情報セキュリティ政策会議　基本計画検討委員会
第16回会合議事要旨

１．日　時

平成20年12月3日（水）　16時00分～ 19時00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
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）
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

（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)第１次情報セキュリティ基本計画の下での取組み、第２次情報セキュリティ基本計画における

基本的考え方について

○　文章中に「安心」という言葉が追加で入っている。また、重要インフラ専門委員会における第２次行動計画のサブタイトルは「安心があたりまえ」となっているようだが、そのご趣旨を伺いたい。

⇒　第２次行動計画のサブタイトルについては、「安心があたりまえ」～誰もが安心できる社会基盤に～ということで、同委員会でご議論いただいた上で、入れさせていただいている。

○　スローガンとしてはよいかもしれないが、“安心”は人の気持ちの問題であり、コントロールできるかと言うと、何だかボワーっとしている印象がある。また、基本計画の構造を追加的に示すことによって建て付けが分かるようになったのは前進と思うが、全体設計図である基本計画では、“事故前提社会への対応力強化”が重要なメッセージとして打ち出される一方、その下の個別設計図では“安心があたりまえ”となっており、異議申し立てまではしないが、国民から見て齟齬感があるとは思う。

⇒ 安全はもちろん客観的に重要である。食の安全でも言われているが、安心できるということ、よく説明した上でリスクをよく理解していただくということも重要である。ＩＴ基本法でも、安全性・信頼性を確保して安心して利用できるようにするという趣旨が記述されており、言葉として統一したとご理解いただければと思う。

(2)政府機関・地方公共団体について

○　電子政府の利便性、セキュリティの向上に関して、利用者の認証に関して言及されているが、電子署名は認証に入らないという考えもあるので、認証だけに限定するのではなく、利用者とのインターフェース、利用者に関わるセキュリティ機能など広い観点で記述していただければと思う。また、“利用者のニーズを踏まえるとともに費用対効果を向上し”とあるが、費用対効果を“向上”という言い回しも気になる。

⇒電子政府ガイドラインに関する委員会、分科会の動向を背景に記述しているが、御意見を踏まえ、表現については考えさせていただきたい。

○　地方公共団体の部分で、業務継続計画とあるが、これは業界用語で言うＩＴ－ＢＣＰのようにデータのバックアップ、リモートアクセスの確保などＩＴに関するものを言っているのだと思うが、地震対策やパンデミックの対策などについてやれと言いたいのでないの

であれば、書きぶりが唐突な感じがする。

⇒ここに書かれているのは地方公共団体のＩＣＴ部門の業務継続計画ということである。そのガイドラインを８月の下旬に作成しており、各地方公共団体に普及を図っていくということである。

⇒そのガイドラインを引用として脚注に記載したい。

○　ＩＰｖ６の対応化について記述があるが、ここは情報セキュリティ対策の推進に関するものであり、ＩＰｖ４からＩＰｖ６へ原則として移行するとした上で、情報セキュリティ上の問題が発生する可能性も十分考えられるため、情報セキュリティ上の対策を十分に考慮しつつ進めるといった記述がよいのではないか。

⇒　情報セキュリティ基本計画であるので、ご意見を踏まえ書きぶりは検討したい。

○　タイトルでは「事業継続性の確保」となっているが、中身は「業務継続計画」という記述になっている。用語の使い分けは私も悩むところではあるが、一般企業では「事業継続」という言い方が多く、金融機関や政府機関では、「業務継続」と表現していると思う。このドキュメント全体を通して、何か規則性をもって記述されているのか。

⇒　文書全体を通して、他の部分でも事業継続性という言葉が使われており、内部でもう一度整理し、タイトルを業務継続性として問題なければ変更したい。タイトルとして、他と整合が取れなければ、そのままとしたい。

○　私の解釈では、企業等では会社が潰れなければよいので、“事業”継続性となり、金融機関や政府機関は目の前の業務自体を止めてはいけないという趣旨で“業務”継続性としている。この際、そうした使い分けを採用していただければ美しいような気もする。

(3)重要インフラについて

○　重要インフラ専門委員会で検討されている行動計画の方に重要な中身が書いてあるので、基本計画にも、もう少し肉厚に記述した方がよいのではないか。他の分野の記述に比べると重要インフラ部分が薄い印象が否めない。分量バランスまで配慮されるのであれば、行動計画から、もう少し具体的な引用があった方がよい。

⇒　重要インフラについては行動計画を別に定めて、その中で記述しており、具体的、

詳細な内容については、そちらを参照いただければと考えている。他の分野については、そういったものが無いため、それなりの分量になっているということもあろうかと考える。

○　事情は了解したが、そうであれば「詳細については行動計画で記載している」という旨を、冒頭だけでなく関係箇所に明記した方がよい。表紙から順番に全部を読み込んで理解する人ばかりとは限らない。

⇒　重要インフラの重点政策部分の冒頭に、詳細については行動計画にある旨、追記する。

○　重点政策として分野横断的な演習とあるが、行動計画の方では、ＩＴ障害発生事を想定した演習であることが明確にされている。基本計画の中にも、ＩＴ障害発生時を想定した演習ということを明確にした方がよい。

⇒　演習部分について中身を少し書き足したい。

(4)企業・個人について

○　「事故前提社会への対応力強化」に向けた事業継続性確保・緊急対応体制等の強化に関する文章が難解だ。事業継続性確保と緊急対応体制の関係で、緊急対応体制を後ろに置いている。例えば、金融機関でシステムがダウンした場合、バックアップセンターに切り替えるといったことが緊急対応であり、その際はコンティンジェンシープランといった言葉を用いている。取り敢えず切り替えた後にデータを補正するなど、事務のレベルでも復旧し、業務を継続する段階が次に来るという流れからすれば、順番が逆のように感じる。

