情報セキュリティ政策会議　基本計画検討委員会
第12回会合議事要旨

１．日　時

平成２０年１０月３日（金）　13時00分～ 15時30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
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）
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

（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) 企業・個人分野について

○　企業内CSIRT構築の促進とあるが、CSIRTとはコンピュータ・セキュリティ・インシデントに関するものか。そうであれば、一般的にはＷｅｂサーバなどのインターネット向けのシステム、ＳａａＳがイメージされていると思うが、企業内CSIRTとするとそことはずれる印象があるので、インフォメーション・セキュリティなど言葉を工夫されるのがよい。コンピュータ・セキュリティとしては限定的すぎないか。

⇒考慮させていただきたい。

○　情報セキュリティガバナンスを経営の一環として位置づけることは重要だと思っている。国内のＳＯＸ法やＣＯＢＩＴ等の内部統制について、内部統制ではＩＴガバナンスを確立するということと、そのＩＴガバナンスを経営戦略の中でどう位置づけるかは区別して議論するものだと理解している。情報セキュリティガバナンスを含め、全てが１００％重要であるということは有り得ないため、経営戦略の中で情報セキュリティガバナンスをどのように位置づけるかは、それぞれの企業である程度考えなければならない。

○　企業が情報セキュリティガバナンスをがんばったとして、それをどのようにアピールするかということが気になっている。公開資料で世間へ公開されるとは思うが、その比較できるなどのようなことが制度上できるとよいのではないか。

○　中小企業について。中小企業は数が多いということもあり、個別に研究が進むものではないので、中小企業を対象とした教育といったものが必要ではないか。経済産業省が中小企業のＩＴ化を進める活動を行っていると思うが、そういったものに近い全国的な教育も必要ではないかと思う。

○　「ＩＰｖ６やＮＧＮ等の新しい環境への移行に対応するための実践的な情報セキュリティ人材の育成」とあるが、かなり限定的である。広い意味での技術対応力のある実践的な情報セキュリティ人材の育成としたほうがよいのではないか。新しい環境への対応ということは、これまでも当たり前のように行われているが、技術が意外と軽視されているとは言いすぎだが、企業の中でも技術をしっかり見ていないところがあり、マネジメント側に流れすぎている面もある。支えている根本は技術であるので、その部分を忘れないと言う意味でも、技術対応力のある実践的な情報セキュリティ人材とされるほうがよい。

○　重要なご指摘である。技術的なところにウェイトをかけ、ＩＰｖ６やＮＧＮ“等”とは書かれているが、広い意味でということに留意すべきであろう。

○　情報セキュリティガバナンスの「経営の一環としての位置付け」の確立の中で、関連法制との関係を整理しとあるが、この関連法制とは個人情報保護法などのようなものを念頭にしているのか、あるいは情報に対する窃盗罪のようなものを念頭においているのか。また、法律に対して改正を求めるというより、問題点を整理するといったイメージか。

⇒ここでは、個人情報保護法やＩＴ内部統制を定めるＪＳＯＸ、下請け関係の法制、労働に関する法制など、様々な法制が定められているが、これらの関係について整理していくことが重要ではないかという趣旨である。それぞれの法目的があるので、情報セキュリティという観点で見たときに、どのように整合性をとるのか、関係省庁で整理を行う必要があると考えている。

○　政府調達の参加者への必要に応じた入札条件化等の推進についての検討とあるが、広く一般の企業についての情報セキュリティガバナンスの確立を論じている部分にあり、これは政府調達に参加する企業に示せば、他への波及も見込めるという考え方なのか。

⇒米国では政府が調達の条件を定め、民間同士の取引への広がるなどの面もある。具体的に何ができるかということはお示しできないが、国が行うことが何かデファクトになっていけばよいという期待も込めて記述している。

○　情報セキュリティガバナンスを経営の一環として位置づけることができるのは、経営者、特にトップであろうと思う。経営者の意識を促すようなものが何らか入った方がよいのではないか。財務、会計に並ぶような経営の一環としての位置付けでは、標準資料類を書かされるといった形になる。経営層の捉え方、意識が薄い。経営層が情報セキュリティについて正しい認識を持つことが重要である。経営者に対する意識付けとして、具体的なところでは、情報セキュリティガバナンスに係る啓発は経営層に対して行って欲しい。

○　「事故前提社会」への対応力強化に向けた緊急対応体制・事業継続性確保等の強化については、システム停止、システムが止まった場合に早期復旧を図るというイメージにとれる。一方で、よく起こっているのは情報漏えいである。第１次提言では書かれていたことであるが、事故の内容についての説明責任がある。重要なシステムが止まったことの説明は、事後でも良い。しかし、大量の情報漏えいがあったらしいという場合に、情報漏えいした記録を残してない企業が今は有利であり、それは常々おかしいと感じている。まじめにログを取っているところほど、漏洩の事実が公表される傾向にあり、それはアンフェア

