情報セキュリティ政策会議　基本計画検討委員会
第13回会合議事要旨

１．日　時

平成２０年１０月１４日（火）　13時00分～ 15時40分

２．場　所

合同庁舎７号館１２階　共用第２特別会議室

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）
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
安富　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）

【技術戦略専門委員会委員長】

佐々木　良一　委員長　　東京電機大学未来科学部教授

【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

○　脅威、リスクが多様化してきており、新しい攻撃も様々出てきている。それに先んじて鑑みると、それなりの対策を臨機応変に採らなければならない、技術的だけではなく、人的対策も必要であることは、最近よく言われてきている。ここでフォーカスを置かれているのは、プロジェクトの推進を、これまで“ガチガチ”であったものからダイナミックに、適した形で進めなければならないということか。その他、暗号や認証基盤、予知を行うなどの新しい要素も議論されていると思うが、どの辺りが大きなフォーカスポイントになっているのか。

⇒今回の説明は、技術戦略専門委員会で議論されているもので、第１次提言に示された内容との関連で整理している。その中で、重点を置いているものの一つは、自由度が上がるべきだということである。他の分野もそうだが、特に情報セキュリティは、攻撃やその対策が変化する、人間の考え方が変わるということを考えれば、ダイナミックに対応する必要がある。各ポイントでしっかりとした努力をしていくということが大きな点である。

また、一つにはグランドチャレンジ型のアプローチは行っていくべきではないかということである。個別に進めることと、中長期的な観点から進めることを考えていくべきである。情報セキュリティの問題にグランドチャレンジ型の進め方が向くか、ということは確かにある。ムービング・ターゲットであるということを想定しつつ、大きな対策を採って行くことはできるのではないか、または必要ではないか。具体的な内容についてはワーキンググループを作り、本年度中に方向性を出していただくことも大きな点の一つである。

また、共通的な環境整備を行っていくということも強調したい点である。マルウェアのテストベッド等もこれからは必要になってくる。総務省、経済産業省のボット対応についての調査結果、実測データを大学側の有志と契約を結んだ上で情報提供し、分析結果を情報処理学会ＣＳＳ２００８とリンクしたMWS２００８で発表することを行った。短い期間であったが、学生を中心として、非常に集中して良い研究も出てきており、全体のレベルが上がったという経験もある。そのように実測データに関する情報、テストベッド等を共有し、様々な議論のベースとなるものを作っていくことが一つ重要な点である。

情報セキュリティは守り、対症療法的な面が強いが、攻めのセキュリティもやはりあるだろうと考える。かつてはデジタルシグネチャーを導入することにより、インターネットの世界でできないことが、できるようになった。一つの攻めのセキュリティである。最近はそういったものが見えない状況である。例えば、情報家電が実現していく中で、情報セキュリティに関する基準で評価を定量的に行い、このような安全性があり、このような使い方ができるという共通認識が持てれば、新しいアプリケーションが出てくるのではない

か。そういったことが可能になるために、いろいろな情報交換、議論ができれば、そこを伸ばしていく国の施策があってもよいのではないか。これは、個人としての考え、思うところである。

○　取り巻く環境についての記述で「リスクは依然存在し、減少しているとは必ずしも言えない」とあるが、むしろ増大していると書くべきではないか。表に出てきている被害額は減少しているかもしれないが、検挙数は増えてきており、被害に換算できないものも増えてきていることからも、認識は改めていただいた方がよい。

○　国策として技術開発すべき分野はあるかということで、論点が挙げられている。先ほどの欧州のフレームワークとしてFP7の話があったが、言い方はきついが、技術をやっておられる方は、このような仕掛けを作ることは一般的に下手である。こういったものは、殆どヨーロッパにやられてしまっている。国策として、そのような仕掛け、標準的な進め方の仕掛けが技術と共に提案されなければ、「広く認められた国際標準」などがヨーロッパで作られてしまう。我々が意図した通りにはならないことが非常に多い。是非ご議論していただきたい。携帯電話や組込みソフトウェアについては、日本は国際競争力があると考えている。独自の技術を開発し、国際標準にしてはいけないことはないので、今述べたような観点を取り込んでいただきたい。また、情報セキュリティを担保できる設計開発手法については、確たるものが世界的にないと思うが、ＳＱＬインジェクションやボットについても、防ぐつもりになれば一定の設計はできるはずである。そういったものも含めて、ご検討いただければと思う。

⇒基本的にはご指摘のとおりである。「リスクは依然存在し、減少しているとは必ずしも言えない」との表現は、事務局が「2007年度の情報セキュリティ政策の評価等」から記述を引用したものとのことで、ご了解いただきたい。リスクの増減については把握が難しく、増えている面もあれば、減っている面もあり、それらをよく見ながら対応していきたい。

国策としての対応は、今述べられた形の対応は確かにあると思われるので、我々の議論の中で考えてまいりたい。

○　成果の活用について、国策などで研究開発を行った場合の成果の帰属を明確にすべきではないか。成果が開発者や企業に移転され、商品化されるという形は今でも取られているかもしれないが、不十分ではないか。そのため、開発を公募した際に第一線級の人が投入されないことがあるのではないか。

○　市場原理に任せては失敗するケースがあるのではないか、基礎研究では費用対効果を考

えるべきではないものがあるのではないかといった論点については、確かにその通りであり、だからこそ国策としての技術戦略、開発が必要ではないか。とはいえ、費用対効果を考えなくてもよい聖域を作るのかというと、そうではない。違う指標、仕組みが考え出されるべきである。是非考えていただかなければ、聖域を作っては大変なことになる。

⇒私が答えられる範囲を超えているかもしれないが、国が行った成果が企業等で活用されるということは、昔に比べれば良くなってきているのではないかと感じる。個人的見解として、製品化が上手くいかないことについては、次のステップとして上手くやっていくルートが出世魚的になっているかということに依存しているのではないか。費用対効果については、おっしゃる通りであり、難しい議論ではあるが、国で行う部分、民間の活力をうまく活用する、上から出なくともよく見ればしっかりやっていたという部分が無ければ上手くいかない。それらも検討課題である。