○　ウイルスや脆弱性等に早期に対応するための連絡対応体制については、別のところに書いてある平時からの情報共有と同じものを、再度言及しているように見える。また、脆弱性等に早期に対応することについては、脆弱性は元々システム内に埋もれており、それが攻撃によって、ある閾値を超えるとリスクが顕在する性格のものではないか。脆弱性等に早期に対応するという話が、「事故前提社会」への対応力強化に向けた事業継続性の確保の中に書いてあるのは、いろいろな種類の話が混ざって混乱しているように思える。どのような関係性で書かれているのか伺いたい。

⇒時系列としては確かにレスポンスがあり、その後リカバリーになるというご意見はごもっともである。ここでは、平時の対応と緊急時の対応を記述している。平時については事業継続性の確保について、日ごろから何かあった場合に備えておくということを中心に

記述している。それに加えて、何か起こった場合の緊急時の対応についても目配せをするという形で記述している。重複しているというご指摘については、平時からの情報共有は、過去のシステムダウンの事例等を共有するという趣旨であり、もう一つは、何か起こった場合、脆弱性が見つかる、ウイルスに感染したので直ぐに対応しなければならないといった非常時の対応である。中身として重複しているとは考えていない。

○　趣旨は分かるが、文章としては誤解が生じやすく分かりにくい。平時の対応がこうで、その後に事業継続が来るという時系列の流れで書くことが適当である。具体的に言えば、「ウイルスが広がった場合は～、脆弱性を攻撃され大変なことになった場合には～」といったことを書き足せば、事後のことであると分かりやすくなる。このままでは、まだ起こっていない脅威事象を早期に予防するということを指しているようにも読める。流れさえ書き分けていただければ、この順番でも読めるのかもしれないが、分かりにくい。

⇒これは、第１次基本計画からの継続でもあり、アウトブレイクが起こった場合だけではなく、そういったことを未然に防ぐということも含め、誰かが脆弱性を発見した場合に、攻撃が起こる前に情報共有を行い修正するという体制を運用している。それを更に進めていかなければ、個人情報の流出などに繋がる。起こったときに行うだけではなく、平時においても発見した場合は、早期に対応するという意味合いも含めている。

○　趣旨は理解したが、その趣旨を表現する際には、例えば改行して、「緊急時のものだけではなく、このような平時のものも重要である・・・」と書いた方が一般には分かりやすいと思う。

○　ＳａａＳやＡＳＰの活用の促進はよいが、記述において論理が飛躍している印象がある。ＳａａＳやＡＳＰなどのセキュリティサービスの活用を推し進めることによって、コスト負担を減らすと理解している。そのためにＳａａＳやＡＳＰを活用し、ＳａａＳやＡＳＰのセキュリティ対策の基準の提示や計測などを推し進めなければならないと理解している。そう読み取れるように、もう少し記述を変えたほうがよい。また、ＳａａＳやＡＳＰなどとなると、どこまで含まれるか分からないが、今あるＷｅｂメールなどを零細企業は利用しており、そういったものも含まれるのか。そういったところのセキュリティ基準などをしっかりしなければ、情報をどんどん預けている。そいったことも読み取れるように記述を変えたほうがよいのではないか。

⇒ＳａａＳやＡＳＰの活用を促進する理由を追記することで考えたい。また、Ｗｅｂメールなどについてのセキュリティ基準をどのようにしていくかは、将来的な議論でもある。ここに含まれるかについては、これからの検討として読み含められればと思う。

○　人材の育成について。民間の活用ということが含まれており、これはよいことであるが、“民間の有効な人材育成・確保に関するフレームワーク”とあるが、有効かどうかは利用者が決めることであり、民間の資格等もあるが、ここで有効と書くことが妥当かどうか疑問がある。また、人材確保についてのフレームワークは聞いたことがないので、“・確保”とするのは不思議な感じがある。

⇒　タイトルをはじめ、育成・確保という言葉を使っており、統一した書き方になっている。フレームワークに掛かるかどうかは検討させていただきたい。“有効な”としていることについては、何でも全て推進するというよりは、良いものを推進するという趣旨である。有効かどうかは、利用者によるということはおっしゃる通りであるが、スローガンとしては有効なものを推進するということで、ご理解いただきたい。皆が有効と考えるものを推進するという趣旨である。

○　「民間の人材育成のフレームワークや各種資格試験の活用を図る」ということであればよいが、有効な“・確保”を促進するとは何だろうかという気がする。民間の資格で有効なものはたくさんあるので、選択的に使用することはよいが、“促進する”ということなので、どのようなものがあるか示す際に、リコメンデーションしなければならない。あっさりと書いた方が書きぶりとしてはよい。どのような資格があり、どのように有効と判断したのか示せということになり、難しい問題になる。

⇒　市場原理に任せ、有効かどうかを判断するということである。

⇒　委員のご心配は、そう書けば政府がどれが良いかエンドースする、或いはリストを作ったりということまで踏み込むのかということか。

○　そうである。また、人材確保のフレームワークというものも聞いたことがない。共通スキルフレームワークに則り、情報処理技術者試験の活用と同時に民間資格の併用は構わないので進めることはよい。しかし、それらを並列に書く場合、両方を推進し、促進すると捉えられかねない。国がリコメンドする国のものがある訳であり、民間のものも併用すればよいが、あっさりと書き込んではどうかということである。

⇒　ご趣旨は理解した。書きぶりを含め事務局で調整した。人材確保についてのフレームワークはないということも分かった。“有効な”と書くことで、エンドースしてリストを作ってしまうと捉えられないように、表現を考えたい。