である。事故内容の説明責任が本来あり、そのためには十分な記録、ログを保存する義務、責任があるということは是非書き込んでいただきたい。記録をとらない方がよいといった風潮にならないようにしていただきたい。

○　重要な点であり、その辺りも考慮させていただきたい。

○　ガバナンスについては経済産業省とも議論させていただいている。ＩＳ（インフォメーションセキュリティ）のガバナンスとＩＴのガバナンス、全体を包含するコーポレートガバナンスという概念がある。ＩＳガバナンスとＩＴガバナンスは、ＩＴというファクターで共通事項がある。ここでは、ＩＳガバナンスについて述べられているという理解でよろしいか。「ベンチマーク、報告書モデル、ＩＳＭＳ等の各種対策の推進」とあるが、ベンチマークやＩＳＭＳを使うことがガバナンスの確立ということなのか。ベンチマークやＩＳＭＳでのセキュリティ監査などの活動との関連を整理して、具体的な対策を推進するとした方が正しいのではないか。また、この報告書モデルとは、ここで作られた言葉か。

⇒報告書モデルは、情報セキュリティ報告書のひな形等を作り、それにより報告書の作成を普及させていくということである。ガイドラインをつくるのと同様のイメージである。ベンチマーク、報告書モデル、ＩＳＭＳ等の各種対策を行うことにより、経営者の理解も深まるという主旨で記述している。おっしゃるように、そのような活動を通じてということもあるので、よく咀嚼したい。

○　報告書モデルは情報セキュリティ報告書を使ったやり方のことということで理解した。報告書モデルという言葉はあまり一般的ではないので、括弧書きにするなど工夫されたほうがよい。

○　記述については、文章にする際に入念に練って、委員の皆さんのご意見を仰ぎ、修正を加えていきたい。

○　モデルとなる「取引・契約書」の提示とあるが、情報セキュリティガバナンスの経営の一環としての位置付けの確立を考えた場合、これはどのようなイメージのものか。また、関連法制との関係の整理について、これが経営との関係での関連法制にとどまるのであれば、それは範囲が狭い。個人情報保護法や金融商品取引法などの法律は、情報セキュリティガバナンスを経営の一環に位置づけるには、大きくとどまっている。もう少し考え直すべきというのであれば、異なった視点での提案をする方がよいのではないか。

⇒モデルとなる「取引・契約書」については、企業間の取引で、下請けとの取引、対等

なアウトソーシング等のような様々な取引において、個人情報、顧客情報、企業情報を含めた取り扱いをどのようにすべきかといったモデルを考えている。関連法制度との関係の整理については、広い意味での企業経営では、ＪＳＯＸも個人情報保護法も重要なガバナンスのアイテムとしてあるので、矛盾がないように整理すべきという趣旨である。

○　ガバナンスとの関係で関連法制を整理するというのはやはりイメージが沸かない。また、モデルとなる「取引・契約書」については、契約形態が非常に多様な中、何を情報セキュリティガバナンスの核となるようなものとしてモデルを示すのか、相当書き込まなければモデルにならないのではないか。できるだけ具体的に、どこを核として情報セキュリティガバナンスを取引・契約書に入れていくべきか提案をお願いしたい。

○　ＩＴガバナンスと契約、取引との関係は少し詰めて書く必要がある。委員のご協力もお願いしたい。

○　ＩＴセキュリティ評価及び認証制度の活用推進とあるが、今の取組みも活用推進だとは思うが、これらの評価、認証制度については使いづらいところがかなりある。もう少し整理をした考え方の提示、改良の検討を行ったほうがよいのではないか。そういった点を加えていただけるとよいのではないか。現状のままでの活用推進はかなり苦しいので、検討していただきたい。

○　推進体制の議論の中で、情報セキュリティ製品・サービスのスタンダード化が進むのであれば、そういったものの活用ということを、「企業の情報セキュリティ向上に資する製品やサービスの提供促進と活動の推進」に加えていただければと思う。

○　「日系企業のグローバルな事業展開を支える情報セキュリティ政策の推進」について、今現実的に困っていることは何かを考えると、海外へアウトソースするというビジネスが増えており、その時に情報セキュリティの考え方を整理する必要があるのではないか。環境を整えるレベルも重要であるが、経営者としてどのように情報セキュリティを勘案していくかについて考え方を整理していくことが必要だと思う。

○　重要な点であり、少し詰めて考えたい。

○　昨日、世界ＩＣＴサミット２００８に参加した。そこでは、セキュリティに関して、海外での経験も含めて様々な議論がなされ、ハッと思わされる点が幾つかあった。シマンテック社の会長兼ＣＥＯである、John Thompson 氏のお話が印象的であった。企業では経営陣が関与せよということを強く述べられていた。単純な問いかけから始めるべきであるとし