○　製品化に関して、技術が製品になったものを国としていかに育てるかというマクロ的な支援策が必要ではないか。単に技術開発だけではなく、マーケティングに関する支援策も必要ではないか。

○　前提として情報セキュリティはテクノロジーよりは総合サイエンスとして考えていくべきだろうと感じている。

○　これは確認だが、「成果を活用する手順（プロセス）」とあるが、イメージが沸かない。これは、先ほどの製品化の話なのか。

○　質問として、「予兆を早期発見するための研究開発が必要ではないか」とあるが、これはテーマとしての話か、事前防止センターといったようなイメージか、分かれば教えていただきたい。

○　標準化がコスト低減につながるか、ということについては、それ以前に比較ができない。現状、社会としてコスト低減なのか増えているのか全く分からない。標準化して初めて、コスト低減なのか増加なのかの議論ができると思っている。その意味でも以前から標準化ということを述べさせていただいている。後々に付加価値を持って外に出て行く場合に、標準化ということで持っていかなければ意味がないのではないかと思っている。

○　過去の状況、車の製造業などを見れば、日本は付加価値に添加して品質をどう高めるかということで、国際競争力を高めてきた。情報システムについて、このようなことができないかと感じている。情報セキュリティは品質の一部として考えているが、その意味で国

際競争力を高めることは必要であろう。では、国の役割、具体的なことは難しいが、必要性を感じていることは意見として述べさせていただきたい。

⇒成果の活用については、中間成果であっても様々活用できるのではないか、それを初めから考えておくということである。予兆の早期発見については、このような研究開発を行っていくこともあり得るのではないかということである。ご意見の部分には特段無いが、標準化は時間とコスト、マンパワーが掛かる、また、いろいろな標準があっても使われないことも考えつつ、標準化戦略を練っていかなければならない。

○　技術戦略では、「いつ」、「何を」、「どのように」、「誰が・どこで」ということが書き込まれなければならない。「いつ」、「何を」、「どのように」はよいが、どのような研究者・開発者、どのような研究の場を前提として、導入形態や対応形態がコンプリートされるのかが、資料からは把握できないように思う。

⇒これらの論点では、国でやるか、民間でやるか、その他でやるかについて明確に書ききれていない。委員会のレポートでは、触れられている。

○　米国のＮＳＦと文部科学省との間では、共同のプロジェクトを持たれているが、欧州のＦＰ７について、コラボレーション等の具体的なアクションをとられているのか。この資料２は単にテンプレートとして参照されているのか。

⇒ＦＰ７のプログラム・ディレクターから、リクエストのコールが掛かっているのは今年の春からである。ＦＰ７はセキュリティだけではなく、非常に大きな枠組である。２０年後のインターネット、ミッドレンジのフューチャー・インターネットについては、昨年の秋にインターナショナル・パートナーを探すためのコールが掛かっている。セキュリティに関しては、今年の７月にプライバシー・コンシャス・コンピューティングに関してのPDからのリクエストが出ている。それは、ＥＵ内とインターナショナル・パートナーについて、両方のコールが掛かっている。プログラム毎に異なるため、一概には言えないが、日米の安全・安心についての協定のように、大臣と大臣が話をしてファンドのマッチメイキングが起こるということは、ＦＰ７ではないと思われる。ＦＰ７の担当者と会話した中では、今後２、３年は、プログラム毎にコールが掛かり、１件あたり日本円にして 3,000 万程度のものが 10 件～20 件で年間４億程度の構造で流れていく。ＥＵ内の２０地域に流れており、その中でどのようにしていくかということがメインになっている。フューチャー・インターネットについては、世界中にコールが掛かっている。一つ一つのエリアで見なければならず、ＦＰ７の総体としてどうなのかは分からない。（山口補佐官）［48:24］

○　日本のＮＩＣＴ、米国のＦＩＮＤ／ＧＥＮＩ、欧州ＦＰ７の３極でフューチャー・インターネットの研究開発が行われている。ＦＰ７は総額で３５０億円程度、ＦＩＮＤ／ＧＥＮＩが４００億円程度、ＮＩＣＴが１５０億円程度の予算を投入している。この中には、もちろんセキュリティも入っている。現在のインターネット・プロトコル、ＩＰを抜本的に作り直そうというプロジェクトである。ＦＰ７は米国との対抗軸もあり、産学連携で無線波である第５世代携帯に力を入れている。米国はピュアな研究を進めて行き、ＡＲＰＡＮＥＴのように、次のもの作って行きたいとしている。今月末に日本と米国のワークショップがカリフォルニアで行われる。このように３極で、協調と競争中で進められている。セキュリティについては、縦軸ではないが、横軸で全てに入ってくると思われる。先ほどあったように、テーマや目標ターゲットに応じて、チーム編成やプログラム編成があり、一律なものはないと思われる。

○　補足のご意見があれば、事務局ま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

○　時期的に、基本計画に盛り込む具体策を議論する段階に入ってきていると思うが、この資料では「考えられる方向性」としながら、あまり方向性が示されていない。漠然と悩ましいということが書いてあるだけで、具体策を出すという意欲がいまひとつ感じられない。前から述べている政府機関内の２・３年単位の短期ローテーションの問題についても、掘り下げて考えたような思考の過程が見えない。「多面的、総合能力を有する専門家の育成」についても、「現状不足している取組み、問題点はないか」と、この時期に丸投げされるより、「これまでの取り組みではこのような問題点がある」、「今後このように取り組みたい」などを提示していただいたほうが、議論として実りがあるのではないか。また、問題提起として、「情報セキュリティ専門家に対する実際の需要が少ないのではないか」とあるが、これでは、情報セキュリティ基本計画を熱心に作る必要性すら疑わしくなり、自己否定的な感じがする。我が国の情報セキュリティについて、何がしか強化しなければならないのであれば、実際の需要が少ないように見えるのは、何かがネックになりそれが見えてこないだけではないか。この材料では、どう議論してよいか、「困ったな」という印象である。