○　情報セキュリティ人材に限らず、この手のもはたくさんあり、このような書きぶりは結構インパクトがあるので、慎重に行ったほうがよい。また、“官民の適切な役割分担の下”とあるが、このような表現も珍しい。役割分担はあるが、その下にこのように具体的なノーテイションがあることは珍しい。書きぶりは調整される必要がある。

⇒　“官民の適切な役割分担の下で”ということに関しては、昨年１月の人材育成・資格制度体系化専門委員会の報告書において、そのような記載がされている。この報告書の内容を踏まえて、事務局では書きぶりを検討されるものと理解している。

⇒　事務局の人材育成に関する理解では、人材育成についてはいろいろな取組みがあり、それが世の中にどのように効いてくるかということは、時々により評価、検討を行っていかなければならない。内閣官房の人材育成に関する検討でも、完全ではないが調整は行った。他の省庁、例えば経済産業省や総務省でも、それはいろいろな形の中で行われている。環境、ニーズ、技術の動向、人材に対するデマンドを踏まえ、継続的に検討を行っていくということは、政府としては当然であるということが基本である。これを計画の中で、どのように扱うかは、基本的に人材育成・確保を横断的な柱として立てており、施策実施の評価のプロセスの中でみていかなければならないという理解である。評価の結果、問題がある、或いは横断的にある程度見直さなければならないというコンセンサスがある場合、内閣官房と関係省庁の間で調整するのか、第２次の人材育成専門委員会などを組織するのかは、事務局と各省庁、人材育成専門委員会の皆さんと相談した上で、考えていくというところではないか。ここでは、評価などエバリュエーションなしで行っていくのではなく、継続的に行っていくことが基本である。評価をベースに、評価というプロセスの中で、内閣官房としては取り扱っていきたい。その先で調整、高らかな政策が必要であるという認識の下に動かなければならないということは、委員会や各省庁の調整の中で行っていくことになるのではないかということが基本的な考え方になるのではないか。

○　書きぶりの問題だと思う。人材育成・資格制度体系化専門委員会の委員でもあったので、官民の役割分担を適切に行うということは適切だと思うが、その後の書きぶりが有効なものを選んで使いなさいとなっており、共通キャリアスキルフレームワークにおける情報処理技術者試験と並列に書かれているところが、これでよいのかと感じる。その部分で多少の段差があってもよいのではないか。共通キャリアスキルフレームワーク、情報処理技術者試験の制度づくりに参画した者としても主張したい。

⇒　書きぶりについてのご指摘は理解している。書きぶりについては事務局で調整させていただきたい。

○　この部分に関して、ここだけ妙に細かいため、読んでいて若干気にはなった。企業の人

材育成に関して、様々なものの活用促進するとなっているが、これは、企業に対して何らかの促進税制、補助金などのインセンティブを出すということを言っているのか。何故、企業に関してこれだけ書かなければならないのか。政府に関しては、どんどん記述してもらいたいが、企業についてこれだけ書いてくれた上で、どのように促進するのか。企業が勝手に促進しろという感じなのか。

⇒　税制や補助金についてはここで書くレベルのものではない。政府の計画でも、到底すぐに書けるものでもなく、この段階ではそういった考えはない。頑張って使って下さいということで、エンカレッジするという意味あいである。

○　民間から見ると余計なお世話というか、これを見て心配になるのは、上乗せして責任を問われるというか、何か起こった場合に、政府はこう言っているが、お前のところは何もやってないではないかと言われかねないということだ。三行くらいのシンプルなもので、書いてもらう方がよい。重要インフラについては、計画の中で言いかねることは封印して、別途行っているが、ここだけ異様な感じがする。しかも、多少害がある気がする。

⇒　重要インフラについては、封印するということではなく、もともと所管法の中で、事業者の方々と政府の間で、横断的に眺めて、改めてやるべきことは何かについて合意を形成しながら進めていくということで、出来ている計画である。その観点では、重要インフラに関する民間の議論が封印されている訳ではなく、これは役割分担の中で計画が決まっている。記述に関しては、先の委員からの意見も踏まえ、うまく調整していきたい。ここの書きぶりは事務局で検討させていただきたい。おっしゃる趣旨は理解している。

○　政府機関、企業部分にある人材育成に関する記述と、情報セキュリティ人材の育成・確保の部分の記述は再掲となっているが、微妙に表記が異なる部分がある。

⇒　これは再掲であるので、合わせたい。

○　これまで、様々な観点で議論がされてきたが、人材育成についても様々な観点がある。国際的な競争力があるような人材を育成するような視点を追加するということは可能か。企業部分に書くべきか、政府機関部分に書くべきかということもあるが。

⇒　三年間で取り組む施策については、内閣官房で取りまとめを行い、各省庁と調整しつつ行っていく。この計画の大部分が政府を主語として、取り組んでいくことになる。国際競争力に資する人材育成については、情報セキュリティの枠組の中で行うのか、その他のところで行うことになるのか悩ましいところはある。具体的に取り組みを誰が引き取る

のかということの調整が無ければ、具体的に書ききれない。情報セキュリティ産業に関する国際競争力の話はあるが、国際競争力に資する人材育成は今のところ出ていない。事務局としては調整が必要になってくる。

○　具体的な引き取り手という問題はあるかと思うが、非常によいポイントではないかと考える。

⇒　国際競争力に資する人材育成とした際に、具体的にどのようなイメージをお持ちかお伺いしたい。

○　幅広にいろいろと国際的に通用する人がいる。アカデミアの世界でも、国の連携の中でもそうである。例えは、企業があるものを抱えて標準化に向かうという話もそうである。そういった視点での育成が今ないのではないか。経験論からくるものなのか、非常に難しい問題であるが。