て、一つは、どのような重要な情報をもっているのか、二つめは、それがどこに格納されているのか、三つめは、それがどのように使われているのか、また実効的なポリシーを立てて組織で共有せよと、四つの点を明確に主張しておられた。それは、企業においてデータ漏洩が増えており、２００７年の侵入が２００５年の３倍になっており、公共政策として加えるべきだということをはっきりと述べられていた。

○　同じく John Thompson 氏が警告していたことは、教育機関への侵入が非常に増えているということであった。増えている理由として、学生はＩＴをよく使い、危険な行為を行っているということで、若者に対して教育しなければならないということを主張されていた。ここでの議論は、若者は義務教育の上に位置づけられるとして、限定した議論しかしてこなかった。非常にＩＴを使う人々である、“若者”という議論をしなくてもよいのだろうかと、昨日のサミットに参加して感じた。また、アメリカの大学機関では、予算は接続を増やすことに集中し、安全に目を向けていないことが問題であるとも述べられており、その辺りは我が国も学ぶことがあると感じた。また、情報漏えいは、教育機関が一番多く、その次が政府機関、医療といった重要なところで発生しているとのことであった。

○　大学については、文部科学省は国立情報学研究所（ＮＩＩ）を通じて、各大学へお願いし、対策を立てていただいている。ＮＩＩ経由では、各大学の情報基盤センターが接点となる。情報基盤センターは極めて重要な基幹部分であるが、各部局の自立性が高く、経営に関する本部と情報基盤センターは離れており、本部から各部局のマネジメントの部分に下ろさなければ浸透しにくい。文部科学省は両方へお声がけしていただくということで、ＮＩＳＣの方針などを出さなければならないと思う。そういったことを徹底できれば、学生対策という部分にも手を打てると思う。

○　「企業の情報セキュリティ向上に資する製品やサービスの提供促進と活動の推進」の部分にボット対策とあるが、ボットに感染して踏み台になるのは個人のＰＣであり、また、その攻撃対象となるのは企業だけではなく重要インフラ、政府機関であり、サイバーテロにも使われる。攻撃される側の対策の研究を行ってもしょうがないので、ボット対策について記述する場所を検討する必要がある。少なくともここではないと考える。

○　企業や行政組織についてもそうであるが、情報セキュリティの内部監査の仕組みがあればかなり違ってくる。内部的には監査を行える人材がいないなど問題で、実態は上手く行えていない。そこで外部監査による情報セキュリティ監査を受けているかと言えば、特定の業種業態分野にはあるが、なかなかできていない。チェックリストを基に内部監査を推進していくことは非常に有効であると考える。特にガバナンスの確立に向けては、チェックリストによる内部監査の推進などが盛り込まれるとよいのではないか。

○　契機的な面での言及も必要である。特に中小企業など、外部監査を受けやすいような体制といった方向性も出せればと思う。

○　基本は外部監査を行うということであるが、まずは内部監査の仕組みができていないので、そこからまず取り組まなければ難しい。

○　内部監査の仕組みに関するガイドライン的なものを出した方がよいということか。考慮させていただきたい。

○　「対策が困難な個人も含めた情報セキュリティ水準向上に向けた取組み」とあるが、この“対策が困難な”という形容は個人に係るものなのか、情報セキュリティに係るものなのか。そもそもこれは、個人分野に掲げられるべきものなのか。

⇒“対策が困難な”というのは個人に係っており、リテラシーがないというような個人、やる気がない個人を含めて、全体的な水準の向上が必要であるという趣旨で記載している。分かりにくいということであれば、表現は見直したい。

○　その中で、迷惑メール対策の強化とあったため、そのような情報セキュリティ対策が困難であると理解していたが、そうではないとすれば、迷惑メール対策の強化がそのような個人を含めた水準の向上につながるのか。

⇒そういった個人に向けては、技術的な対応、自動的にアップデートするような仕組み、ＩＳＰがウィルスをチェックして排除する仕組みなどを含めて考えていかなければならないという趣旨である。その中で、迷惑メール対策もメーラーやＩＳＰが行うなども必要ではないかということである。表現は考えたい。

○　具体的取組みの方向性として挙げられている一般ユーザの質問、アドバイス、訪問対応を行えるサポータ、地域団体ネットワークの実現とあるが、これは「対策が困難な個人も含めた情報セキュリティ水準向上に向けた取組み」に含まれるべきものではないか。こういったものが、対策が困難な個人の受け皿となるのではないか。

○　対策が困難な個人とはベースラインであり、ここから先はないという状態ではないか。例えば、かなり強力に、サービスプロバイダの約款などで、迷惑メールを１日に何回以上送れば、その個人に対してそのポートは閉じるなどといったイメージと理解している。先生が出かけて行き、教えれば何とかなるというレベルではなく、ベースラインを守るため

