# 情報セキュリティ政策会議　基本計画検討委員会
# 第15回会合議事要旨

## １．日　時

平成20年11月17日（月）　16時00分～ 19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 |
| 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 |
| 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<br>（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)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

○　ニュアンスを強くしたいために敢えて「事故前提」という言葉を使っていると思うが、ニュアンスを別にして、その意味を探ると、サイバー攻撃等の情報セキュリティの脅威を考えた場合、それは犯罪行為であり、「犯罪を前提にするのか」という連想が強く働き、違和感があるかもしれない。一方で、地震などの天災を考えた場合、規模や被災の仔細は“想定”するのだろうが、地震が来ること自体は“前提”としなければ日本では生きていけない。そういうニュアンスで考えれば、“前提”という言葉で、あながちおかしくないと思う。

○　「力強い『個』と『社会』の実現」とあり、その他にも“強い”個と社会を強調している節がある。一方で、情報を預ける主体としての個を考えた場合に、専門的な情報の非対象性というか、預かる側は専門的なことを要求されることは当然だと思うが、預ける側は非常に細かい点まで確認するわけにはいかない。強い個を求めるのはよいが、弱い個に対しても配慮しなければ、あまり強い個を強調しては、弱者切捨てのような印象を与えかねないということが、多少心配である。

⇒強い人ばかりではないのは事実であり、弱い者については具体的な施策として、個人の部分、情報提供主体の部分で対策を考えていくという構造になると考える。

○　切捨てという印象にならないように、何らかの配慮はするというニュアンスをどこかに入れておく必要がある。よろしくお願いしたい。

⇒「力強い『個』と『社会』の実現」に関する記述のバランスを考えていくということもあるが、情報セキュリティ先進国としての考え方の中で、先進国の意味として、弱者切捨てではなく、できない人も対応できる社会を創っていくという意味ももち、それと併せて、主体的に強い社会も考えていくというバランスの書き方でどうだろうか。

○ それでよいと思う。

○ 個人の方は、まさに専門家ではない人ということになる。専門家はきちんと説明をし、専門家ではない個人は、説明されたことは理解して下さいということである。専門家は理解できるように説明しなければならないが、その前提で、説明されたことは一定程度理解する、重要な事項に関して理解する必要がある。情報セキュリティに関する重要事項の見方

などのガイドライン等になるのかもしれない。

○　“事故前提社会”と“事故想定社会”について、今回２つの選択肢として提示された経緯をお伺いしたい。

⇒先の委員も述べられたが、“前提”とする場合、「事故はあるものだ」とする強い意味が出る。“想定”とすれば、考慮に入れておくというニュアンスもある。“事故前提社会”は、本文には対策を怠る訳ではないと書いており、また“対応力強化”というところまで読めば良いが、言葉が一人歩きする懸念もある。“想定”であれば、多少ニュートラル感がある。

○　“事故前提”では強いというイメージがあるというご意見があったという理解でよろしいか。そうであれば、あまり強いとは思っていなかったため、“事故前提”の方が良いと考える。一委員の意見として表明しておきたい。

○　“事故想定”でもよい、また、復旧や原因究明が必要だということも書いてあり、それについてはなんら異存はない。事故が起きた場合の被害を受けた人たちへの救済という記述が一切ない。トラブルに巻き込まれた場合、冷静に対応しようと政府に言われても困る。“救済”、“適切な救済措置が採られる”などといった言葉をどこかに入れておかなければ、いささか冷たい印象がある。

⇒“救済”ということについては、“犯罪の取締り及び権利利益の保護・救済”の部分があり、ここで内部的にも検討させていただきたい。

○　今の委員がおっしゃっている点は、例えばサブプライムの問題で、アメリカのセンスで言えば“自己の選択である”、ヨーロッパであれば“もう少し公的機関は介入すべき”というニュアンスであり、そのこととパラレルである。あれも、一種のセキュリティ問題だと思うが、どのような関与の仕方をするか、ある程度は書き込まなければならない。

○　ここに書かれていることは、“官も”、“民も”ということであろうと理解しているが、“人民”の話もある。政府が全て介入しろということではなく、“事故前提”或いは“想定”と、救済・補償はセットであると思っている。一方的に“事故前提”として、コンセンサスが得られた政府の出す報告書にあるからとして、「諦めてね」とすることは普通はないだろう。当たり前のことをどこかに入れておいた方がよい。

○　事業継続性確保や対応するときの活力を、民間をベースとして、自助的に、或いはコミ

ュニティベースで行うのか、それとも、ここでいろいろと議論された公的な法規をある程度意識するかで、対応が違ってくる。

○　個別の問題になると思う。銀行であれば契約であり、パソコンやソフトウェアであればトラブルが起きても責任はとれないと書くケースもあるだろう。ただし、例えば、住基ネットで漏れれば、被害を受けた人には一定の救済をすべきであろう。間違って逮捕されてしまった人には、補償などの対応をするなど、いずれにせよ対策、補償する手立てがあるだろう。全体を見ると、そのことが言及されていない。具体的に、どこまでどうやることを書けという要望ではなく、「諦めてね」と言っている結論を出したととられることが嫌だという趣旨である。

○　多少は意識して書いておられるように思うが、それが弱いという御指摘だと考える。「事故が有り得るから諦めて、事前予防のための対策を行わないとか、被害に遭うのは仕方がないことであると諦めるということを意味するものでは決してない」ということだけは書かれており、「だからどうだ」ということをもう少し、ポジティブな恰好で書ければよいのではないか。

⇒おっしゃるとおり、ややサプライヤーの側に立って書いているので、御指摘を踏まえ少し考えたい。個人情報の保護に際して、情報を預ける主体の問題になるが、それは被害者であり、情報が流出した企業もどのような形態かによって、被害者になる場合や加害者になる場合がある。必ずしも個人だけのものではないが、少し考えさせていただきたい。

○　弱者の問題と事故前提或いは想定の際の対応策についての記述で、ある程度言及する必要があるのではないかという意見がかなり出てきている。その対応は事務局の方で、お考え頂きたい。

○　記述について検討頂く際に考えていただければよいが、事故前提／想定社会で事故の中身について、例えば天災は防ぎようがないという意味では、想定の中に入れられなければならない。また、防止する側と、犯罪や故意に行うとするものの間のテクノロジーの差において、それも防止することは難しく、前提としなければならないかもしれない。人がその他のことで故意に行う、誤って実施してしまうことについては、事故が起こる前に対策として防ぐことは、どこかの水準に決めるというよりは、最大限努力してとどめるという合理性、それが合理性に裏付けられたアプローチということになる。事故前提とされている事故の原因なども、対象、その定義、意味合いを書かれた方がよいのではないか。