⇒　英語ができ、国際の場で主張、調整できる国際人を作るという議論にも受け取れるが、問題意識はどういったところか。

○　もう少し具体的に言えば、例えば、国を背負ってある技術を持って出る場合に、かなりリーダーシップをとって、国際の場でいろいろな連携ができないと話しにならない。提案文書を英語で読み上げるだけではない。他の国では、そういったことを行っている人がたくさんいる。どのように人材を育成するかは、クリアな提案を持っていないが、そういうレベルのものはここには書きにくいだろうか。

⇒　おっしゃることの重要性はよく分かるが、情報セキュリティとしての枠組があり、この分野として特に国際人が必要だという説明が、なかなか付きにくいというのが率直な意見である。

○　引き取り先についての問題もあると思うが、個人の部分が非常にシンプルであり、国民に対するメッセージとしてどうかという印象がある。主語が無く、例えば、リスクを被害に変えないための環境整備などは誰が行うのか分からない。また、質問への適切なアドバイスや訪問対応を行えるサポータの育成は誰が行うのかなど、もう少し具体的に書かなければ分からない。誰が責任をもって行ってくれるのか、非常に不親切な気がする。国民に対して公表するということでは、国民の方のレベルが非常にまちまちで、個人が対策の基本となることを考えれば、非常に不親切である。

⇒　政府の計画であるので、主語がないものについては基本的には政府がということになる。

○　政府がリスクを被害に変えない環境を整備するということになるが、それは民間も含めて政府がそういった環境を整備しますという趣旨か。

⇒　政府がそういった取組みを進めるということである。三ヵ年の大きな計画であるので、その方向性を示している。個別具体に誰がいつまでにどうするということについては、これまで同様に、セキュア・ジャパンの年度計画の中で書いていくという構造を持っている。３年間に通じる書きぶりを相談しながら書いているということである。

⇒　一般利用者のセキュリティレベルを上げるために、様々な団体のネットワークを活用し、団体の方々と協力し、普及・啓発を行っていく仕組みづくりの推進を考えている。電気通信事業者による予防的措置として実施する情報セキュリティ対策については、私どもの研究会で、永遠のビギナーといった話もあり、利用者の意識があっても能力がない、意識がない方々に対しても、ネットワーク側からセキュリティ対策をある程度行うということが、利用者のセキュリティの穴を埋めるということで有効ではないかという報告があり、そういった施策を推進してまいりたいということである。

○　個人に関する記述で、“情報モラル”という言葉があるが、未定義語であり、気持ちは分かるが、解説が必要である。

⇒　解説を追加したい。

○　クラウドコンピューティングに関連する記述に、自身が直接的に関与しないサーバで管理するとあるが、これはクラウドではない。自分が自分の持ち物でないものに預けることは、業者やプロバイダーに対してもあるので、これは技術的におかしい。また、情報を預ける人が気を付けるとあるが、クラウドでは分からない。情報がどこにあるのか分からなくすることがクラウドであるという定義をする人もおり、セキュリティ的には崩壊している。更に複雑なのは、日本企業、法人が運営しているのであれば、雲・クラウドでも構わない。世界中に散らばり雲になれば、情報の取扱いに関する日本の法律が全く機能しない。例えば、複数のサービスを動的に結合させ、ひとつのアウトプットを行うサービスを考え出した場合、Ａ企業からＢ企業に情報が渡り、Ｃ企業でそれを検索した結果が返ってくるということは、すばらしいサービスに聞こえるが、その過程で情報が漏えいする可能性もある。日本の個人情報保護法は向こうでは役に立たない、また、国が変わり、複数の企業を跨いだ場合にはどうしようもない。やる人が考えてやるべきという言い方は酷い。

○　また、２０１２年の姿の部分では、クラウドコンピューティングの記述が消えており、今後取り組む重点政策の中では、情報を預ける主体についての記述がひとつもない。２０１２年に向けて対策がないのだとすると、クラウドについては今ある課題が全く整理されていない。法律の問題、漏れた場合の保護の問題、国際協調をどうするかという整理が一切ない。地方公共団体はお金がなく、コスト削減しようということであれば、真っ先にクラウドに行くと思われる。メールサーバを捨てれば安くなることは明らかである。年間で１アカウントが千円くらいであれば、自分でやるよりは安い。それに飛びつくことがあった場合に、本当にそれでいいのか。重要インフラの一事業者が、メールの管理、図面、オフィス機能を持っているとして、図面のやり取りなどをクラウドは便利だということで、使ってよいのか。政府機関も同じである。そういった問題解決がないまま進んできている。個人的な意見としては、安全が確保されるまで使うべきではない。相手は雲であるので、安全かどうかも分からない。法的、或いはガイドラインなどの縛りで解決しなければ、将来間違いなく大変な問題になる。情報が漏れましたといった際に、否認されればお終いである。クラウドについてわざわざ触れるのであれば、後ろへ何か書くか、いっそ書かないか、どちらかにすべきである。

○　今の委員の意見は私も気になっている。クラウドの価値評価は意見が異なる。この問題抜きで、セキュリティは論じられないのではないかと思う。総務省や内閣官房との仕事をしているが、クラウドへの対応はほとんどできていないというのが実状である。まずは勉強してもらう必要があるなとは思う。そのような段階でどう書くかが問題である。いっそペンディングにしてしまうか、書くのであればきちんと勉強して書かなければならない。

⇒　ここは、今委員が述べられたような問題意識をどのように伝えるかという部分であり、記述を適正化し、今述べられたことを抽出して書くようにしたい。クラウドについては、新しい問題をどう解決するかということであり、ＮＩＳＣとしては、それを認識した場合にそれを問題としてレイズし、政策会議の命を受けて、委員会を設けたり方策を検討するという機能がある。そのことを明示的にこの計画で示していないので、ＮＩＳＣが本来持っている機能として、新たに登場してくる問題に対して、技術的、社会的、法律的にアイデンティファイし、問題解決に取り組むことを明示していくことで考えたい。クラウドや情報を預ける主体に絡む問題、法律的、国際的問題などについて、本来のＮＩＳＣの業務を節をひとつ立てて明示したい。クラウドなど、新しい技術が出てきた場合の問題を含め、これから解いていく、解かざるを得ない問題を、政府も勉強しながら解いて行くということを記述したい。