の強力なものと理解している。普及・啓発が効かない領域に対して、網を掛けるというものではないか。

○　それは対策をとろうとしない人のことだろうが、やりたくても出来ない、やる能力がない人もいるのではないか。

⇒対策が困難な個人への取組みを通して、気付きが起き、勉強しなければらないという意識を持ってもらえれば、それは「個人の底上げに向けたより効果的な普及啓発活動の実現」の領域に含まれてくると考える。

○　永遠のビギナーという考えがあるが、そういった方も「個人の底上げに向けたより効果的な普及啓発活動の実現」へ含めて取り組まれるのか。

⇒永遠のビギナーについては、全く無頓着な個人と新しくユーザになる個人に分類されるのではないか。前者は「対策が困難な個人も含めた情報セキュリティ水準向上に向けた取組み」の中で、後者はその取組みと「個人の底上げに向けたより効果的な普及啓発活動の実現」の領域のどちらかに分類され含まれるのではないかと考える。

○　今、ご説明いただいたように表現を分かりやすし、記述させていただきたい。更にご意見がある方は、事務局へメール等でお寄せいただきたい。

⑵ 地方公共団体について

○　政府機関や企業の取り組みのレベル感は、ディスクロージャの段階までは進めるのではないかといった印象である。地方公共団体においても情報セキュリティ報告書などのディスクロージャをどうするかについての検討あるいは研究を行うということを盛り込んでもよいのではないか。記述が見当たらなかったので、その辺りもご検討頂きたい。

○　小規模な地方公共団体については、ＬＡＳＤＥＣや中央官庁の支援はかなり重要だと思うが、一定規模の地方であれば、地方の民間企業を活用するということも行っていただきたい。東京だけで情報セキュリティのビジネスや人材が育成されるということだけではなく、地方でもビジネス、人材の育成に繋がっていくと思われるので、地方の民間活用ということも盛り込んでいただきたい。

○　それは発注・受注といったものではなく、その前の勉強会といった段階から入っていただくということでよろしいか。

○　はい

○　それぞれの地方がセキュリティに結びつく施策を考えていくということもある。もう一つは、何か外圧があって動くということがある。外圧は住民意識が大きく、例えば、格付けのようなものがあれば、それはかなりの外圧になる。行政の情報セキュリティ報告書のようなものが、サンプル的に示されて、そういったものをどこかが出し始めれば、横並びで出されるはずである。内容が表にでるので、格付けといったものが徐々に広がっていくことが効果的ではないかと思う。

○　住民、クライアント・利用者を意識した形で行った方が動くということだろうと思う。それは重要な視点であろうと思う。

○　後に、他のご意見が出てきた場合には、事務局へメール等でご連絡いただきたい。

⑶ 対策支援主体、情報提供主体、推進体制、論点資料説明

○　メディアについてであるが、「表現の自由等の諸権利との関係を十分に踏まえつつ、何らかの自主的な取り組みを期待できないか」というのは、要するに「何も注文を言いません」ということになっていないか。「事実を書くな、曲げて書け」といったことは言わないが、表現の自由とは別の次元で、メディアには、基礎的な一定の勉強をし、ＩＴ分野を扱うに足る知見を得てから取材をしていただきたい。システム障害の例で言えば、結果だけ見て、原因が不可抗力に近いようなものから、組織的に弛んでいることが原因のものまでを、ほぼ同列に扱ったような記事は書かないで欲しい、できればその上で今後こうすればよいといった建設的な提言まで含めた記事を期待したい等、そういった要求くらいは言う自由がこちら側にもあるのではないか。諸権利との関係や様々な配慮があるのかもしれないが、メディアの重要な役割として、そういったことを期待している。メディアとしても、当然自覚しているはずであり、教育や啓発にも相当大きな力を持っていることについて整理し、何がしかのメッセージを書き込んだ方がよいと思う。

⇒ご指摘は重要である。できるだけ今おっしゃっていただいたことは踏まえた書きぶりに留意したいと思う。

○　評価等の方法の検討において、第２次基本計画の対象機関後の「姿」を描き出し、評価指標なども活用し、「姿」に対して現実がどの程度到達したのかを測るという表現は、心地

よく聞こえる部分もあるが、正確ではなく、わかりにくいのではないか。「姿」は、具体的に、しっかりした到達目標だと思う。この到達目標をどのように作っていくかということが、あまり具体的に書けないため「姿」という言葉を使っているのか。

⇒１次計画には「姿」的なものは書いていない。次期計画は２回目でもあり、ある程度計画が終わった後の結果、あるべき姿がこのようになるという形を想定し、それに対して実際にどこまで進んだのかを検証するためのものである。そのようなものがなければ、全体的な達成の評価ができないのではないかという趣旨で書いている。まだ、具体的にどのようにするかを考えている途中であり、委員にご意見をいただきたいということで、このような表現になっている。