○　“事故前提社会”或いは“事故想定社会”という６文字の漢字をどうしても使わなけれ

ばならないかということも含めて御検討頂きたい。やはり、一般の方には耳慣れない言葉であり、ここではそれが何であるかという議論をしているが、この用語のままで行くのであれば、注にある記述ではなく、この言葉はこういったことを想定して使っているという定義付けを行っていただかなければ、かなり誤解を生じると思う。このような用語を使い、それへの“対応力の強化”という難しい表現を使わない方がよいのではないかと感じている。

○　個人について、先ほどから力強い個や救済ということについて議論されているが、基本的に個人は、消費者基本法で言っている個人を想定するのであれば、情報力や交渉力の格差にかんがみて、対応がとられるはずであり、その辺りを考慮した表現にして頂く必要がある。今回、何を指しているのか、その意味では消費者とは、消費者即ち自然人であるというような形で定義していないので、この部分も論議を呼ぶのではないかと感じている。

○　今述べていただいたのは、契約等での情報の非対称性を念頭において、保護も考える必要があるということだろう。“事故前提”或いは“事故想定”について、止めたほうがよいのではないかということについては、これまでかなり議論してきたことでもあり、コンセプトとして打ち出すことは、６月の段階で意見募集も行っている。他の委員からの意見が多ければ別であるが、リスクは様々なところに偏在しているということは認識していただかなければならない、その対応力をつけなければならないということが基本だと思われる。それは何とか活かす方向で、表現はまた検討したい。

○　先ほど、被害者救済に関する議論があった。例えば、個人消費者のカード情報がA社から盗まれ、A社で使われた場合に、それを補償することは分かる。A社で盗まれた情報を用いて、B社でサービスが使われた場合、これを救済しようとB社のサービス代金を無料にすれば、B社が被害者になってしまう。単純に物が買われた場合はよいが、サービスのような形が無いものが使われた場合、それを救済しろといわれてもB社が困る場合がある。小さい会社であれば、潰れてしまう可能性もある。A社が盗まれたにも関わらず、B社が使われたのでB社が悪いという世論になってはまずい。誰も証明ができず、どこから盗まれたか、もはや分からない可能性がある。使われたB社だけが妙にクローズアップされる可能性がある。こういった場合に体力のない会社は耐えられない。誰が被害者であるかは、非常に複雑に絡みあう問題であり、消費者を助ける観点だけではない。このような複雑な状況があるため、被害救済を明記するという単純な問題ではない。救済に向けての仕組みや方策について、検討を前向きに行うということを言っておかなければ、複雑なことになるのではないか。

○　今のご指摘は、サブプライムの問題などの構造と同じように、複雑化しているというこ

とである。誰がどういった形で責任をとるのか、複雑になっている。それに対応する仕組みをつくる、どのように対応していくか検討していくことを強調するということだと思う。

○　まだ、御意見があるかと思うが、これまでに有益な御意見を頂いた。何とかブラッシュアップし、この文章に活かさせて頂きたい。次回までに事務局に検討していただき、次回再度揉んで頂きたい。

**(2)政府機関・地方公共団体について**

○　政府においては、電子政府がＩＴに関するセキュリティを実装すべき部分である。電子政府との連携、その中へ融合的に入っていく、次期電子行政サービス基盤などといったものとの融合が２０１２年の姿としてあった方がよい。それを具体化するものとして、情報セキュリティ対策推進会議等の設置などが示されており、電子政府側としてはＣＩＯ連絡会議があるため、そことの連携などがある。行政管理局との組織としての連携は述べられているが、施策としても連携するとした方が、具体的に動いていただけるのではないか。

○ 事業継続性確保については、防災会議等を含めた広い範囲で、そういったものとの関連性について、一言、二言、言及した方がよいのではないか。

○ 特別管理機密に関する部分については、検討中とのことであるが、意見は次回の方がよいか。特にこの部分に現段階で意見があるわけではないが、その他の検討中の部分を含めてである。

⇒ 特別管理機密に関する部分については、政府内で調整をしており、最終案を提示する形になると考えている。意思決定をする部門が多岐にわたり、事務局の一任という形でお願いできればと考えている。

○ 特別管理機密の部分については、おっしゃる通りだと理解している。電子政府に関しては検討中のものは殆どないが、他の検討中の部分については、次回に意見提示ということでよろしいと思う。

○ 電子政府については、ＩＴ担当室とＮＩＳＣが検討を進めており、どう書くか難しいところもあるだろうと思う。日本政府は電子政府を進めると言っており、情報セキュリティは必須であり、うまく文章の中に入れられるものは、入れていただきたい。また、電子自治体も進むため、そことの関連で、情報セキュリティは求められる。勝手に記述しては困るということもあるだろうが、何らかの形で盛りこんでおく必要はあるかと思う。

○　政府における人材の育成・確保について、どの程度の規模の人数になると考えればよいか。

○　利便性については、可能であれば、ユーザにとってはある程度共通しているようにといったニュアンスがあった方がよいのではないか。政府の情報システムを整備しても使われないという、国民からの批判を受けているという現状もある。各省庁からサービスを受ける際のセキュリティについて、ある省庁はこのやり方、このカードでということで、一つ一つは最適化されていても、全体としては１０枚も２０枚もカードを持っていくということが起きかねないという若干の不安を持っている。統一できるものは統一するというニュアンスは持たせたい。

⇒　専門的な人材の確保については、民間の方の活用をいかに行うかについて全体的に進めていかなければ、難しいと考えている。政府全体で必要な人材がどの程度かということについては、もう少し検証をしなければ分からない部分がある。政府全体のガバナンスを考えていくという中で、省内の様々なシステム部門があり、人材が分散しており、仮にそういったものを上手く整理していくことができれば、必要な人材の確保が図られるのではないかなど、いろいろと検証していかなければならない部分がある。その中で、予算もそうだが、どの程度の人が必要かということについては、しっかりとした統制構造がある中で、うまく回していけないかということは考えてまいりたい。

利便性についてはおっしゃるとおりで、それぞれの役所がいろいろなシステムを作って良いとは全く思っておらず、共通化出来る部分があれば、今、政府全体として最適化が府省共通化でシステムに関して進められているが、そういった中でセキュリティに係る部分をどうやるか認証に係る部分をどうやるかを視野に入れて検討していきたい。

○　電子政府関係ではセキュリティカードのことなどを懸念されると思うが、財務省の主計局はかなり厳しくチェックしているので、勝手にいろいろな考えを通さないように雰囲気がある。電子政府に係るシステムだが文部科学省の６３６手続きのシステムを停止することを決定した。４件の申請しかなかったという防衛省の申請システムも停止させることに決定、国土交通省のワンストップサービスも抜本的に関係機関が集まって協議し、ビジネスモデルを考え直すこととなった状況である。