⇒ＩＴの専門家へのニーズは、産業界、教育の中でも、おそらく一定の認識があるが、情報セキュリティ単体の専門家がどのように扱われるべきかは、まだ疑問がある。ＩＴ専門家の一つのスキルとして具備すればよいという考えもあり、またソフトウェア開発ではセキュリティの専門家がいなければ、開発プロセスのマネジメント自体ができないということもあり、情報セキュリティの専門家がどうあるべきかは疑問点として現実的にある。求める像が分散しており、そういった問題意識の現われでもあると理解していただきたい。

○　情報セキュリティの問題を人材育成という観点で論じる際に、どのような人材像を考えるかについては、２種類に類型化できるのではないかと考える。一つは、守るべき情報資産などを分析し、ポリシーを策定する人材、もう一つは、それを担保する技術的な方策、最新の暗号化技術などテクニカルな面でどうすればよいかを考える技術的人材の２種類である。各省庁に技術的な側面の変化をフォローしていく人間を配備することは、短期の人事ローテーションを４、５年にしたところで難しいのではないか。技術的なものは、どこか集中的なところをリファーし、各省庁に置く専門家はポリシーを策定する、どの情報資産を守るべきか、重要度はどの程度か、どのようなリスクを想定するかを分析する人材に留めなければ、両方を備えることは無理ではないか。そういった議論はこれまでにされているか。

⇒人材育成の専門委員会でも、一部そういった議論はされている。委員長も何度が述べられたが、アウトソースを行うにはインソースを充実させなければならないという問題がある。政府の各組織をみると、業務解析、要求仕様決定などの根っこの部分を丸投げしている状況もある。根っこから投げるということは、業務のどこに穴、リスクがあり、どこを真面目にやらなければならないかということが手元にないということだ。全てではないが、多くはそういった状況にある。どこから補強するかといった組み立てから考えなければならず、おっしゃるように、技術的な専門家だけを入れてもどうしようもないということは事実である。ではポリシーが組める人間を入れればよいかは、もう少し手前のところも見ていかなければならない。インソースはガタガタの状態であり、それをどう考えるかも含めて、政府内の専門家の配置とアウトソースの関係を考えなければならない。

○　ポリシーを策定するところで、外部から人を借りても即効性のある取組みは望めない。内部の業務の専門家が、ある程度中長期的なスパンで情報セキュリティを勉強していく形へ持っていくしかないのではないか。

⇒そこには短期の人事ローテーションの壁がある。ＩＴ部門の人材も絞られ、アウトソーシングを行い、中身は管理業務になっている。インソースは疲弊状態であるというのが、正直なところである。その中で長期的な人材育成をどうするかという問題になってきている。ある程度の業務スパンの中で企業がポートフォリオを組み立て直し、育成を行うというほどには、霞ヶ関に対応能力がない。丸投げ以外の答えを考えなければならない。ここへ来て５年目になるが、辟易するほどできない。普通の組織ができることを、ここでは４年、５年と指摘しても何故できないのか。本質的にできないとは思いたくないが、そのくらいできていない。特効薬はないと思うが、これから３年間で何をするか考えなければならない。ミニマムのインソースをどのように手当てするか、情報資産のマネジメントに対

して何を行うのか。人材育成の委員会を終え、実際に取り組んでみて、非常に困難であり、上手くいかないと感じている。

○　アウトソースに頼めるところはテクニカル、技術的な面では存在するが、業務に関連するポリシー等については外注しづらいということで、問題意識は一致していると思う。ある程度量的なものは有るという前提で、内部の人材を如何に育成するかの問題は扱えるが、量的なものが全く無く、それをどう確保するかというのはリソースの割当、経営的な問題であり、この委員会では議論しづらい話題である。ある程度、人を集めることはでき、どのような人材が必要か、どのようなカリキュラムで育成するかについてはお答えできるが、過去４年間やってきて人が集まらないというのでは、議論が進まない。

⇒資源割当は確かに経営の問題であるが、どのように資源の割当を行うか、一定の合意が得られれば、国の計画であるので増やすことに口は出せる。情報セキュリティ政策会議の下であるこの委員会で考えなければ、他では誰もやってくれない。その意味では、経営問題まで具現して計画を書くこともあり得ると思う。現状は、徹底してリソースが無いというよりも、育成して育つか、コケるかの二つが混在している。小さい省庁は人材が殆どいない。大きな省庁は、教育すればまだ間に合うという状態であり、大きい組織には担当者がまだいる。ＩＴ関連の専門家を如何に内製するかということでも悩んでおり、大きいところは何とかなるが、小さいところではリソースの割当を考えなければならない状況である。政府内でどうするかは、グループ経営をどうするかに近いところがある。

○　ＩＴに関して拘ってしまうと、インソースの育成は難しい。ポリシーを作る人材を内部に抱えることが重要である。そのような人材の像は、業務と守るべき情報資産の価値を知っている人間である。ＩＴをよく知っている人ではなく、業務をよく知っている人に対して情報セキュリティの基本論を教える方がよいのではないか。

○　経営問題に関しては、おっしゃるとおりである。セキュリティポリシーの改定・改修する人間は省庁に数名いればよい。各部局で技術的な対応行う、現場でどうすればよいか考えるセキュリティ担当者とは数のレベルが違う。ポリシーマネジメントを行える人を各省庁で少なくとも一人、二人置きなさいということは、できないこともないと思う。情報セキュリティ担当者の知識・スキル不足を補うことは、数十人単位であり、議論を分けた方がよい。そこが議論の行き違いにもなっている気がする。

○　短期の人事ローテーションは、問題として認識しているが、大きい話でもあり、現状意見は無い。ＩＴ人材育成計画を各省で作成しており、そことの整合性を図ることも盛り込まれた方がよい。また、大きい省庁では部門内でのローテーションもあり得るので、考え