○　いろいろな委員の方々から評価についてのご意見はあるだろうが、評価というのは難しい。一般的に、例えば、セキュリティマネジメントの評価について言えば、達成するレベルを決め、何かの活動を実施し、レコードという測定結果が付いてこなければ、最終的にどこまでできたのかについては言えない。メジャーできるものがなければ、評価は曖昧になってしまう。「体制ができました」ということに対しては評価できない。例えば、委員会が２５名で構成され、出席者が常に２３、４名であればＯＫとすることは正しくない。メジャーできるものとできないものがあるが、その辺を含め、どういった評価を最終的に、例えば２次計画が終わった後にやるのかについては、もう少し議論する必要がある。

⇒おっしゃるとおりである。今回の説明では、現在の状況を示し、現時点で事務局として想定する「姿」はこのようなイメージであるということを示している。それほど具体的なものではないのかもしれないが、これらについてどのようになったかを、終わった後に考えるというイメージである。

○　今のご指摘は重要である。セキュリティとは異なるが、現在、電子政府評価委員会の座長を拝命している。全ての重要項目の指標は、アウトカム、アウトプット、インプット、スループットという管理体制、業務遂行状況を示す指標、全ての段階においてできるだけ取得できる指標にし、各府省庁からデータを挙げて貰い、分析する体制にしようと取り組んでいる。各省庁は、対応したデータを取る体制が十分に取れていない。今後、徐々に整うだろうと思うが、そのような体制が必要になるだろう。その際の指標の取り方については、ここでは「姿」とあるが、ＥＡでいうＴＯ ＢＥ ＭＯＤＥＬ（トゥービーモデル）であり、あるべきものはどういったものかというものである。そこから指標を出し、現状からデータを採り、移行プランを採るという形がよいのではないか。実際に、大学の法人評価の委員をやっており、第三者評価機関は全て作文をしない、エビデンスに基づいて作成する、ファカルティ・デベロップメントはどう行ったか、何月何日に開き、何を議論し、そ

の結果、教育効果がどのぐらい高まったのか、アンケートは採ったか、ということを聞かれる。そのレベルまでやらなくてはならないということだろう。大学で取り組んでいるので政府にできないことはないだろう。それをある程度示す必要が、ＮＩＳＣにあるのではないか。その書きぶりをどうするかはもちろんあるが、その辺りは今のご指摘を踏まえ、事務局で書きぶりを考えてもよいのではないか。

○　推進体制で、「事故があった場合の調査や評価は自主的に行い、それによって信頼性を高めるべき」とあるが、これだけで問題解決が進むのかという疑問を持つ。重要インフラ等にからむ重大な問題に関しては、○○事故調査委員会ではないが、そういった徹底したものを作る必要があるのではないか。そこで基本的な問題点や原因等が徹底的に解明され、技術的な知見を蓄積する構造に反映され、失敗が成功に生きていくといった連鎖が行われるという仕掛けが必要ではないか。報道されるトラブルは、何が原因か知らないまま終わってしまう。発表されているため、調べればわかるが、きちんと発表され、今後の進展に反映されるリンクを構築すべきではないか。

⇒原因究明は大変重要であり、できる限り情報を共有し、同じ過ちを繰り返さないということが目標であり、そういった点から重要インフラではセプターという仕組みを作っている。さらに、セプターカウンシルという横断的な仕組みを作っている。まず、そこを作ることが重要であり、現段階では重要インフラに限らず政府もそうだが、自分が被害者であっても不祥事のような気がして、情報を出したがらないため、信頼関係を作り、情報を出す仕組みを作ることが重要である。第三者的に強制力を持って調査することは、現時点ではできないのではないかというのが我々の考えである。航空事故調査委員会のようなものは、人身事故が起きる強制力を働かせる仕組みであるが、情報セキュリティに関してはそこまでの事故は一般的でないため、まずは不祥事と思わず情報共有をしっかり行う必要があり、そのためには信頼関係を築く必要があるのではないかと考えており、努力していきたい。

○　セプターの中にも、情報を積極的に公開して生かしていく仕組みを、もう少し明示的に取り込むべきである。もちろん趣旨は分かるが、本当の原因や問題は出しにくい、出さないという雰囲気が未だにある。それが出ない限り、次のアクションが取れない。情報は調べればいくらでも出てくるが、調べなければ出てこないという状況はもう少し改善されるべきである。

⇒情報が出せる体制が必要。おそらく情報を出させるには何かインセンティブを用意しなくてはならないのではないか。その辺りの仕組み作りも考えなければいけないのではないか。

○　メディアの情報発信に関連する検討は、もう少し深く書いていただきたい。メディアは新聞に限るのかということも議論になると思われ、メディアという書き方でよいのも含めて検討していただきたい。新聞の他にも情報発信できるところもあり、特に一般の方々への影響度から言えば、放送局がどう使えるのかは考えていただきたい。新聞と放送は、ほとんど資本が同じであり、また、放送に関しては通信との融合の中で、ＩＴの提供事業者として対策を行わなければならない側に一部入ってくることになる。そういった主体としての意味を持つグループとしての認識を持ち、情報発信に関して積極的に取り組むことを期待したい。