○　実際にユーザビリティから考えると、例えば、ワンタイムログインなど、基本的なインフラストラクチャの統一性がないと電子政府の利便性は上がらない。非常に皮肉なことを言えば各省庁バラバラに作っているのでその分だけセキュリティが保たれるということがあるかと思うが利便性をとるにはどうするかという観点がないと、セキュリティを確保す

ると同時に、やりようによっては利便性を上げられる。電子政府の会議ではそのような動きがでているようだが、我々の会議でもユーザの利便性も考えながらそういったことを考えるべきである。

○　電子政府全体としてのセキュリティのグランドデザインをしなければならないのではないか。そういう意味では、電子政府という観点での連携等の話はあるが、その中でセキュリティの立場としてもグランドデザインを築きながら、横連携など極力少ない認証方法でいろいろなところに行けるような全体のグランドデザインをかかなければいけないと思っている。日本全体として、社会インフラとしてのセキュリティグランドデザインはどうなのだという話までいければ良いと思っている。まさにそこと連携しながら、考えていかなければならないと思う。

⇒　ご指摘のとおり電子政府は各省バラバラで使い勝手が悪いと悪評であり、それを踏まえ、先月来、ＩＴ室とＮＩＳＣで電子政府ガイドライン作成検討会というものを開催しており、画面の作り込み、セキュリティの観点でなるべく各省共通の使い勝手の良いシステムを作っていこうという検討を進めているところである。方向性が見えたところでご報告したいと考えている。

○　ここで書き込む際に、どのように書き込むかは、委員からご指摘をいただいたようにグランドデザインが必要ということであれば、抽象的な書き方になるかもしれないが、ここで構想すべきということは言ってもよいかもしれない。

⇒ご意見を踏まえ整理したい。システム構築にあたっては、利便性・柔軟性の実現、セキュリティの確保など、いろいろなベクトルをより高い次元で妥協させていく、どちらかに妥協するのではなく、より高次で妥協する方向に持っていきたいと思っており、文章を整理し、わかり易くさせていきたい。

○　今の電子政府の計画では、電子申請等の利用率を高めるということが政府目標になっていると理解している。ＩＴに対する国民や政府の依存度が高まっていくため、それに比例してセキュリティも強化しなければならないという観点で、重要インフラでも全く同じだと思う。従来よりもＩＴへの依存度が高まっていることに対してバランスをとり、セキュリティをより強固にするというトーンが必要ではないか。政府機関だけの議論をしているが、重要インフラで書かれている文章と、政府や地方公共団体で書かれている文章を横並びでみると、政府のサービスは重要インフラの一部としては挙げていないが、最たるものだと思われるため、政府も重要インフラと同程度はやらなくてはならないというニュアンスをどこかに記載すべきではないか。

⇒ロジックとしてはわかるが、重要インフラについては業法で縛っているため、重要インフラの自主性というところで、やれるところはやると書いている。本来であれば、政府はもっとやるように書きたい。

○　政府は自らの取組みであるので、重要インフラよりも弱い取組みの文章ではバランスが悪い気がする。

○　これまでの議論ではあまり違和感はなかったが、“ＰＤＣＡサイクルの強化”というサブタイトルであり、サイクルは循環であるが、内容は“ＰＤＣＡのプロセスマネージメントの強化”に思えるが、どちらなのか。

⇒違和感があると言われるとそのような気もする。我々の趣旨としては、ＰＤＣＡを回している仕組みを今後作っていかなければならないということであり、ご指摘を踏まえ検討させていただきたい。

○　２０１２年の姿というタイトルの割にはそうなっていないように思う。“なっていること”と“この３年間にやらんとすること”と“３年間を含め第２次計画全体でやろうとしている試み”が切り分けられていないように思う。

⇒政府機関について、いきなり２０１２年の姿を書くよりは、将来的な to-be モデルを冒頭で書いた上で、２０１２年においてはこの辺までやって欲しいということで“何々をしている”ということがいくつか書かれている。これは、そういう状態にもっていくためには、具体的にどのような対策が必要になるのかは重点施策として書き込む整理をしているところである。

⇒２０１２年の姿は何に使われるかということであるが、政策会議の有識者構成員から言われていることは、対象が結果としてどうなっているかというアウトカムと、実際の政策群のアウトプットがどのように反映されるかということをわかるようにして欲しいという意見があったため、このような書きぶりになっている。企業の部分が典型的な書き方であり、“姿となっている”までが、結果として企業がこうなっているというアウトカムである。次に、ある政策群によってアウトプットはどうなったのかということを書くという形で、アウトプットとアウトカムを並べた構造になっている。政府の部分は具体の手が多いため、アウトプットのボリュームが増えるかもしれない。逆に地方公共団体は具体的なアウトプットが書けないといったような、いろいろな制約の中で同じ平仄、同じ構造で書いていこうとした結果である。具体的にアウトカムパートをどう書くかという御意見をい

ただければ、結果として政策評価インデックスとして使われるため、何を視点として記述せよと言っていただければありがたい。

○　政府機関については、他の部分の書きぶりと若干違う気がする。

⇒　政府機関部分の記述はいきなりアウトカムがあるのでもう一度考えさせていただきたい。

**(3)重要インフラについて**

○　“ＩＴ障害に関する情報共有の価値の普遍化”についてであるが、２０１２年のあるべき姿、“情報共有体制の強化”が書かれているが、体制強化するためにしなければならないことはわかっていると思うので、具体的に記載したほうが良い。例えば情報提供者側はＩＴ障害を隠すべきものではないと記載れているが、積極的、能動的に情報提供していくなどの仕組みを作るとか、実際に提供された情報をうまく運用していく仕組みが必要になってくると思う。情報収集者側もどのような義務、権限を与えるかといった部分も含め、情報共有の価値の普遍化、本格運用についての整備まで記載したほうが良いと思う。

○　次世代電子政府グランドデザインについても、今、委員がおっしゃっていた内容まで記述し、ＩＴサービスを普及させ、電子政府もそれに乗っていきたいということだと思う。個人情報も全てトレースするが、本人がチェックできる体制を作るということだと思う。ある程度そういうことまで書き込むほうが、リアリティがあるのではないかと思う。

⇒　重要インフラについては行動計画の中で詳しく書いており、具体的な情報共有の仕組み、例えば、各事業者の方からの所管省庁を通じたＮＩＳＣへの情報提供、ＮＩＳＣからの情報提供など、関係機関の間で情報共有する枠組みを作っており、基本計画の中ではそこまで言及していないため、具体的にどうするのかというところが分かりにくいのかと思う。現行動計画と次期行動計画で行うことを踏まえると、普遍化しておりわかり易いかと思うが、ご指摘を受けて、書き方については考えたいと思う。