ていただきたい。

○　マネジメントを行う人材、技術的な人材は必要である。一般の会社でも環境は同じであり、困難な要素を持っている。要素は三つあり、一つは、育成には時間がかかるということである。そのため育成すること自体に本気で取り組まない。直ぐに成果が現れないため、育成という行為が評価されず、継続的に行うことが難しくなっている。二つ目は、知の伝達は仕組みや計画が無ければ難しいということである。三つ目はモチベーションの問題である。情報系や情報セキュリティについて知識を上げることに評価が伴わなければ、モチベーションに繋がらない。特に優秀な人間がやるかといえば、やらない、避けてしまう。ただし、技術的な面で、専門家と共通語で話せるレベルになければ、言いなりの状態になってしまい、結果的には丸投げと同じ状態になってしまう。専門家と会話ができる技術レベルは持たなければ、意味がないだろうと思う。うまくできないというのは、三つの困難性の何れをとっても、民間より環境が悪いため、難しいのだろうと思う。民間も大変であることは同じなので、できないのであれば別の仕組みを考えた方がよい。一つのアイデアだが、各省庁毎に人材を育成するのではなく、民間であればユーザー企業等でも持っている情報子会社のようなものが中間にあり、技術の評価を行う、発注について見ていく、別立てにするというのも一つの方法ではないか。望ましい姿ではないが、現実的にできないよりは、少しましではないか。

○　公務員の中で専門家を育てることが難しいという話であるが、人材の流動性をもち、官民一体となって動ける、政府の中でエキスパートになっていけば民間に流出するなどを促進していけばよいのではないか。そのためには、人材をどう評価するかが重要であり、その点で資格というものが必要になってくる。ただし、公的資格というものには賛成いたしかねる。激しい動きが求められる中で、公的資格ではそれに追従できないと思われ、民間の資格を積極的に活用していくべきである。また、情報セキュリティは非常に横断的であり、各分野の人が同じ言葉でしゃべり、すばやく理解するためには、同じ世界を共有しなければならない。その点でも、資格というものがプラスになるのではないか。こういったものを政府機関が率先垂範すれば、遅効的だが、良いセキュリティ施策を発案し、ＩＴシステムやネットワークに実装した人は企業でも活躍できるのではないか。企業を含めた全体として捉えれば、柔軟な考えができるのではないか。

○　縦軸としての専門家はもちろん必要だが、横軸として情報セキュリティの責任者、それを補完する人材をどのように手に入れるかは、ＣＩＯ補佐官という制度を設け、それなりに成果を上げているので、それと同じようなことができないか考えるべきである。ＣＩＯ補佐官のセキュリティ担当を増やす、情報セキュリティ補佐官を増やすなどやり方は幾つかあるが、ある程度の糸口はあり、それを拡大・拡充する方向で、外から人材を入れてい

くことも考えるべきである。

○　資格については公的な資格を作る方が、普及度は高いということもある。必ずしも、民間の資格に拘る必要はない。場合によっては制度を作ることも検討すべきである。

○　先ほど委員が述べられた、守るべき対象と技術的な方策は分けて考えた方がよい。業務的なところで、何がどの程度のセキュリティを要求するかについては、業務の内容が理解できていなければならない。これは個別のセクションではなく、鳥瞰的に、どのように情報が伝達されて、加工されていくかが把握されていなければならない。その人材の要請は、インソースでなければ果たせない。それは必要なことであり、できることだと思う。電子政府の調査で昨日フランスから戻ってきた。ＳＯＡでは、業務の内容が分からなければシステムを構築できない。業務を把握した上でＳＯＡを構築し、浮いた人員が出てくる。それをうまくアロケーションする。ベルギー、デンマーク、フランスだけしか見てきていないが、どの政府もそういったことを言っている。日本政府もその観点を強く打ち出し、そこで浮いた人員を、情報セキュリティを統括できる人材として育成するなどを考えなければならない。それにより電子政府構想と情報セキュリティ構想を両立させることができる。そのような発想が必要ではないか。組合の問題や、違う業務をやらされることへの警戒感等があるかもしれないので、調整をした上で行う必要がある。そういった戦略性を持たなければ、ＩＴは使いこなせない。第１次提言にあるルネッサンスをやるためにも、使いこなせなければならない。その体制を政府で作っていく必要があるのではないか。

（３）犯罪の取締り及び権利利益の保護・救済について

○　サイバー犯罪を減らすためには確実に検挙できる環境が必要である。匿名性がベースあり、利用者などが犯罪行為を行った場合に特定する仕組みがない中で、確実に検挙できるという具体的なものについて、技術的なものも含め、方策をどの程度お考えか。

⇒技術的に分かるケースも多いと思うが、技術レベルが高い人ほど足下を隠すということもあり、それは問題である。また、海外からのものも多く、どの国も悩んでいるが、国際的な体制も必要である。

○　もともと国境のないものであり、海外の犯罪については国際的な協力を徹底的に考えなければ無理である。そこを前提にせず、まずは国内で行われる可能性がある犯罪について、徹底的に検挙する方向が見えてくれば、抑制する上で有効ではないか。

○　町中の映像を公開するようなサービスについて、公開を禁止する国や、地域を限定し、

制限する国もある。そのような問題に対して、日本ではどこか、どのようなトリガーで制限していくのか。そのような仕組みがあるのか。そのようなところが、機敏に動くという機動力がなければ、予防的活動の取組みは難しいのではないか。

⇒おそらくプライバシーの問題と考えられるが、政府部内でプライバシーを守ることについては、今後できる消費者庁、あるいは内閣府国民生活局も個人情報保護法を担当しており、そちらになるのか、担当については政府の中で調べたい。

○　インターネットを利用した犯罪の検挙を念頭に置かれていると思うが、インターネットが普及し、国民生活に不可欠なものになってくると、一部の専門家が技術的に対応する、それぞれの個人が高度な情報セキュリティを理解し対応しなければならないということでは、社会的に成り立たなくなっている。あまり知識がない人でも安心してインターネットを使い、情報のやり取りができる対策を政府として講じる必要があるのではないか。技術的な対策だけに頼らず、法的な整備を行わなければ、犯人を割り出すことはできても、検挙することができないことになる。法的な整備で一番必要なのは、詐欺的行為により情報を騙し取ることに対して厳しく取り締まれるようにすることである。また、ボット等の配布だけでは、犯罪として取り締まれないのではないか。ボットを使い攻撃を仕掛け、実害があれば取り締まれるかもしれないが、配布することへの規制、法的対処が必要ではないか。そのような観点で法整備をしなければならない状況に来ているのではないか。