⇒このメディアには新聞、放送両方含めており、今おっしゃっていただいた点は踏まえて書きたい。若い人へのメディアの影響力を考えると、今はｗｅｂの影響力が相当大きく、学生達に聞いても、テレビや新聞はあまり見ていない。全てｗｅｂベースで情報が入ってきており、マスメディアに近いｗｅｂ、ブログ、ＳＮＳがある。相互作用的な情報伝達仕方について何か書いてもよいのではないか。影響力という点では、徐々にそちらへシフトしているのではないか。

○　情報提供主体について、個人情報の所有者としての報提供主体という印象が強い気がする。「情報提供主体が情報を保護されると合理的に期待できる範囲に関し」というのは、企業や政府のような組織としての、情報提供主体としての検討も必要であり、そのことについても書かれるということでよいか。また、推進体制について、「技術面での知見を蓄積・活用できる構造に関しては具体的な検討分野はどのようなものがあるのか」と書かれているが、基本的には情報システムのセキュリティに限定した技術検討だと思っている。米国で進んでいるリポジトリーといった概念を借りるなど、それほど限定しなくても良いのではないか。逆に、各セクターや各企業が、それぞれの中で提案できるようなものが、こういったところを経て出てくる。もちろん、審査の構造や基準についても持つ必要がある。先ほど、ＥＡのＴＯ ＢＥ ＭＯＤＥＬの話があったが、ＫＧＩやＫＰＩは区別すべきである。ゴールインジケータとしてのＫＧＩはもちろんそうだが、途中プロセスとしてのＫＰＩを意識した方が、ＫＧＩへ効率的に行き着くことになる。そこを区別したほうが良い。

⇒情報提供主体は企業も含めるので、アウトソーシングの場合や通常の取引の場合も入っている。

⇒技術面の知見を蓄積・活用できる構造については、具体的なイメージの案があれば事務局側に意見を言っていただきたい。

○　対策支援主体について、セキュリティ対策は技術的な部分と人的な部分の両方をやらなくてはならない。特に教育機関・研究機関からは、技術上の理論的なサポートや、システム技術的な対策についての発信等が沢山出てきて欲しい。非技術的な部分については、それぞれがそれぞれの立場で、難しいものを作り、それらを見て対策を行うということがあるかと思う。以前、技術の部分が重要だということを述べさせていただいたが、問題が起こる根本には技術があり、非技術的なものの理解が進まなければ、技術的な対応は難しい。そういったことの積極的な発信を行うことは重要である。研究はされているようだが、自発的、理想的な発信をしていただけると良い。

⇒この問題にどうアプローチできるかについては、少し詰めて考える必要がある。できれば、このようなものが良いのではないかといった具体例があれば、ということであろう。その辺りも事務局で考えさせていただきたい。

○　評価については、評価をする以上、推進や実効性を期待するなど、様々な部分がある。その意味でも、行政評価局の評価との関係はどうなっているか。政策評価の委員もしているが、「基本計画の計画期間は３年でよいか」については、この手のものは３年以上でなければ、政策のチェック評価対象にならないため、途中チェックという意味でも有効かと思う。国の行政評価局の評価に掛かる場合、掛けるかを決める段階と評価の段階で、各省庁のヒアリングを行い、どこまで進んでいるかという指標に照らしてチェックができる。ここで、独自に行った場合に、各省に対する実効性を確保できるのか。

⇒行政評価局の評価と同じ評価という言葉を使っているために紛らわしいが、基本的に政策評価と、ここでの評価は異なるものである。ここでの評価とは、情報セキュリティ政策の企画立案・総合調整のために必要な範囲で情報の収集及び分析、その他の調査を行うことであり、第１次計画でのＰＤＣＡということを言っている。計画に基づいて作られる施策は、年度計画セキュア・ジャパンという形で取りまとめられている。施策をいつまでに実施するかということもあるが、ここでは実施した施策の効果を見ることを「評価」と呼んでいる。その見方は、施策が実施できたか否かというアウトプットに加え、社会情勢を踏まえた全体的な総合評価を行い、それに基づき次の年次計画を作るというセキュリティ政策の全体的なＰＤＣＡによる不断の見直しの構造を採っている。総務省で行う政策評価は、政策の統一性、総合性や客観性担保、行政運営・制度改善を図るものである。ＮＩＳＣでの評価の枠組みは政策会議にかけて決めており、作業方針も政策会議に毎年説明している。