○　委員がおっしゃったように、ある程度書き込んでもよいのではないか。

○　具体的にシステムそのものをどうするのかなどの記述が一つもなく、技術的な対応の話も一つもない。情報共有と演習だけをやって、このような２０１２年の姿になるのか。第１次計画から第２次計画に渡るなかで社会情勢は非常に変化しており、重要インフラ事業者のシステムも複雑化している。重要インフラ事業者同士が連携をし始めている中で、単

に情報共有する、共同の分析や演習をするなどで対応できることは限られており、もっと技術的・科学的に取組んでいけばたくさんあると思う。それについて行動計画に書いてあれば良いがそうではないのではないか。

⇒　ここは、必ずしも２０１２年の姿を書いているわけではなく、将来の理想とする姿を書いているところがある。そもそも行動計画は重要インフラ事業者の自主的な取組みでやっていただいているところがあり、そこまでやらなくてはいけないという義務を科す形になるのは好ましくないということもあるため、将来の夢のようなことを書いているところがある。例えば、セプターカウンシルはまだ準備会をやっている段階で、カウンシル自体もできていない。あまり過度なことを言うと入ってくれるかどうかも心配であり、直ぐにできるのか、具体的な手順はどうなのかということについて言うと、第２次行動計画をやって２０１２年にこうなっているというよりは、このような姿を目指して体制を作ることや、情報共有をしていくことを各事業者が努力して欲しいという趣旨で書いていると御理解いただきたい。

○　企業でさえＩＰｖ６への移行を図るといったことや、若い人材を育てるといったことなど、具体的に書いてある。一般企業に対してそういったことが要請される、或いは期待されているにもかかわらず、重要インフラのところだけがサラサラっと書いてあり、そんなことですむのか。

⇒　基本計画の中に入るのはエッセンスだけであり、具体的にどのようにやっていくのか、どのように検証してくのかは行動計画をご覧いただければと思う。行動計画には、基本計画に記載した内容だけではなく、国際関係やリスクコミュニケーション、人的な部分も記載されている。

⇒　第一に、第２次行動計画の素案の取りまとめが委員には見せられる状況に近づいているため、みていただきたいと思う。第二に、各事業分野の中でのインフラの変化とそれに対する技術的対応は、現状では基本的に業法の中でみていくということがあり、内閣官房で取りまとめている重要インフラ関係の行動計画というのは、あくまでも屋上屋を作るものではなく、各業法は尊重し、その運用は所管官庁がやっているということが前提としてある。したがって、この部分を加味して、その上で安全基準の指針で全体のレベルバランスをとるための方針を一緒にやっていこうということがある。そういった意味で技術的・科学的アプローチがもっと必要だということは、業法と行動計画とのあわせ技で見て頂きたい。行動計画だけをみても、共通脅威分析は科学的・技術的アプローチでと考えているが、それ以外は業法に依存する部分が多くあるということは御理解いただきたい。第三に、分野間で連携する演習については、個別機能ベース、或いは個別リスクベースでやっているが、本当は総合的なストリートワイドエクサ

サイズというレベルまで辿り着かなければと言われている。それは、今後３年間の計画の中で、演習の行動化という中で読んでいこうというところがあるが、事業者側からするとストリートワイドエクササイズまで辿り着ける自信はどこにもなく、今回の演習も、その辺はトライアルしようとしており、高度化はこれからの中で吸収したい。この３点がお伝えしなくてはならないところだと思っている。それ以上に、もっと情報をかき集めて誰かが解析すべきだ、或いは情報提供は、官からではなく民側から集めて解析しようという意見も無いわけではない。現状として、民側から政府が情報を集めることは大変抵抗感が強く、これに対しては、重要インフラ事業者及び所管官庁も非常に大きな懸念が出されている。そういった意味でも民側からは業法に基づく情報提供、官側からは資する情報提供というアンバランスで、同じような構造になっていないが、そういったところで努力をしている。

○　重要インフラにおけるＩＴ障害が国民生活や社会経済活動に重大な影響を及ぼさないようにとあるが、他の章では情報セキュリティに対する対策などの言い方をしているが、ここだけ“ＩＴ障害”と限定した言い方なっているおり、もっと広く“情報セキュリティ事故”などの表現のほうがうまく当てはまるような気がする。何か使い分けをしているのか。

⇒ＩＴ障害という言葉は、本委員会や重要インフラ専門委員会のなかでも議論していただいたが、ＩＴ障害はサービスに支障が出るような障害のうち、ＩＴの機能が起こすものと定義している。つまり、重要インフラはサービスを国民や事業者に対して提供するものであり、それについてＩＴに不具合が生じサービスが止まることがないよう対策を行うことが基本であり、ＩＴ障害を限りなくゼロにするに越したことはないが、ＩＴ障害が起きてしまい、それによって国民生活や社会経済活動に重大な影響を及ぼさないことを一番の目標としている。そうならないようにする対策が情報セキュリティ対策である。

○　例えば、犯罪的行為によって情報が盗まれるといったことは含まないという意味合いを込めているのか。

⇒　重要インフラのこの部分は、第１次行動計画からの流れがある中で、原因は何であれ、結果がＩＴを触媒にするのか、具体的なエンティティにするのかはわからないが、それにより重要インフラサービスに影響が出て重大な影響を起こしてしまうことを防がなければいけないということである。原因スペシフィックに書いているのではなく、結果スペシフィックに書いている。従って、ＩＴ障害が起きる原因が意図的であろうが、非意図的であろうが、オペレーションミスであろうが、自然災害であろうが、なんであろうが含んでみている。したがって、このＩＴ障害は、原因を書いているというよりも、結果としてＩＴコンポーネントが障害を起こし、サービスに影響を及ぼす状況を避けるための行動計画という書き方である。

○　一般的に、そのような言葉の使い方をするのかわからないが、外部的な要因によって使えなくなるような状況もＩＴ障害と呼ぶのか。犯罪行為等も含めているという理解でよろしいか。

⇒　そうである。ＩＴ障害という言葉が混乱の原因になっているのも事実であり、第１次行動計画の頃はＩＴ障害といっても誰も使わなかったが、最近は一般用語化しているので第２次行動計画の中では定義を記述する形になっている。

○　ＩＴ事業者の中では、ＩＴ障害というとＩＴシステムの内在的な故障などによって動作しないことについて言うことが多い気がする。もっと広い意味合いで使われるのであれば、わかるような形で書いていただきたい。