⇒サイバー犯罪条約批准のための刑法改正が、なるべく早く国会で審議されることが重要だと思っている。

○　官民の相互信頼醸成があまり進んでいないと述べられているが、基本的に今の法制度で行える取締りをしっかりやることが重要である。少し、警察が引けている感じがする。サイバー的な犯罪でも厳しく取り締まるということが大事であり、今の法律に基づいて悪い人間を捕まえて欲しいというのが一番の要望である。それが、信頼感にも繋がるのではないか。何をもって信頼を醸成するか明確ではないので、悪い者は捕まえるという当たり前の警察の機能を果たしていただきたい。

○　町の映像を公開するサービス等に対する予防的なものをここへ盛り込むことは、どうかと思う。予防的なものに警察が出てくる、法律が次々にできるということは行き過ぎのような気がする。

○　警察の方に確認したいが、ウィルスは配布は駄目で、作成は禁止されていないのか。サイバー犯罪条約批准のための刑法改正で、それが出来ればよいのではないか。

⇒悪い人間を捕まえるのは当然であり、昨今であれば、ネット上で犯行予告している者の検挙、注意喚起も含めて行ってきている。様々なサイバー犯罪があるが、行ったものを捕まえる警察本来の業務をしっかり行っていきたい。そのような警察業務を通じて、民間の方から信頼をお寄せいただきたいと考えている。また、サイバー空間上では匿名性が捜査の大きな壁になっている。本人確認等をすべきところでは、しっかり行っていただきたいということで、県警レベルでも通信事業者、重要インフラ事業者、ネットカフェ経営者の方々に、捜査上の問題、問題解決のためにどのようなご協力を頂きたいかを説明し、信頼を確保し捜査できるような環境づくりを進めて行きたいと考えている。

刑法の改正は国会に掛かっているが、現状ではウィルスの作成、配布の行為に罰則はない。今年、ファイル共有ソフトに感染し情報流出するウィルスを作成した者を検挙しているが、その際は、その中に含まれる画像について著作権法違反での検挙であった。使える法律を出来る限り使い、サイバー空間の安全性を確保することも必要であり、取組みを行っているところである。

○　「愉快犯から経済的利益の取得へ犯行の主目的が変化」とあるが、どのような認識からこのようなことが言えるのか。サイバー犯罪で検挙されているものをみれば、経済的利益の取得というほどのこともなく、様々なものがあり、ここまで言い切るには、いささか事実認識が違うのではないか。また、不正アクセス等はＩＤ・パスワードを何らかの方法で入手して使用するなど、極めて単純な方法である。セキュリティ・ホールへの攻撃もゼロに近い状況であり、「犯行の巧妙化」という記述についても認識が違うのではないか。

○　サイバー犯罪の検挙件数が増加したとのことだが、暗数が相当ある。暗数との関係で見なければ、検挙件数だけでサイバー犯罪が増えたとするのは表層的な理解である。

○　日本政府も海外から狙われており、海外だけでサイバー攻撃の脅威が増大しているとは限らないのではないか。

○　犯罪が“確実に”検挙されるということは妄想でしかなく、おかしな表現である。他の犯罪も確実に検挙してもらわなければ困るが、ここで敢えて言うのは変な話だと感じる。

○　被害者の権利・利益を保護救済するための方法論や情報の法的な評価の在り方については、「既存の法制度、国際的な動向、被害の発生状況等を勘案し、」とあるが、これよりも基本的なものを考えなければ問題は解決しない。単に、「検討を深めていく」という抽象的な表現で事足りるのではないか。

○　サイバー犯罪を念頭に置かれているが、サイバー犯罪という言葉は日本の警察白書で使

われ、ＣＥ（Coucil of Europe）が作ったサイバー犯罪条約では情報セキュリティを意識して使われているが、情報セキュリティ基本計画という枠組の中で、サイバー犯罪と表現する、そのつながりがよく分からない。情報セキュリティを保護すべく、様々な犯罪への対応、権利利益を守るという発想で整理されるのが良いのではないか。警察白書等をご覧になれば分かるが、不正アクセス禁止法違反が主なサイバー犯罪であり、情報セキュリティに対する攻撃に対して法的な何らかの手当てをするという発想を一言入れていただければ、基本計画の今後の展望にもつながる。

⇒現状認識は確かに良く分からないところはある。一般的に現象面だけを見れば、愉快犯的にウィルスを配布するだけの者は減ってきており、目的を持っているケースが多い。かつ、それは経済的な利得に繋がることを目的とするケースが増えてきている。ＩＤ・パスワードの盗用による、ネットオークション詐欺行為が増えてきている。特に内外の為替物価水準の違いから大きな利益になることもあり、海外から狙われるケースも多く、そういったことで記述している。組織化は、ボットネット等で、ウィルスを作る者、それを使う者で分かれてきているということもあり、記述している。定量的に証明することは、なかなか難しいところである。

サイバー犯罪と情報セキュリティの関係については、関係省庁とも相談し、ご指摘を踏まえて考えさせていただきたい。

海外の政府機関を狙ったサイバー攻撃等についての記述は、よく言われるのはエストニアや昨今のグルジアの事例であるが、把握できていない部分も多いので、表現の仕方は検討し、気をつけて記述したい。

○　愉快犯や組織犯罪化についての背景は分かった。ウィルスやボットを想定しているのであれば、現行法では犯罪ではない。そこをイメージして“愉快犯”等としては、処罰されないものを犯罪とすることが前提になるため、まずいのではないか。現行法での構成要件などから、犯罪として類型されるものを前提とし、現状認識として書かれた方がよい。世の中で、これはけしからんというものがあったとしても、罰則規定がないものをサイバー犯罪として表現することは誤解を招く。