○　了解した。ただし、クラウドは何が問題かと言えば、技術的云々ということもあるが、

利用した人が守られることがおそらくないであろうということだ。捕まらない上に、守られないという問題がもはや目の前にあり、ＮＩＳＣが検討するとなると技術的な話題になりそうな気がする。

⇒　捕まらない、守られないということを検証する必要があることは事実である。また、ＮＩＳＣは、技術だけではなく、政策面でのコーディネーションにも入っていく。その意味では、技術面に偏らない、問題の変化にきちんとキャッチアップしていく、といった形で記述したい。内閣官房単独ではなく、実質は各省庁と連携をとりながら、調整しながら進めている。各省庁も、クラウドなど新しい技術が出てきたことによる問題は感じている。それを改めて記述したい。

○　これまで議論があった具体的なサービスや技術について、ここで書いてもきりがない、また、来年新しいものが出てくるかもしれない。おっしゃられたように、新しい技術に伴う懸念や問題点を早く抽出し、気が付いたら自治体や重要インフラが使っていた、これで高齢者の自宅が分かるということがないように、早く対応し、後手に回らないように、ひとつ節を設けて、新しい技術に対応するということを盛り込むことは、よいことだと思う。

○　クラウドといったバズワードをこのような形でおもて出ししない方がよい。強いて言うならば、ＳＴＰ化されたコンピューティングファームの提供形態だと思う。クラウド、ＳａａＳ、ＡＳＰにしても、今言われたような問題は発生し得え、セキュリティレベルが可視化されていないサービスはどんどん増えていく。これはある意味で、いたしかたないことだが、電力やガス、水道の供給は国内で一定のレベルで限定されており、そういったものが可視化される、規制の対象となることはあるが、コンピューティングファームはどこにあるのか分からない。そのような事態が、ユーティリティ化されればされるほど、出てくる。それが、クラウドであれグリッドであれ関係ない。括弧付きで例示のような形であればよいが、おもて出しすることは賛成しない。

○　クラウドは、ＩＴ企業がアピールしている形態であり、その他のサービス提供事業者もこの形態は結構であるとしている。新しいネットワークデータスペースの在り方ということか思う。遠隔グリッドで行うということもあるので、グリッドも念頭には置いておいた方がよいだろう。

○　個人の三つのパートの記述の部分についてだが、２００９年の状況、２０１２年の姿、重点政策を続けて読んでいくと、最後の重点政策の部分が具体的にメッセージとして伝わりにくい。パブリックコメントにかけると、誰がどうやってやるのかというコメントが消費者団体からたくさん出てきそうな気がする。先ほど総務省からの説明では、既にそうい

った取組みも始まっているということであった。また、情報通信審議会などの消費者系の懇談会に参加してている当方からすると、もう少し具体的に示さないとなかなか動いていただけないのではないかという懸念がある。

○　目指すべき姿として書かれている部分で、いろいろと書き込まれているが、一般の人が読む場合に、ロジックがよく分からないのではないか。このまま読めば、政府は最大限の努力を行い、その結果、教育機関などがこのような姿になっていると書いてある。２０１２年のこのような社会において個人が以下のような姿になっていることを目指し、関係者は今後の取組みを進めていくと書いてあるが、その次には姿だけを書いているのではなく、取組みが書かれており、文章として読んでいくと、なかなか理解しづらい。例えば、「リスクを理解しても対策を行わない個人等に対する対応の開始」とあり、対策を行わない人は一定数いる、情報弱者も存在し続けると考えるとある。目指すべき姿とすると、これらに呼応してしまうので、文章を整理していただいた方がよい。少なくとも、「以下の結果となっている」を「結果となっているとみられる」のような表現にしていただかなければ、最後の重点政策のについて正しく読まれない。

○　個人の２００９年の現状で、インターネットの利用に不安がある個人が４割を超えるということは、グラフを示し、事実を書いていると思う。それとは別に、「利用に関してリスクが高まっていると考えられるなど」とあるが、「考えられる」という表現はカットすべきではないか。また、「リスクは依然として下がっていない状況にある」とあるが、リスクは存在し続けるもので、下げることを目的としているかといえば、おそらくそうではない。このパートで述べたいことは、情報セキュリティ対策の重要性を認識し、自分で対策をし続ける個人を増やすということが目的だと思うので、それが分かるような整理した書きぶりにしていただきたい。「あらゆる個人に対して情報セキュリティ対策の重要性を浸透させることは容易ではない」など、いろいろと書かれているが、そういった思いは抜いていただき、もう少し分かりやすい表現にしていただきたい。つまり、重要性に対する認識を高める必要性だけを言っていただければよい。

⇒他の分野との平仄をとるために、テンプレート化して記述していったところがあるため、つながりがうまくないところがあるかもしれない。上手く直したい。また、ファクトベースの方が分かりやすいということを中心として、全体のトーンを合わせる形で見直したい。

(5)情報セキュリティ技術戦略の推進について

○　「経済的メリットの獲得を目的とした、計算機及び利用者に害を与えるプログラム（マ

ルウェア）は年々増加しており」とあるが、経済的メリットの獲得を目的としてはいけないのかとも思える。“ 不正 ” という言葉が頭に出てきていないために分かりにくくなっている。

⇒害を与えるプログラムを何故ばらまくかといえば、それは不正な経済的メリットを獲得することを目的としているということを表現しているので、経済的メリットの前に “ 不正な ”、“ 不正に ” という言葉を補えば趣旨が明確になるかと考える。