⇒そこは注意して、検討する。

○　「行動計画」と「基本計画」の関係性や違いが分かっていて、かつ、重要インフラの部分はカセッタブルに基本計画に組み込まれる、など私自身がこの場で学習して分かったことを、これを読む人が全員分かる筈がない。従って、行動計画内から、主な内容をプラスアルファとして引いてくると共に、「基本計画とは別に行動計画というものがあり、それにより詳しく書いてある」とリンクを付けることが適当である。行動計画にはクリアな定義が記載されているので、エッセンスを脚注等で引き継げば、両者の関係性を巡る混乱はだいぶ収まるとは思う。その上でこの基本計画全体として、同じ事象をＩＴ障害と呼んだり、情報セキュリティ事故と呼んだりしているところがあれば、チェックし、調整することが必要と思う。

○　監督官庁があり、業法があり、そこで検討しているのだから責任はそこがとるとはっきり書いたほうがよいのではないか。行動計画がそのような書き方になっているのであれば、一見、基本計画で取りまとまっているように見えて、実はしり抜けになっている。基本計画だけを読む人は、結局そのような印象になり、不安が残ることはまずいと思う。

⇒読み方と書き方は工夫する。ただし、所管官庁が責任を持つというところは考えさせて欲しい。

⇒ご指摘のあった趣旨は、行動計画の中では、業法と呼ばれる当該分野に属する事業を営む者を規律する法制度の枠組みに加え、それとの整合を図りつつ、各重要インフラ事業者との自主的な取組みを充実することが求められる。そのためこのような行動計画を作成

したとあり、そのような趣旨を書くことも一つの方法かと思う。

○　そもそも業法が成立した時期に、これほど情報システムやＩＴの重要性やネットワークはなかった。業法自体がそのようなことまで考慮して作られているのかということ自体が検討されないまま、それぞれで検討しているから大丈夫だと言われても、実態としては非常に不安である。しかも、最近起きているトラブルはみな、そのようなことに絡んでおり、かつ、重要インフラ事業者の情報システムはみな古く、現代の新しいテクノロジーにキャッチアップできていない会社が多くある。本当は再構築等しなければならないが、やられていないケースが非常に多いので、もう少し真剣に考える必要があると思う。

⇒ご指摘の件は、懸念としてもっともだと思う。元々の計画については、まず重要インフラ企業と所管官庁というものがあり、その枠組みの中でシステムをキャッチアップできるか、そのリスクを追いかけられるかということに関しては、法律の構造も事業分野ごとに異なっており、その中での法律のターゲットとしているものと、実際の国民生活の関係で言うと、表現が違うところがある、或いはシステムが古いところもある。内閣官房としては、各所管官庁において、これらに関しての努力はきちんとやって欲しいという調整権能を発揮することが、まず第一歩であると考えている。これが十分になされているかは、今後の各省庁の取組みの、それぞれの法律及び運用に係わるところでの政策評価、或いは法律体系の中での評価に委ねられているところがある。その先に、連携や、繋がっている、依存している、或いは一緒にレベル感をあわせなければならないといったことに関して、更にプラスアルファの部分がある。この部分は、行動計画により、なんとか事業者と所管官庁の調整ができているということが現実である。従って、内閣官房が取りまとめているこの計画の中でできているものは、委員が１００％満足するものではなく、かつ、分散的な責任構造になっているのも事実であり、今の重要インフラ事業者にかけられている規制の中で、技術要件、或いはシステムに対する要件が、少なくとも所管法の中、或いは所管法に関わる政令等の中で決まっており、この上にアドオンされる構造でしか組みようが無いところでやっているということを御理解いただきたい。当然、アドオンしているため、各事業者や所管官庁が、システムが古いなどの問題をみていないわけではない。具体的に言えば、多くの事業分野がある水道やガスでは、中小の事業者が古いシステムを使っていることに対してのリスクをどのようにみていくかについて、所管官庁が努力している領域でもある。また、カバレージが所管法にないところがあり、例えば、航空旅客については、予約発券システムは業法の外であるが、常に事業協会を含めて、今回の計画の中では一緒にやっていこうということをみている。その意味では業法だけに任せているわけではなく、それぞれが自主的に努力をし、業法の外のシステムも改善していこうというように動いてきている。

### (4)企業・個人について

○　政府機関の部分では、設計段階からきちんとやることによってＴＣＯ削減に繋がるということが書かれており、一般企業についても、これ以上セキュリティにお金を使えないほど使っており、更に使うのかというところもある。企業の部分にも、後付けのセキュリティばかりではなく、最初からやって欲しいため、設計段階からのセキュリティによるＴＣＯ削減ということは、明示的にうたうべきだと思う。

⇒この重点施策は具体的な施策に落とせるかどうかということがあるので、各省とも相談してみる。政府は自分のことなので、やると決めればできるが、企業はガイダンスかガイドライン等の施策で強制力がなく、できるかどうかわからい。

○　そういう意味では、企業がこれをやりなさいではなく、対策支援主体、情報セキュリティ業界やＳＩ業界として、こういうものを推進すべきだということである。今のビジネスモデルの構造からすると穴だらけの物を納めたとしてもセキュリティの問題はバグではないので、そのお金は払いたくない、或いはエンドユーザの方もセキュリティ付きにすると値段も上がるので、無理な用件定義をしたくないというところでデッドロックに入っているため、やはり、情報セキュリティ業界やＳＩ業界がＴＣＯ削減に向けて企業にサービスを自ら考えて提供すべきであるという趣旨である。

⇒施策としてどのようにできるか検討させていただきたい。

○　企業について、規範というか、何をやればよいか不明であることが原因で、うまくセキュリティ対策が進まないとあるが、どの程度コストが掛けられるのかという財政的なことについて書かれていない。そういったことが原因でセキュリティ対策が進んでいないとすれば、その２つについて対応していただかなければならない。規範の存在がないということについては、関連法制との関係を整理し、ガイダンスとして整備するとあるが、ガイダンスという位置づけではまだ不足であり、自らが進んでやらなければならないが、企業はもう少し強制的な対応、取組みを推進しなければならない。そういったことがなければ、難しいのではないか。財政的基盤がないために、セキュリティ対策をやりたくてもできないのではないか。中小企業については、セキュリティ対策が十分にできない理由として、認識不足及びリソース不足とあり、リソースとは人の問題と読み取ったが、中小企業に限らず大企業でもお金をどれだけかければよいのか、或いはかけたい時にかけられないということがあるとすれば、コストに対する援助、具体的に言うならば補助金であるとか、対象としてセキュリティ対策コスト、研修のコスト、監査のコストなどを含めた税務上の所得控除等、財政的な支援策を政策として盛り込む、またその端緒となる記述を盛り込んで

いただければと思う。

⇒「ガイダンスの整備」については、関連法制でどのような要求がされているのかを分析し、それぞれの法目的に沿った要請について、整合性のある形でガイダンスしていきたいという趣旨である。リソースについては、人間の問題だけではなく、当然お金の問題も入っており、補助金や税制対応については既にあるものもある。今できることを検討し記載しているが、他にできることがあるか再度検討する。これで不十分ということであっても、財政的な制約もあり容易には書けないことは御理解いただきたい。