⇒おっしゃるとおりであり、表現は気をつけて記述したい。

⇒動機の観点で補足させていただきたい。不正アクセス禁止法違反で検挙された者について動機の聴取をしているが、平成１９年中に検挙した者について、不正に金を得るために攻撃したといったものが１，１８６件であり、検挙した中では最も多い動機になっている。平成１８年当時では、４１９件であり、最も多い動機となっていた。不正アクセス禁止法違反で検挙して分かったものだけになってしまうが、数字上は金を得るために不正ア

クセスを行ったという動機が非常に多い。また、割合としても平成１８年から１９年にかけて、この動機が大きくなってきている。これらは、公表させていただいている。

○　大学に対するネット上の爆破予告も増えてきており、不審物を見かけた場合は本部に通報せよといった通知が頻繁に出るようになった。今年辺りから増えてきている。このようなことを含めネット上での嫌なことは増えてきている。

○　ニュース等をみていると、既存の法律で罰せられることはかなり多いはずである。そのことを世の中が知らないのではないか。法律の中身をどうするか、強化することについては考えていないが、既存の法律でどう解釈できるかを知らしめる必要がある。経済産業省の活動で、「電子商取引及び情報財取引等に関する準則」を出されており、解釈を示している。刑事関係も、準則だけがやり方ではないが、知らしめる、普及させる様なことが必要である。

○　匿名性については、インターネット上では完璧な匿名性があるという誤解が世の中にあると思う。ログの保存義務がないという若干の問題はあるが、開示請求をして開示していただけることもある。ある程度のトレーシング性があることを知らしめるという動きも必要である。法律を作る必要があるかという議論と共に、既存の法律等の解釈も知らしめるという方向性が欲しい。

○　運用の段階では、今の観点は重要になってくる。現行法で対応できる点は多々ある。

○　緊急対応の業務で、ログや記録を警察に提出することがあるが、受理されないケースが非常に多い。ログのフォーマット等、これを出せばよいというものが無い。その時々で、顧客が持っている記録でＩＰアドレス等を提示するが、受理されないケースがある。社内の場合では、この人がということで、名前まで持って行かなければならない。受理する・しないの基準が全く分からない。企業としては、提出した後に捕まえる云々について、深く完璧を求めてはおらず、きちんと記録をとり、提出したものが受理されることである程度の義務を果たしたことになる。また、サイバー犯罪は時間が経つと被害が増えていくので、一刻も早く見つける積極的な検知は義務である。通信記録、サーバーのログ、データベースのログ、入退室記録など、こういうものがあれば良いといった目安があれば、提出する方も出しやすい、受け取る側も捜査が進み、検挙率が上がるなど、お互いに良いのではないか。官民の相互信頼醸成の部分に盛り込んでいただきたい。

○　重要な点であり、事務局でまとめ、反映できるものは反映させていただきたい。まだ、ご意見ある場合は、事務局へメール等でご意見をお寄せいただきたい。

（4）重要インフラの情報セキュリティ対策に係る行動計画の検討状況について

○　前回の委員会で述べ、今回意見書としても提出させていただいたが、自然な発想として、ひとつの“家”（政府の委員会）でスローガンを出す場合に、兄と弟（基本計画と行動計画）が違うことを言っているように見えるのは、上手くない。行動計画が最終的にどのような表現になるかは、重要インフラ専門委員会にお任せするにせよ、基本計画がどのような表現になるかは、文章が提示された段階（今後の委員会）で意見を出させていただくことになると思う。基本計画の重要インフラに関する記述は、“カセッタブル”ということであったが、それは基本計画の重要インフラの部分に重要インフラ専門委員会が作る目標がそのまま貼り付けられる、ことにはならない方が適当であろう。そうした理解で良いのか、基本計画の構成について確認しておきたい。

⇒現在、重要インフラ専門委員会では行動計画を策定している。行動計画は、独立したものとして政策会議決定を受けるという構造になっている。第１次基本計画のやり方は、全体の流れを検討する第１分科会と重要インフラ部分を検討する第２分科会で構成されていた。政府が事業へ「あれをやれ、これをやれ」ということは業法によって行われるが、現在の重要インフラ専門委員会の行動計画は、ある程度のラフコンセンサス、業法の外側で、ボランタリーに動けるところをどこまで頑張るかということで官民で合意していくという構造になっている。そのエグゼクティブサマリーという形で基本計画の中に入ってくると考えている。意見付与はできるが、それらをどのように踏まえるかは、重要インフラ専門委員会での合意形成のプロセスを優先する必要がある。事務局はその範囲で、できる限り equivalent（イクイバレント）になるよう努力するが、最終的に乖離がある場合はコンセンサスがある方を優先せざるを得ない。

○　「ＩＴ障害をゼロ」といった目標も含めた重要インフラ専門委員会側の表現を、できる限り本委員会の基本計画と齟齬が生じないように調整する方向だと理解した。基本計画の重要インフラ部分に入ってくるエグゼクティブサマリーの中に、基本理念的なものが、総論部分と重複して、もう一度（しかも違うニュアンスで）書かれるようなことにはしない方がよい。

⇒その辺りはまだ議論していないところである。まだ、決められていない。第１次基本計画での参照のレベルは、達成したいことと、そのために具体的に何を行うかというが概要として記載されている。それ以上のことは書かれておらず、エグゼクティブサマリーとして記述している。

○　事務局には常識的な文章編集がなされることを期待したい。

○　検討中の行動計画では、「ＩＴ障害の発生を限りなくゼロにする」ということが、挙げられているが、この“ＩＴ障害”は、情報セキュリティ対策の文脈で、情報セキュリティ事故に関わるＩＴ障害と理解してよいか。情報セキュリティに限らず、ＩＴ障害は全て含めるという考えか。ＩＴの専門家の間では、信頼性の問題、性能の問題により、十分なリソースが得られずＩＴサービスの継続が困難になるということもある。それは、セキュリティという観点で論じられるものではなく、信頼性の問題として論じられ、セキュリティという概念とは少し異なる。ここでは、情報セキュリティ事故の文脈で論じながら、情報セキュリティ以外のＩＴ事故もゼロにすることを主張されているのか。