その枠組みに沿って、従来どおり行えばよいのではないかということを書いている。

⑷ 今後の国際協調の方向性について

○　インターネットの世界では、国内国外を問わず通信する時代に入っており、国際的な連携が非常に重要である。技術だけで安全性を確保するとなると、課題が多い。法律によって取り締まる部分と技術によって安全を確保する部分を分けて考える必要があり、国際的な整合性の確保を考える必要があるのではないか。例えばフィッシング対策のように、国内では取り締まりの方法があるが、外国で行われた場合に、各国が協調して取り締まることができないか。ボットについては、平常時から踏み台にされないために、ソフトウエアを排除するような仕組みを求めるということが必要であり、技術だけで確保するには限界があるのではないか。いろいろ調べてみると、ネットワークそのものが壊れたというケースよりも、特定の重要サイトが攻撃を受けて機能不全に陥る事例が圧倒的に多い。ネットワーク自体が落ちるということはない。政府及び重要機関のサイトがサイバーテロ時でも容易に切り替えられるようなバックアップのようなものを作る、或いは、外国からの攻撃に対して、ボットを自動的に検出して排除するようなネットワークにつなぐといった観点での対策が必要ではないか。

⇒ネットワークがボットを摘出していくようなメカニズムは研究開発と一緒に行わなければならない。バックアップの必要はあると、政府内では検討している。

⇒政府対策の部分でバックアップの必要性は明記している。研究開発でもボット対策について記述している。国を超えた法律・制度問題については、サイバー犯罪条約の批准に向けた取組み、犯罪捜査の共助や犯人引き渡し条約等、いろいろな取組みが国際的にはなされている。

○　法的対応については、１０年前にe-commerceを立ち上げるということで、法対応の必要性があるということであった。現実問題として、各国が法の平準化に向かって歩み出さない。特にEUと米国の意見が一致しない。一つの例は、個人情報保護法で包括的法制にするか、セグメント方式にするかで議論し、結局、米国は未だにセーフハーバー方式、或いはセグメント方式で対応している。この穴を付く攻撃もありうると思う。捜査管轄権の問題もあり、中国と日本が捜査協力をした際の実効性、対応のスピード等で困難を抱えているというのは否めない状況であり、努力すべき問題ではあるがそう簡単には行かないと思う。

○　国家主権を超えた枠組みの中で法規制を考えることは難しい。可能であるとすれば、条約という形で規制をかけるしかない。条約を作るときに何を守る条約を作るか。情報セキュリティを法益とした条約を作ることを、日本が先駆けてやるべきではないか。他国にとっても、我が国にとっても貢献度を高めることになるのではないか。ただ、情報セキュリティという法益自体、世界共通の法益として理解されているかは各国に温度差がある。サ

イバー犯罪条約の規定を整備することをEUで謳っており、少なくともEUでは受け入れられるのではないか。アメリカとは個別の法律で対応することになっているが、情報セキュリティ概念を否定するものではない。情報先進国における条約の働きかけは実現するのではないかと思っている。一番難しいのはアジア諸国との関係であり、どのように協力を求めていくのかは課題であり、法的な枠組みで何かしらの対応は必要だと思う。

○　政策レイヤーにＩＴＵが入っていることがわからない。オペレーションレイヤーは重要インフラも係わっていくということか。標準に関わるレイヤーがあるのか。

⇒従来、国の役割は政策レイヤーが中心であったが、事業継続性やインシデントの対応などについて、国の機関同士の意見交換、それを純化して政策に高めるようなプロセスもあり、国の役割が出てきているということである。標準化については、ある種の基準を作るという意味では政策に近い部分が多いのではないかと思っている。標準の中身もデジュールからデファクトまであり、また実際の日々の活動に近いものまであるのではないかという意味で両方に入りうると思う。ＩＴＵは国だけではなく、民間もメンバーになっており、通信事業者のオペレーションについての議論も行われている。そういう意味では誤解を招く資料かもしれないが、国が関与している部分という意味では政策レイヤーに主として分類されるのではないかと考える。

○　システムがグローバル化している点が気になる。条約の可能性を考えた際に、製品・サービスの品質保証へ話が落ちてくるのか。ITセキュリティ評価制度ベースのコモンクライテリア相互認証ではなく、条約のようなイメージで行くとかなり異なる。ITセキュリティ評価制度を国際間でどのように使うのかを検討研究をする必要があるのではないか。政策・法律レイヤーとともに、技術レイヤーとしての検討が必要ではないか。

⇒標準的なフレームワーク、CCも含めて技術戦略で整理しておきたい。CCやスタンダードの中身について基本計画の中でどこまで書くかについては、細かいところまで書くことに対してはネガティブである。例えば、15408 をどうするか等を書くことは、計画に馴染むのかという懸念がある。確かに活用に対しての取組みをどの様にしていくかという見直しも含まれるが、方向性までは必要ないのではないかと思っている。

○　ITU-Dでは、各国又は世界的にボットを減少させるmitigationをやろうと提言している。どのような施策で行うのか、大きな政策の中へ落とし、そこへ技術や方法が入る。そういった方法論や技術をオペレーションレイヤーに渡さなければ、オペレーションができない。政策的な話を、より具体化する人が必要である。先ほどの話では、政策レイヤーの中に、具体化まで落とす人たちがいて、それをオペレーションレイヤーに渡していくという理解