○　企業の２０１２年の姿について、当面のゴールについての記載がない。具体的な施策でも、ＩＳＭＳをやろう、セキュリティ評価や認証をやろうとはあるが、基本的に企業として何をどこまでやればよいのかを示さなければ、企業は推進できない。それを国が出すということはできないと思う。それぞれの企業や業種、業態がもっている、最高のやるべき情報セキュリティ対策を出し、そこではこういったリスクが残っているということを世に問う仕組み、それが世にそぐわないようになれば、それがスパイラルアップしていくような仕組み、コンセンサスを形成できるような仕組みを作る、支援するような施策をとるべきではないか。つまり、各業態や業種での情報セキュリティ対策のモデル等をできるだけ出していくようなことをすべきではないか。

⇒おっしゃる趣旨はわかるが、企業も個人と同様にいろいろな企業があるので、例えばＳａａＳやＡＳＰの業態の場合にはこういう基準であるということはあり得るだろうが、業種･業態いろいろなものを考えてあるべき姿を支援するのは厳しいのではないかと思う。部分的にある種の業界を想定してやるのは可能かもしれない。関係省庁と話をして、どの程度のことができるか、あるいはできないのか検討させていただく。

○　例えば、医療情報であればレセプトを扱っている業界があるのだから、そこで自ら律するような基準を作っていけばよいのではないかと思う。そういった基準を作っていきなさいということを支援するような施策はとれるのではないか。全てを包含した横断的なものをやれということを言っているわけではない。

⇒どのような基準が存在するかということについて、２つ注意しなければならないところがあると思う。例として出たレセプトや電子カルテの問題は業界が既に取り組んでおり、しかもいくつかのステークホルダーが関係して得られているものも出てきており、そういったところの存在に関しては関係省庁がやっているケースもあるため、一体何をやっているのかということに対しての調査はできないことはない。その先のレベル合わせと支援に関しては、政府としては非常に入りにくい。経産省が、一般的な企業体に対してガイドラ

イン的なものを提供しており、それで読むのが精一杯ではないかと思う。したがって、取組みについて、どういうことが起きているのかを調べに行くのはできるだろうが、政府としてこれがベストプラクティスである、最小限やるべきものであるなど、そういったエンドースについてはできることとできないことがあり、その境界線を踏み越えるは、企業の自由経営やマーケットの自由化等の関係も含めて、やれないことも結構あるのではないかと直感的に思う。

○　政府が踏み込んでまでベストプラクティスを出せとまでは言っていない。その業界、業種、例えばＩＴ産業におけるＩＴ開発の受託関係、サプライチェーンなどの中で、自分で自らを律して、責任関係、情報セキュリティに関する取扱い保護などは決めていきなさいといった指導、支援をしていくということである。できあがったものを、良いか悪いか政府が判断するということではない。その判断は、ステークホルダー、受益者が行うべきである。

⇒　応援ということではないと思うが、その先に何か具体はあるか。

○　開発や受託に関しては、そういったものを同意してやりなさいということである。それを作れということが支援だと思うが、それが指導であれば指導でもよい。中小企業の受託関係になると、あまりにも重い対策を求められたり、逆にザルになる対策を求められたりということが、往々にしてある。

⇒　例えば、経産省が行っている契約のテンプレーティングのようなもので、情報産業の下請けのようなところで、非対称型の契約を是正するために、契約書のテンプレートを提示し、皆さんに使っていただくといったソフトな仕組みがあるが、それでは足りないということか。

○　不足である。それを実現するために何をすればよいかというところまで、踏み込まなければ、非対称の片側にいる力の弱い方は無理だろう。

⇒　世の中の実態と、現状の施策のどこに隙間・差分があるのか議論するには時間がかかるため、別途議論させていただきたい。経済産業省に関連する施策がいくつか存在し、その先にあるものを言われていると思うので、調整しどのように記述するか考えさせていただきたい。

○　“情報セキュリティガバナンスが経営の一環としての位置付けを確保するためには、関連法制との関係で整理が必要となる論点”とは具体的に何を言っているのかよくわからな

い。Ｊ－ＳＯＸ法では情報セキュリティのガバナンスというところまで、法律上想定しているとは思えない。“関連法制度の分析整理を行い、ガイダンスとして整備するような取組みも推進する”とあるが、これも具体的に何を言っているのかよくわからない。Ｊ－ＳＯＸのことを述べるのであれば、情報セキュリティガバナンスとは概念的に合わない。

⇒Ｊ－ＳＯＸも含め、その他、例えば、セキュリティを取り巻く関連法制は、労働分野等含めいろいろとある。セキュリティの専門家の方々は技術等には詳しいが、法律でこういったことはやって良いや、或いは裁判の論点になり得るのかといったことについては、なかなかご理解いただいていないため、そういったところを網羅的に整理することによって、情報セキュリティの対策がより法律に則って進むことができるということを取りまとめる施策である。

○　情報セキュリティとの関係で関連法制との整合性を保つ企業にはいろいろな提案をしていこうということであればわかるが、“情報セキュリティガバナンスが経営の一環としての位置付けを確保する”という意味での関連法制とは何か。

⇒ガバナンスの中には、遵法や法律に従った形での企業運営も求められているところであり、コンプライアンスの関係でも法律にのっとって対策がなされるかどうかが大きな課題であると考える。ガバナンスによって企業でこのようなセキュリティがなされているということが企業活動に繋がるという際に、情報セキュリティからやや遠いと思われる法令に抵触しているかどうかを整理することによって、セキュリティ上問題がないことを説明できると考えている。

⇒ここはおそらく、産構審での議論がベースとなっている。情報セキュリティガバナンスというのは経産省の方でどのように考えているのかというと、情報セキュリティ対策を実施する、或いは情報セキュリティそのものを円滑に行うために経営者の方針判断が必要になるケースが出てくる。また、法令遵守に基づいて考えていく際に、実際の法律の存在と、企業で働く法律の実務者の間で方針が見えてこないところ、混乱するところや、既に問題が指摘されているが、それに対して是正できていないところがある。具体的には金商法、労働基準法、派遣労働者に係わる管理の法律、賃金支払適正化法、不当競争防止法、独占禁止法などで、企業の経営者が判断する、或いは保全のためにどのような契約を結んでいくのかということを判断できない。法の実務者に聞いても混乱をきたしているところがある。法律を改正するということに対する方向性は、政府の側に無いわけではない。現在ではいろいろな法律が存在しており、法の実務者が混乱しているところをどのように判断すれば良いかは、企業における法の実務者と経営者にも、このような問題があることを啓発していくこと、これをガイダンスのような形で整備し、提供してくという施策が昨年