○　分からなくはないが、経済的メリットとは何か、それに “ 不正 ” を付けるということがよく分からない。単純に考えれば、計算機及び利用者に害を与え、経済的なメリットのみの獲得を目的とした、とするほうが分かりやすいのではないか。不正な経済的メリットとすると、ひとつの言葉として、どう理解してよいか分からないところがある。

⇒マルウェアなど、メールやＷｅｂを介して感染する場合がある。例えば、クレジットカード番号、ショッピングサイトのＩＤを盗み取るキーロガーなど増えてきている。その目的は、盗った上で、それを不正使用し何らかのメリット、経済的利益を得ようというものであるということを表現したい。利益の受け方も、様々な形態があるのでここではメリットと表現している。

○　不当利得の獲得を目的とした、と直してはいけないのか。メリットという言葉が非常に気になる。

⇒「経済的メリットの獲得を目的とした」という言葉が、読点で区切られ「計算機及び利用者に害を与えるプログラム」に掛かっており、分かりづらいのかと思う。「計算機及び利用者に害を与えるプログラム（マルウェア）で、経済的利益の獲得を目的としたものは、年々増加してきている。」などとすることで、分かりやすくなるのではないか。

⇒この部分は、近年非常に多様化してきているということで、シンプルにしきれないという悩みはある。実際、マルウェアは最終的にはなんらかの形で、経済的メリットを得る方向に向くが、それぞれがいろいろな目的で作られ、いろいろな形態がある。単純にクレジット番号だけを盗り、何らかの利益に換えるシンプルなものであればよいが、その部分が変わってきているという認識でこのような不明瞭な書き方になってしまっている。主張を的確に表せるように検討したい。

○　愉快犯的なものは認識していないということか。

⇒それもあるが、愉快犯的なものよりも圧倒的な害を与えるものへ大多数がこの数年でシフトしたということがある。愉快犯的なものが依然としてあるということは事実だが、害を与えるマルウェアが増えてきていることを、この文脈ではフォーカスしたいと考えている。

○　メリットという表現は良いことのようにも思えるため、やはり違和感がある。

○　犯人側から見ればメリット、ということであろう。いずれにせよ大した話ではないと思う。

⇒記述の適正化はもう一段図りたい。

○　「情報セキュリティに関するデータベースの整備と共有、あるいは隔離ワークベンチの構築などによって」という記述があるが、「データベースの整備と共有」、「隔離ワークベンチの構築」は別のものなので、「あるいは」で繋げないのではないか。

⇒おっしゃる通りであり、全て並列となるよう見直したい。

(6)情報セキュリティ人材の育成・確保について

○　企業における情報セキュリティ人材の育成・確保について、共通キャリア・スキルフレームワークや各種資格試験の活用が、企業の部分に書いてあることに違和感がある。政府機関の部分に書く、あるいは、情報セキュリティ人材が保有するスキルの見える化の推進の部分にもフレームワークの活用について記述があるので、こちらへ移していただいたほうがよいのではないか。

⇒ここは、企業部分からの再掲であるので、先ほどの意見とあわせて改善することで、事務局として対応したい。

○　政府機関の部分で、「最高情報セキュリティアドバイザーやそのサポートスタッフを中心に戦略的にアウトソーシングの利用を進める」とあるが、これはアドバイザーやそのスタッフを雇うことが戦略的アウトソーシングなのか、それともアドバイザーやそのスタッフが戦略的アウトソーシングを進めることを判断するということなのか。

⇒趣旨は、アドバイザーやスタッフについて外部の専門家をアウトソーシングして活用するということである。その趣旨に合わせて文章を見直したい。

(7)国際連携・協調の推進

○　「政府が特に強みを発揮できる分野」として、リスク情報の共有という観点と、インシデント対応の国際的な連携体制構築と読めるが、これは正しいのか。

⇒諸外国政府機関等との間での政策動向に関する意見交換など、情報収集や情報交換がまずあり、それに加えて「例えば」として例示として挙げており、それだけではない。各国政府との関連の中で行われている情報収集がまずベースとしてある。

○　情報セキュリティ政策に関するＰＯＣ機能の強化と情報共有の促進とあるが、第４章にあるＮＩＳＣの強化と役割の部分にも、国際連携でのＰＯＣの機能の強化を担うということを記述した方が、より明確になってよいのではないか。

⇒ＮＩＳＣの強化の部分に、ＰＯＣ機能についての記述を盛り込ませていただく。

○　個人の部分では、“安心”という表記があっても違和感はないが、企業に関して“安全”はあっても、企業が“安心”してというのは、あまり聞かない表現である。

⇒私の個人的な“安全・安心”という言葉についてのインプレッションは、ひとつになっている。情報セキュリティだけではなく、普段の事故や障害が起きないといった、広い意味でのセキュリティを意味する安全・安心だと理解している。例えば、ディペンダビリティでは、非常に狭いディペンダビリティからニューディペンダビリティという広い概念がある。このような形で、セキュリティに対応した安全・安心ということで、これを切り離してはおかしくなるのではないか。

○　安全は、ここまでやれば安全だと定義が可能な概念と考える。安心は、心の問題であり、いくら対策を講じても予期せぬことが起きるかもしれない、天が落ちてくるかもしれないということは杞憂だと言われても不安だ、ということは定義できない。企業は定義された活動を行う、またプロであり、リスクをきちんと評価し、安全という水準を定めて行うという概念があるのではないか。安全と安心は一体不可分なものではないと感じた。

⇒アジアに展開するのは大企業だけではなく、中小企業も最近は出て行くこともある。企業を組織として見た場合、企業のオーガナイゼーショナル・マインドがあり、安全を定義して運用していく。例えば、経営者のマインドから直接展開されるところで、実際に安心できないと思う経営者によって、活動が縮退するということも現実にはある。経済活動

