

○　ある程度高いレベルの対策が為されていても問題が発生してしまう「そこそこやっている」という状況になってしまっている。対策への投資効果が見えていないのかもしれないということで対策が進まない、障害が起こってしまうとう状況ではいけない。

○　情報セキュリティに対する規範性、クライテリアのようなものを準備しなければならない段階か。いくつかある規準、スタンダードをもう少し具体的、拘束力をもつ形で、“規則の規”を書くという方向性を打ち出していけば、社会的な障害を抑制し、損失を小さくできるのではないか。

○　個人へ目を向けると、第一次基本計画ではＩＴ利用に不安を感じる個人を限りなくゼロにするとあるが、お仕着せ・押し付けではなく、自分のマインドとしてセキュリティに不安を感じ、あるいは自分からセキュリティのリスクが出ないように対応するという方向を目指す、個人全体がセキュリティを検討することで、いわゆるセキュリティ文化というものの実現が出来るのではないか。

○　セキュリティ倫理の教育、セキュリティ教育等を推進し、個人自ら、例えばＢＣＰ（ビジ

ネスコンティニュイティープラン）ではなく、個人行動のビヘイビアコンティニュイティープランあるいはビヘイビアコントロールプランのような､個人が自分でパニックにならずに、どう行動すればよいのかという意識の観点が重要ではないか。

○　重要なのは、予防の観点、運用の観点、それから起こったときの対応、リカバリー、その各フェーズに応じたことを実際にどう動くかということを考えないといけない。

○　深夜ＮＨＫで、「地震が発生して、まもなく大きなのが来ますから」というのがあったが、ずっと身構えても来ない。エラーを起こした後の対応を、ちゃんと考えてもらわなければと思う。

○　Suica と PASMO のシステムは、様々な異なるサービスが組み合わさった、高度で複雑なシステム。トラブルが発生すると、かなり複雑な対応を求められる。複雑なシステムに対してどう対応するか、予防するにはどうすればよいかを考えなければならない。国民生活、今のカードの普及を見るとかなり組み込まれており、現実問題であると思う。

○　将来のシステムも考えなければならず、ＮＩＣＴの方でポスト・インターネット研究も今年からスタートする。どういう要件をポスト・インターネットは満たさなければならないかも、情報セキュリティの観点からいろいろとご意見を頂きたいと考える。

○　第一次基本計画含め、最初に行なったことは、リストラということもできるが、ショック療法であったと思う。第二次基本計画を作る際には、規範性の話であるとか、出来る限りいろいろな形で分かっている事、分かっている問題を解決できるフレームワークをきちんと作っていくことが重要だと思う。

○　社会、特に役所の中での記憶喪失の問題がある。これは、人事による記憶喪失、経験を利用しないという記憶喪失、政策が変わることによる記憶喪失もあるが、これに対応できる情報セキュリティ政策が必要である。

○　政策のカスタマーは誰なのかということを明確に考えなくてはならない。消費者・国民だけではなくて、一つは安全保障論、公共の安全という観点があり、これがバランスしなければおかしいことになってしまう。その意味での政策の組み立てがいると思う。

○　個人的に 2010 年問題とか、2011 年問題とか呼んでいるが、暗号の危殆化、IPv4 の枯渇、地上波デジタル放送開始、皆が信頼している PSTN がなくなる、経済システムがかなり仮想化してくる、というようなポイントが 2010 年、2011 年と思っている。おそらくかなり準備していろいろなことを考え、「またやっちゃうのか」ということが起きないようにしなければならない。その問題も今回解いておかなければと思っている。

○　本委員会は、３年間の基本計画を議論する場ではあり、１０年、２０年の長期的なビジョンを考えることは本来の目的ではないのだが、あえて国策としての長期的な情報セキュリティ政策､あるいはもっと大きく国家として IT 技術とどのように関わっていくかに関する意識を喚起してみたい。

○　情報化・IT 化の波は世界的に見ても加速しており、そのトップランナーはいうまでもなく欧州・アメリカで、近い将来には中国やインドを代表とする第三勢力が台頭してくるであろう。われわれの子供が作っていく将来の日本の社会が、10 年後 20 年後に、世界と対等以上に技術的・社会的な能力で勝負していくためには、いわゆる情報力の向上を図っていく必要がある。

○情報力とは、簡単に言えば、情報を取得、処理、加工するという情報処理の能力を表したも

のであるが、将来的には現在国家の力を表現する経済力、工業力、国防力などの尺度と同列に扱われるようになっていくことは想像に難くない。情報セキュリティの施策は、その辺を見据えながら、やっていかなければいけないのではないか。

○　短期計画における各分野でのそれぞれの問題を直しながら、かつ最終的には国家としての情報力を総合的に強化する方向に結果的になっていく、そういう方向づけてやっていければと考える。

⑻　自由討議

⑼　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。