ぐらいから少しずつ動いる。ただ、法律が他省庁にも関わっているため、作業が難航しているが、より具体的な法律の整理が必要になれば、関係省庁に対して働きかけをしていくということがこの取組みだと思う。

○　この情報セキュリティガバナンスは、政府機関における情報セキュリティガバナンスと同じ意味なのか。

⇒ここでのガバナンスとは違い、政府機関における情報セキュリティガバナンスはより強い内部統制の話になる。一方、ここでのガバナンスは企業経営等の話になると思う

○　違いが分かるような記載にしていただきたい。

○　“事業規模を問わない適切な対策の進展”という記述は、事業規模を問わず同じような対策をすると読めるので、“問わない”という言葉を変えたほうがよいのではないか。個人に関するところだが、“情報を預ける側の主体が気付かない間に安全が図られる技術的発展の実現”とあるが“気付くべき”だが“気付かない”ということもあるため、“意識しない”などに変えたほうがよいのではないか。企業について、情報セキュリティ対策レベルの評価を政府調達の入札条件の一つとするとあるが、これだと評価の条件だけになりそうなので、総合評価方式の加点ということも明示的に検討として入れていただきたい。

⇒総合評価方式の加点の部分に展開するには、法律が無い限りできない。今の会計法に基づくところに組み入れるには、法律を作るしかない。グリーン調達については、議員立法でできた。法律の専門家の方に伺った範囲では、加点方式において、セキュリティを金額に一定限度合理的な理由で算入するための法律がなければできないというのが現時点での認識であり、踏み込むのは大変難しいと理解している。

○　技術点の中にそういった趣旨の項目を入れることも不可能だということか。

⇒　技術的な要求基準として書くことはできる。具体的に書いてある総合評価の中へ入れていくことはできるが、抜本的にグリーン調達と同じように、例えば環境インパクト係数が少ない経営をしている企業、製品を持っている企業は点数を優遇するなど、そういった形での書き方はできない。提供される製品・サービスについて、客観的なデータに基づいたものであれば書ける。例えば、ある企業が提供する製品Aが、このような要件を満たしているので何点ということはできるが、その企業が情報セキュリティについてすばらしい行為をしているので何点分として算入することはできない。Pマークを持っていることを入札条件にはできるが、Pマークを持っているから何点という書き方は、一般的にでき

ない。Pマークが関わっているサービスを買う場合、それを０／１の条件にはできるが、幾ら分になりますということはできないと言われている。グリーン調達も同じ問題があり、それを突破するために議員立法で法律ができ、何点という読み換えを行った。そのような形にならない限り、PマークやＩＳＭＳ取得は０／１の条件としては書けるが、値段に関係する加点を幾らにすると書くことは大変難しいと聞いている。

○　マネジメントに対する技術評価というものもあってもよいのではないかと思っていた。完全に定量的なものではないが、何段階かのレベルでやっていたと思う。確認はしていないので、私の解釈が間違っているかもしれないが、そういったものも含めて無理だということか。

⇒確認させていただきたい。

○　個人について、“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、個人に危険性を認識して欲しい、無防備に使う人をゼロにするという取組みを個人に求めるのだとするのであれば、おかしいのではないか。

⇒ご指摘のとおり誤解を招く可能性があるので検討させていただきたい。

○　“一般利用者のセキュリティレベルを効果的に上げるために訪問対応を行えるサポーターの促進”とあるが、趣旨としては理解するが、訪問対応を装って詐欺のような犯罪に悪用されるのではないか。もう少し丁寧に書き込まなければ、悪用される不安がある。

⇒ご指摘を踏まえ検討させていただきたい。

○　“情報家電、ゲーム機がネットワークに接続され”とあるが、“情報家電”ではなく“情報端末”の方が個人には分かりやすいのではないか。

○　“児童・生徒や保護者への教育・啓発を推進する”とあるが、“教育・啓発を推進”ではなく“対応が求められる”等の方がよいのではないか。

○　“関係府省庁がより効果的に実施”とあるが、これだけでは重複やバラバラに実施することが想定されるので“関係府省庁が連携し効率的に”等とした方がよいのではないか

○　まだ、御意見あるかと思うので、事務局へメールでお寄せいただきたい。

**(5)情報セキュリティ技術戦略の推進、情報セキュリティ人材の育成・確保について**

○　技術戦略について、具体的な施策の中にテーマのようなものを入れなければ、２０１２年の姿との結びつきが見えなくなってきている。全体的に“合理性に裏付けられたアプローチ”が見えなくなってきている。フレームワークの中でテーマとして入れてはどうか。

○　“合理性に裏付けられたアプローチ”は繰り返し強調した方がよいのではないか。

⇒この領域は、ＮＩＳＣがみる領域になっているが、現実の政策実施のアームは、総合科学技術会議であり、ＮＩＳＣ側からは意見をインプットし、研究ファンドを持っている各省庁と、総合的にみていく総合科学技術会議に対し影響力を行使していくことになる。行政的な観点からいうと、中身に関しては総合科学技術会議のプロジェクトチームを含め基本戦略の審議会などが引っ張っているところになるので、２０１２年の姿に書かれているテーマは、そこへ向けてのインプット項目になる。行政手続きに対しては、中身はいざ知らず、こうしなければ駄目だということはＮＩＳＣとしては影響力が行使できる領域であろうということで総合科学技術会議と話しているため、手続き的なことが増えている。これ以上書けるかどうかは、総合科学技術会議の事務局と相談させていただきたい。具体的なテーマを設定するのは我々ではなく、こういったものがあればよいといったことで、影響力を行使している。我々がやれということは屋上屋を掲げる構造になるため、このような記述になっている。

○　３つ大きなテーマを挙げられているが、それに向けて何を追求するかは各個別に決められるという御説明かと思う。その意味では、“２０１２年の姿に向けて”という一言で終わってしまうかもしれないが、テーマに向けての方向性くらいは、２０１２年の姿に入れて下さいというお願いはしてもよいかと思う。個別の中身については理解した。

○　基本計画そのものの書き方であるが、２０１２年の姿に書かれている内容と受け方が違って、後半は政策的なことが書かれているのか。

⇒２０１２年の姿に書かれている内容を受けて施策を書いており、施策の立案と推進に関してはＮＩＳＣが総合調整を行い、政策会議をレポートのＴＯにするという構造にしている。しかし、政府の科学技術投資に関しては、総理議長の総合科学技術会議がヘッドクオーターになっている。ＮＩＳＣは研究開発費を持っておらず、また、総合科学技術会議の監督の下に入っていないので影響力を行使するしかない。影響力を行使するにしても、正面からは行使できないので、他機関と連携するというような書きぶりになっている。重点政策に書いてある事項については、総合科学技術会議の情報通信ＰＴの中で、内閣官房