において安全を確保していくことは、政府として一番最初にやるべきこととして挙がってくる。もひとつは、その地へ展開していく企業が安心して活動ができるということに対しても、心配りをしていくことも政府の役割としては必要ではないか。そういったことで、安全、安心を一括りとして書いていた。安心は個人に属するものであり、経済活動、企業とは切り離して考えるということもあるが、経営者を含めそこに関わる人々のマインドによって左右しているものもあり、それらを含め取り扱ってはどうかと考えている。

⇒　あくまで個人の気持ちになるのかもしれないが、今の補佐官の説明のようなこともあるので、安全・安心という言葉を使うということで、ご了承いただければと思う。

○　答えられるようにしておけばよろしいのではないかと思う。

○　企業においては、“安全・安心”ではなく、“安全・安定”だと思う。政府が行うとすれば、そのための基盤づくりだと思うので、できればあまりマインドの問題ではない“安定”という言葉を使ったほうが、理解が進むのではないかと思う。

⇒　日本語としての語感もあり、どの言葉がよいかは一概には言えないが、基本的には定義の問題だと考える。“安定”、“安心”の定義があって、“安定”のほうがよいということだと思うが、ＩＴ基本法でも安全性、信頼性、安心といった書き方があるので、使っているとご理解いただければと思う。

○　補佐官がおっしゃるように、世間に定着していると仮定するならば、単なる心の問題だけではなく、“安全・安心”と組で使われる場合には、哲学的に言えば、共同主観である。intersubjective という言葉が現象学にある。そのようなニュアンスもあり、単なる主観ではない。哲学ではないので、そこまでは書けないが、そういったニュアンスが伝わるように言ってもらえればよいのではないか。それは定量化は困難であるということも書いておかなければならない。“安定”や“安全”は、何かメジャーを作り、定量化可能なものに近づけるということもあるが、そうではないものも世間にはある。そういったことも入れておくということもあってよいのではないか。

○　元祖“安全”派ではあるが、安心を使う場合にも、「安全・安心を確保するため、安全・安心なビジネス環境を構築」といった、同義反復的で、意味の空疎さが目立つ使い方だけは避けていただければと思う。

○　各種取組み施策の表で、（ア）の情報セキュリティ政策に関するＰＯＣ機能の強化と情報共有の促進が無いが、何か意味があるのか。

⇒これは、ＮＩＳＣの機能の強化として表全体に関わるものである。

○　表には分野として政策の欄があるので、(ア)は政策ということではないのか。あるいは、全体に関わるということで記述が無ければ違和感がある。

⇒　意図としては、表全体に関わるものということであるので、誤解がないように書き方を考えたい。

(8)犯罪の取締まり及び権利利益の保護・救済について

○　「また、サイバーテロに対しても同様の取組みにより備えを強化する」とあるが、同様ではないと思う。サイバーテロはいつ起こるかわからない、いわゆる経済犯のように繰り返し発生しある程度類型化できるものとは異なる。サイバーテロは全く違う意図と、技術力を持っている可能性がある。その意味でも、同様とすると経済犯と同じレベルと読めてしまう。もう少し補強があった方がよい。

⇒　同様にとしているのは、官民連携による取組みを推進するといったものであるが、書き方については検討したい。

⇒　意図と技術力は異なるかもしれないが、備えるための対策は、例えば周知、啓発や国際連携など、方法論としては同様のものが必要であり、このような書き方にさせていただいた。

○　それは分かるが、これを見せられた国民としては、ここで特出ししている割りには、同様となっており、形だけ進めるという印象があるので、もう少し記述していただきたい。

○　「国民が不用意に犯罪に関与することがないように」とあるが具体的にはどういったことか。著作権の侵害やスパムの送信のようなものを言っているのか。

⇒　不用意にとは、制度をよく理解していないために、違法行為を行ってしまうなどがある。

○　おそらくそういうことであるとは思うが、何故それを敢えて盛り込んでいるのか、具体的な記述がなければ、理解しづらいのではないか。少なくとも一つは例示がいるのではないか。前提条件として補足すべきことが入れられるのであれば、入れておいたほうがよい

のではないか。

⇒　目指すべき姿の部分に補う形で、例示を入れるということでよろしいか。

○　その部分は将来の姿であるので、法的な制度の変更もあるかもしれないため、現況を説明している部分で、現状そういった実態があるならば、入れてはどうか。例えば、自分の常時接続のパソコン経由でウィルスをばらまいている、ファイル共有ソフトで出してしまったなどを記載し、それに対応させてはどうか。

⇒　問題意識が明確に示されずに、唐突に出てきていることが気になるという理解でよいか。問題意識が明確になるように、記述は考えさせていただきたい。

○　権利利益の保護・救済のための基盤整備の推進について、保護については書いてあるが、救済については、あっさりと基盤整備をするということだけが書いてある。これは具体的なものが何かあるのか。

⇒　今後、具体的なものがあれば出していきたいということであるが、現状では書けるものが出てない。

○　国民生活センターなどに問い合わせなどは行わないのか。

⇒消費者行政は、保護行政でもあるが、救済については様々な形態がある。例えば、銀行口座などは制度で救済しているが、一般的には民事での損害賠償などである。消費者行政では、まず問題になっていることを消費者側で上手く助けるということがあり、犯罪に巻き込まれたときにそれをどう手助けしていくかということが、消費者行政の一番最初に来る。ロー・エンフォースメントは、犯罪化したところをどのようにパニッシュメントを与えるかということである。また、最後に救済を社会システムとしてどうやっていくかという三段階の構えになっている。消費者行政は前段のところにあるという理解で書いている。