でよいのか。

○　このドキュメントの考え方は、政策レイヤーの対話とオペレーションレイヤーとの対話、法執行機関との対話、政策とオペレーションでは達成目標をどうするかという対話が発生している。オペレーションへ、どのようにブリッジしていくかは各国が独自に行っている。標準化の枠組についても、レイヤーと書かれているところは対話を示している。国は対話し、ある一定の方向性についてラフなコンセンサスを得たものを、国内の施策或いは政策の構造として展開し、その一部がオペレーションへまわっている。レイヤーは自分の中のサブの構造であり、そのブリッジも自分が責任を持つ形になると思う。ブリッジは自分の政府であり、レイヤーというのは対話の構造と理解してもらうとすっきりするのではないかと思う。

○　国際協調という題名であるが、セキュリティは国際連携、国際関係の方が良いのではないか。国際動向に関する情報収集や具体的な連携体制の構築は専門官が一人で、人でこの対応ができるのか。委員会や組織、そういった体制がなければ、できないのではないか。

⇒専門官のイメージは一人でやるのではなく、複数の人間がいるバックヤードがあり、イメージは通商交渉間のようなものを考えていただきたい。365 日の内、250 日間を統一して国際会議にプレゼンスを持って出て行く。情報セキュリティは閉鎖的なコミュニティであり、一人なり、二人がコンシステントに出て行き、顔と名前、やっていることが一致する構造で行った方が良いのではないか。技術的なコミュニティは人の出入りがあるが、政府間の安全保障等では、人が変わることが非常に大きなリスクでもある。しっかりとしたサポートの下で特定の人間が、行った方が良いのではないか。題名の関係、連携、強調については考えさせていただきたい。

○　バックヤードも整備することは必要ではないか。

⇒旅費がたくさん付いている人をつける。バックヤードの充実というのは当然でありそれが無ければ動けない。

○　重要インフラについてであるが、重要インフラ専門委員会では「ＩＴ障害の発生を限りなくゼロにすることを基本姿勢として継続する」となっている。ＩＴ障害の発生を限りなくゼロにすることは困難であり、この目標設定は不適切ではないかということで、本委員会では「目標を変えよう」というコンセンサスが得られたと認識していた。同じＮＩＳＣが運営する兄弟のような委員会が、財政再建派と上げ潮派に分かれたようなフレーズを書くことは、読者である国民や関係業界から見ると奇異に感じられる。重要インフラだけは

政府の方針から離脱するのかといった、コンフュージョンな感が否めない。ひいては、両計画の意義がよくわからないということで、存在感が低下してしまうのではないか。理念は、当委員会の基本計画を優先していただき、具体的な方針を専門委員会で検討していただくという建て付けが普通ではないのか。ＮＩＳＣないし政策会議においてハーモニーをとるような指揮棒を振るっていただかなければ、同時期に行われている会議で理念が二つにわかれて、変ではないか。政府、地方自治体や企業、個人と同様に議論してきた中から、重要インフラだけカセットのように、他の委員会の結論が入って来るのはおかしいと思う。

⇒元々の政策の構造自身がそうなっており、カセット状に重要インフラの行動計画がはまる形で作っている。重要インフラの行動計画は、基本的に行政サイドと重要インフラ事業者との間でのコンセンサス形成プロセスの中で出てきた施策が入る。どちらかと言えば、重要インフラ専門委員会側の意志決定が優先される。基本計画検討委員会の意見は、参考として聞かせていただくという形で行ってる。事務局は、役割として、できる限りコンシステントな形で理念を作ることに対して努力している。現在、重要インフラ専門委員会の議論では、基本計画検討委員会の話はわかったが、こういうことではないかということを委員長からも言われている。事務局としては、調整を考える努力をしており、ご理解いただきたい。カセッタブルになっているのはおかしいということに関しては、行動計画をカセッタブルに作る、カセットのようにはまるような構造で基本計画を作っているということでご理解いただきたい。

○　結果的におかしなことになるのではないか。

⇒結果的におかしなことにならないように事務局は努力するが、コンセンサス形成のプロセスの結果、多少おかしくても、それで行かざるを得ないというところはあるかもしれない。

⇒事故前提社会の対応力強化との関係で、限りなくゼロにするということは、事前対策を強調することになるのではないかという懸念であると思う。重要インフラ委員会としては、気持ちではゼロにすることを掲げたいというのが、大方の意見である。「ＩＴ障害」の範囲については議論がある。また、評価対象とする重要インフラサービスについて、検証可能な合理的なサービスレベルを設定するとも言っており、無理のないように努力させていただく。

○　アイデアがあるので、後日、改めて提案を含む意見を出させていただきたい。

⇒重要インフラについては１０月１４日の第１３回の会議で焦点をあて皆さんの意見を

伺いたいと思う。

○　まだ、ご意見がある方は、事務局までお寄せ頂きたい。

⑸ 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 －