⇒ＩＴ障害の整理としては、サービスに影響が出る状態というものを想定している。様々な議論があり、ここについては調整を行っているところである。ＩＴ障害は、ＩＴの機能不全等によって重要インフラが主要なサービスレベルを維持できない状態に陥る障害、ということを前提にしている。情報セキュリティという観点でどのように考えるかについては、機密性の他、可用性もあるため、ＩＴシステムがきちんと動くように確保されていることが情報セキュリティであるという考え方で記載している。ここでは、止まらない、使えるということで情報システムが確保されている状態を情報セキュリティと考えている。

○　そのように情報セキュリティとして広い意味で、止まらない、限りなくゼロにするということを求めるとなると、非常に重くなってしまう。そのように重い意味であることを宣言しなければ、安易に紙の上に書けないのではないか。情報セキュリティの意味をもう少し狭めるような修飾をしていただくことも手かと思ったが、何しろ止まらないということをここでは言っているのか。

⇒元もとの主旨では、機密性、可用性、完全性のどこが失われるかは別にして、それらが原因となってＩＴが上手く動かない、サービスに影響が出る、所用のサービスレベルを下回ってしまうという状況にならないことをしようということである。“象徴的な目標”と表現している。“ＩＴ障害”という言葉自体の受け止め方の差があるということもあり、書き方については現在調整をしているところである。現実的にはサービスに影響がでないようにしたいということである。検証対象については、サービスをある程度選び、具体的な検証レベルを決め、達しないものがあれば検証を行おうとしている。目指す方向で考えるところと検証対象として見て行こうとしているところが、大きく異ならない書き方をしたいと考えている。非現実的な目標を立てて、達成できなければ困るということは言うつもりはない。方向性としてはこうだが、現実的にはこういったところを検証していきましょうということである。ＩＴ障害の発生をゼロにするということだけを強調しては、それは行動計画の一部になってしまう。

○　我々もよく経験することだが、専門的に一番難しい問題となるのはトラフィック特性をどのように見積もるかということである。端末数が限定されている場合は見積もりやすいが、インターネットにおいて、予想を超えてアクセスがあった場合に、予期せぬ理由で機能不全に陥る場合がある。設計値どおりに製造されているが、設計値の予測を超えて予期せぬ機能不全が発生してしまうことはよく経験する。予期せぬものについてもＩＴ障害として扱われることは非常に危険である。予測可能な範囲できちんと行われているかといった、誤解がない表現をしていただいた方がよい。

⇒その点については、重要インフラ専門委員会でも議論されている。認知されるものがリスクであり、それらについてはしっかり対応を行う、不確実性の部分をどのように認知し、処理するかについて、重要インフラの役割を考えた場合、やらないということは言えないだろうという議論がある。不確実性がある部分でＩＴ障害を引き起こしたとして、行動計画がそれをカバーする領域から外すことはないだろうということについては、一定のコンセンサスができている。現状の行動計画の検討では、予測し得るものだけをカバーするとはしていない。また、それをもって駄目だとすることはよろしくないという議論になっている。不確実性により発生したものを合理的にうまく料理できないか、つまり、どれだけ被害を押さえ込めるか、問題をどのように追いかけるかを、官と民で共に行うことについて、行動計画がどうあるべきか検討を行っている。専門委員会で議論した中では、予測できるもの、明確にリスクとして認知できるものだけを計画の中で取り扱い、狭めることはない、ということは大まかなコンセンサスはできている。要するに設計値を超える状況があり、仮に障害が発生し、それを以って責めるというものではではなく、その先にしっかり対応ができたかということを検証すべきということである。重要インフラは国民生活への影響が非常に大きく、不確実性に基づいて発生したものについては、一定の責任を官も民も持たなければならい。一部の領域では、業法を設定し免許事業者だけが独占的にやるという構造になっている。元もとの、この構造考えれば、不確実性を以って免責されるものではないということが、専門委員会で得られているコンセンサスであると認識している。

○　ありとあらゆる局面において、責任を問う際には、予測可能性があるか否かということが根本概念としてある。予測できないものに対して責任を取れということは難しい問題がある。医療行為、あるいは現場の設計においても、どのような予測を行い、予測したものに対応することは求められるが、予測不可能なものに対して責任を取れというのは、なかなか難しい。

⇒そのような責任論については、現在の専門委員会の議論、また第１次の行動計画にもあるが、責任を問えるのは法的に成立しているものしかない。それは業法の枠組である。

何故、行動計画が不確実性のところまで言及できるかについては、よりよいインフラをどのように作っていくのか、そのために官と民でどのような役割を果たしていくのかということがメインであり、責任の所在はどこなのかという構造にはなっていないからである。行動計画で定める行為そのものは、法律に基づくものではなく、その先の広い領域において、運用的に上手く行く為には、どういうことを官が支援し、民はボランタリーに、自主的な中で行っていくかという構造でこの計画はできている。委員がおっしゃるように、この行動計画の中で、責任を問うという行為を行うことはおかしい。責任を問う計画ではなく、それは業法の枠組の中で、それに関わる法律の中で行われる。ＩＴが関わる領域横断的な中で、どのようにＩＴのリスクを低減してくのかを官と民が協働で行うこのフレームワークをどのようにしていくのかが第１次の行動計画である。それを踏襲して検討していくということで、ご理解いただきたい。

○　予測可能性がないものについて、それをよりよくすると言っても、具体的にどうすればよいかという手段は何も与えられないのではないか。

○　警察庁でも「交通事故死ゼロ」ということを目標に立てており、そんなことを言えば、何回、警察庁長官が損害賠償を請求されるのかという話になる。中方防災会議でも「災害犠牲者ゼロ」を目標に掲げており、それでは防災担当大臣は何回クビになればよいのかという話になる。そういうことではなく、これはあくまでも理念的な目標であり、基本的には良いと思っている。理念的な目標について、予測可能性や賠償責任において何かおこるのではということまで事業者が考えるのは、なにかおかしな話になるのではないか。原子力については予測可能性に基づいて何もやっていないという話があったが、原子力では予測可能な範囲で、リスクの可能性を10^{-6}という目標まで立ててやっている。ここに書いてある目標は、「交通事故死ゼロ」や「災害犠牲者ゼロ」とあまり変わらないと解釈すれば、よいのではないか。