○　前回、ＡＤＲに関する意見があったがそのことについては触れなくてもよいのか。

⇒政府の計画であり、実際に政府が取り組むものになっている。新しい問題として出てきた場合は、新たな課題への取組みということで吸収したい。情報セキュリティに関して、ＡＤＲを作るという動きはまだない。刑法の改正の課題など、現状で犯罪化しなければならないという政府の取組みは凡そできている。それらを踏まえ、各省庁とも相談し、現状

で施策として書けるところで書いている。

○　「情報を預ける側の権利利益情報を預かる側が保護する取組みに係る情報開示の促進」とあるが、書きぶりがおそらく不足しているのではないかと思う。この意図を推測すると、インターネットで買い物をする際に、サイトの約款などは長く、大事なことは一番最後に書かれており、実際は読まないため、重要な事柄について分かりやすい共通の言葉でおもてに表示するということではないか。例えば、それを義務化するなどにより、ユーザが見て、このサイトは、カード番号が盗まれればお金を返してくれる、このサイトはそのようなことが起こってもあなたの責任ですと書いてあるということが分かり、そのことによりユーザがサイト選ぶ際の参考にできるようになるがために、競争が生じて、よりよいサービスが出て行きやすいだろうということではないか。ここで書くべきことは、保護する仕組みではなく、情報を預かる側が漏えいなどの不測の事態が起こったときに、どこまで救済するのか明示的に分かりやすい共通の言葉、方法で提示するということだと思う。

⇒書き方は意見を踏まえ、関係者と相談したい。重要事項説明の義務化については、先回りの施策はもちろんあるが、規制的なものについては、マーケットに対する関与の仕方として適正かどうかという議論がある。特に重要事項説明の義務化については、不動産取引などでは義務化されているが、それは多くの問題でてきて、どこに問題があるか説明するということで義務化されている。約款の後ろに小さな文字で書かれているなど、確かに問題があるが、明示することを義務化することによって今の問題が解決するかということは検証できておらず、ここは促進という表現にしている。

○　義務化せよということではなく、促進でも構わない。保護する内容を開示されてもしょうがないということである。

⇒保護はどうなっている、救済はどうなっているという視点が書いてあればよく、保護する仕組みは重要ではないということで理解した。

○　可能であれば、保護・救済に関して「事故前提社会」ということを踏まえてという趣旨のことを入れられないか。情報や技術の非対称性がある。使わせる側も、このようなリスクがあるということを、救済とまではいかないまでも、提示しなければ、よい意味での普及、利用に繋がらないのではないか。

○　そういったことは入れてもよいのではないか。非対称性、消費者保護、契約適正化の前提に立てば、そいったことはむしろ入れるべきではないかと思う。

⇒事務局で検討させていただきたい。

○　先ほどの安全・安心の議論に関して、「サイバー空間の安全の確保に向けて」とあるが、ここは“安全”だけになっている。また、国際連携・協調の推進の表について、本文からのリファーがない。また、広報啓発、権利利益とあるがこれは、他の４文字熟語の表現に合わせれば、広報・啓発、権利・利益ではないか。

(9)政策の推進体制と持続的改善の構造について

○　先ほどの委員の意見で、ＮＩＳＣの強化について、ＰＯＣ機能の強化についても言及するということで、事務局には対応いただきたい。

⇒その他、新しい課題への対応についてもここに記述したい。

○　ＮＩＳＣの強化について、「民間の人材を積極的に活用することに努めるとともに、諸事情によりこうした人材の確保が難しい際にも、政府内の人材を最大限活用し、」とあるが、「諸事情によりこうした人材の確保が難しい際にも」という記述は要らないのではないか。民間で難しかった場合に、政府内でということは止めていただきたい。

○　調整が必要かもしれながいが、今の意見について事務局で検討していただきたい。

(10)全体を通して

○　　中小企業の情報セキュリティ対策の推進に関して、「人員、予算、時間など、主にリソース不足から～」とあるが、時間は皆に等しく与えられており、企業規模に関係ないと思われる。３つ並べたければ、ＩＴインフラやファシリティといったものに変えた方がよい。

○　　中小企業と大企業の格差を示す図で、「情報セキュリティ監視ソフトの導入」は格差が９．３ポイントと、格差が少ないようにも読めるので工夫が必要ではないか。全体の情報セキュリティ監視ソフトの導入率がそもそも少ないのではないか。

⇒全体の導入率がそもそも少ないということであれば、検討したい。

○　　図表の番号が、参照される順番になっていない。また、ＩＳＭＳの取得数については、１２月の段階の最新版を使われたほうがよい。また、マルウェアとコンピュータウイルスという表現については、書き分けられているが、敢えて分ける意図がないのであれば統一

したほうがよい。国際連携・協調の推進に向けた取組みの各種施策の表で、リージョンの標準化の欄が斜線になっているが、標準化についてはアジア標準といったものも議論されている。

⇒表の斜線については、現状の取組みがないということで、斜線を引いているが、少し検討したい。また、図表の番号については、実際の図・表の配置とともに見直したい。

○　今日いただいた意見を踏まえ、事務局で整理し、各省庁と協議の上、第２次基本計画の案文を本委員会の案文として、１２月１０日に予定されている情報セキュリティ政策会議へパブリックコメント案として諮りたい。今後の修正については、今日いただいたご意見を極力踏まえ、事務局と委員長である私に一任いただければと思うが、よろしいか。

○　（異議なし）

○　それでは、そのようにさせていただきたい。議事は以上で終了する。

○　今年の１月から１２ヶ月間にわたり、非常に活発かつ有意義な討論、ご指摘、ご質問をいただき、改めて感謝を申し上げたい。

(11) 資料の公開、今後の予定について

事務局より、資料の公開、今後の予定について説明がなされた。

－ 以　上 －