○　この計画の議論を伺っていて、国民に語りかけるメッセージがないと感じる。事業者、ＩＴベンダー、役人に関係する中身だけではないか。「事故前提社会」も、事故が起こる、リスクは在るので「がまんしてね」と言っているだけである。行動計画の中で、事故が起きた場合に、被害者をどうするかという観点がまるで無い。「広報公聴活動」と示されているが、ここでは何をやるのか。意見として述べたいのは、「ＩＴ障害ゼロ」といった目標に対して専門家レベルの厳密性をおくのではなく、社会通念上問題ないのではないか、また、唯一国民分かりやすいメッセージであるということで評価したい。

⇒広報公聴活動については、障害が発生した場合にその影響を極力小さくするためには、国民が状況を踏まえて冷静に対応することが重要であるということで、国民に対して説明

責任を果たし、必要な行動がとれるよう必要な情報を得られるようにして行こうというものである。行動計画についても関心を持つ主体を増やし、広く支援が受けられるようにしようというものである。具体的には広報活動、Ｗｅｂを活用する、セミナーの機会を捕らえるなどを考えている。また、リスクコミュニケーションの充実ということで、関係者間のリスクに関する誤解や理解不足を解消するために、関係者主体間の直接的なコミュニケーションの機会を増やす、機密情報を開示することは言えないが、情報共有をお願いしている。

⇒金融、通信等の１０分野があり、一つひとつについては、所管官庁、業法があり、トラブルが起こった場合に、どう考えていくかという動きがある。そこでは、各省庁がしっかり行っているので、頑張っていただこうということである。しかし、問題になるのは、地震等の問題で、全て一気に倒れると影響が大きいということである。ＩＴの特徴として、システム化が進めば他の領域が関わってくることは事実である。未だトラブルはないが、例として、航空予約システムは運行システムと深く関わり、決済システムとも深く関わっている。他の領域との相互依存関係が何らかの形であるのではないか、現在、電力、通信、水道といったところは明らかに関係があるということが見えてきている。その中で、領域横断的にどう対処するのかについては、地震等については調整が掛かってきているが、未だ上手くできていないところがある。一般的に発生しそうなことについては、領域間の対話が始まっていない。第１次基本計画の下での行動計画は、各分野は業法に基づき取組みを行う、地震についての災害対策法等は別だが、横断的な部分についての業法がないので、官と民との持ち寄りで頑張りましょうということで始まった。業法ではリスクについて考え、それを超えた場合に、罰則をどうするかについてそれぞれの領域で考えている。それぞれの領域で考え方は異なる。それは別としても、少なくとも相互に関係し合っているところは、皆で問いを解いていかなければならないということが行動計画であった。様々なシステムの障害、障害の原因があり、それらを限定することは企せずに大きく見るということで、どこまで官或いは民ができるのかを相互に検討していくということである。国民の視点がないのではないか、「がまんしろ」ということについては、そうではない。利用者、ステークホルダーとしての国民が、どのように施策に対して影響するのかついて見なければならない。共倒れは避けなければならず、まだ全くできていないが、ファンクショナル・トリアージングのように、何を優先して復旧させるかについて、民の側から官の側への要望が出てきている。全てについて情報は出せませんということは止めていただきたい、民間同士でも、サービスに関する情報はＷｅｂサイトを見てくださいと言うことは止めて欲しい等が、演習を通して明らかになっている。そういったことも含めて、横断型の対応が円滑に取れるということがこの計画の目標である。個別には業法があり、それらに被せるスーパーバイザーな仕掛けは困難であり、それは個別に頑張ってほしいという前提で、広くこの国の基盤としての総合的な観点を見ながら、解決していこうというのがこの行動計

画である。決して「がまんしろ」ということではなく、きちんと「聞いていきます」ということである。それを落とすべきところは、業法或いは横断的なところなど、いろいろと考えていかなければならない。

○　サイバーテロといった観点での基礎的な、こういったケースがある、それに対する対策、攻撃の技術に関する研究の必要性を盛り込む必要がある。システム障害にばかり焦点が当たり過ぎる。サイバーテロは国際的なものが多く、事前の情報提供が必要である。短い文章でもよいので、情報提供をすべきである或いは期待する等といったサイバーテロに関する書き込みも重要である。サイバーテロに狙われるのは民間企業では重要インフラであり、政府機関のホームページへの攻撃はサイバーテロとは言えないので、やはり重要インフラが狙われやすく、この部分の是非書き込んで頂きたい。

⇒重要インフラ事業者や所管省庁が具体的にどのようなことを行うかを書き込む箇所があり、現在の行動計画でも攻撃手法について情報収集を行っていくということが書かれているが、そういったところへ入ってくるのではないかと考える。情報共有については、現在構築されている枠組の中で、全体的な主旨の中へ含まれていると考える。

○ 「ＩＴ障害の発生を限りなくゼロにする」という目標について、基本的には良いのではないかという意見は、その通りであろうと思う。別の委員が気にされていたことは、この基準がかなり影響力をもってくると、ＳａａＳやＡＳＰの個別契約において、どこまでの可用性が求められるかの条項が変わってくる。そうすると、契約のレベルで、トラブルが発生してくる。将来の電子投票システム等を考えれば、国民投票の権利に関わるものとして最高裁まで行くようなことも考えられる。運用については、もう少し詰めたことを共有すべきであると思う。理念としてはこの目標で良いのだろうと思う。その辺もまた、ご意見をいただき、事務局で重要インフラ専門委員会との橋渡しをしていただければと思う。

○ 他に、ご意見があれば事務局へメール等でお寄せいただきたい。

（５）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 －