からも申し入れはしているところである。多様性については新しく追加した領域であり、申し入れはまだだが、グランドチャレンジ型の研究開発や効率的な実施については、総合科学技術会議の情報通信ＰＴのフォローアップ等でこれらの表現は入っている。その中で、適切に実施するということで、これらをみながら各省庁は予算要求をしている。グランドチャレンジ型でやりたいという予算要求も文部科学省から出ていると聞いている。また、弾力的な構造で行うことも、経済産業省を含め出てきており、反映はされてきていると思っている。それを引き続き行っていきたい。追加された多様性を維持するという項目については、具体的には科研費は多様性をもった運用をしているが、多様性を維持できているかを含めて、情報通信ＰＴで検証する方法はないかという話もしている。

○　まだ、御意見があれば、事務局へメールでお寄せいただきたい。

**(6) 国際連携・強調の推進、犯罪の取締り及び権利利益の保護・救済について**

○　検挙件数が増えたことは事実であるが、犯罪が増えたかについては分からない。暗数があるはずである。犯罪の検挙件数の部分だけ具体的に書かれていることに違和感がある。“犯罪の手口についても高度化・多様化”とあるが、エビデンスがあるのかわからないため、非常に不可解に思う。不正アクセス禁止法によるセキュリティホール攻撃の検挙件数はこの２年間、ゼロである。また、海外では政府機関に対する攻撃が報告されているので、日本でもサイバーテロの驚異が現実のものとなる可能性があるというのも曖昧な評価で、気になる部分である。また、権利利益の保護・救済についての記載がないのではないか。これらについてご検討いただきたい。

○　サイバー犯罪等の“等”は何を含めているのか。“サイバー犯罪”と書かれている部分、“サイバー犯罪等”と書かれている部分の使いわけがよく見えない。また、ここに書かれていることは第１次基本計画からの内容的に進展がないイメージを持つ。第１次基本計画から踏み込んだところで何をしようとしているのか。２０１２年にこういった姿になっていると書かれているが、そこまで言い切れるのか、不思議に思う。

⇒“等”の表現については検討させていただきたい。権利利益の保護について記載していないのはご指摘のとおりなので、何が書けるかを含め関係省庁と調整させていただきたい。

○　権利利益の保護について、民事の関係については、国際関係等になるとＡＤＲをやれば第１次基本計画とだいぶ違うのではないか。ＡＤＲなど具体的な内容を書いていただければと思う。

○　インターネット利用者の半数以上が利用に関して不安を感じている状況にあるとあり、２０１２年の姿ではサイバー犯罪が増大し不安感を増大させる要因になっていると記載されているが、読み方によっては今より悪くなっている、社会不安が増大しているから、取り締まる側が強力にやると読める。２０１２年のあるべき姿として書くのであれば、きちんと対策をとって、インターネット利用に不安を感じさせないようにもってくるような記載にすべきではないか。重点施策の部分もインターネット利用に不安をもたないという書き込みが必要になってくる。

⇒検討させていただきたい。

○　最近の振り込め詐欺もそうだが、起きていることの説明や教育の側面がなければならないのではないか。起きている事象が認識されているとは限らないので、啓蒙活動のようなものがあって、尚かつ取締りを強化するとした方が良いのではないか。技術にも絡むが、銀行のシステムに対して、振り込め詐欺のパターン分析などを行い、防止する仕掛けを作り得た実績もある。サイバー犯罪について取締りを強化するのではなく、技術的・科学的に対処する方策を記述する必要があるのではないか。

⇒重点政策の項目に記載されているが、犯罪の被害状況や手口、具体的な対策の方法等についての啓発はするつもりである。技術についても、ごもっともな意見であるので関係者と相談し、どの程度書けるかを検討させていただきたい。

○　そもそもサイバー犯罪とは何を指しているのか。サイバー犯罪の定義が必要ではないか。

⇒サイバー犯罪として考えているものは、一つは不正アクセス禁止法違反の不正アクセス行為、もう一つは刑法上のコンピュータ等を対象とする犯罪、もう一つはネットワーク利用犯罪といわれているが、ネットワークを利用した詐欺等のインターネット利用する犯罪が含まれている。

○　振り込め詐欺はサイバー犯罪なのか。

⇒ネットワーク利用犯罪に関しては、定義で構成要件の一部としてネットワークを利用されたものが該当し、ネットワーク利用詐欺となる。電話で行うようなオレオレ詐欺の類は、大半の場合、ネットワーク利用詐欺に該当しないが、やり方次第ではネットワーク利用詐欺に該当する場合がある。

○　電話はネットワークではないのか。

⇒基本的には高度情報通信ネットワークと考えている。相手に対して金品等を出させる行為が構成要件になっており、その中で、ネットワークを利用しているかによって、ネットワーク利用犯罪として統計上の検挙件数として整理している。

○　ＡＴＭを使った犯罪はサイバー犯罪にはならないのか。

⇒例えば、電子計算機使用詐欺にあたるような形態であれば該当するのではないかと思うが、ＡＴＭを使えば全てサイバー犯罪になるとは限らない。

○　今のやりとりのような定義や分類等、文章だけでなく図表等をいれると読み易くなるのではないか。全体的にビジュアルにしていただけるようご検討いただきたい。

○　いろいろな形での情報通信社会における犯罪があり得るので、広い意味で含めるのであれば、サイバー犯罪ではなく“等”を付けた方がよいかもしれない。

○　仮に“等”を付けると何が入るのか。

○　情報通信やＡＴＭを使ったもの、クローズドなものも入るのではないか。

○　そうすると、ＡＴＭを使った振り込め詐欺等を防ぐための手だては、重要インフラである金融機関が自主的にやることになり、警察としてはサイバー空間として取り締まるつもりはないという理解でよいか。

⇒犯罪にあたる以上は、警察としては取り締まることになるし、その未然防止を行うは必要があると考えている。

○　構成要件など難しい問題があるかと思うが、それらをよく考えた記述にする必要がある。まだ、御意見があれば、事務局へメールでお寄せいただきたい。

**(9)政策の推進体制と持続的改善の構造について**

○　“国民生活審議会との関係においては、情報を提供する側の主体に係る取組みを進めるにあたって十分な連携を確保する必要がある”とはどういうことか。

⇒個人情報保護を主として念頭に置いている表現である。

○　国民生活審議会の情報保護部会があり、そちらで何をどのようにしていくかということを踏まえ、個人情報は何なのかという書きぶりの方が分かり易いのではないか。

⇒書きぶりを含め検討させていただきたい。

⇒書きぶりに関して、消費者行政関係についてどう書けばよいのか難しいところがある。基本的には個人情報保護であるが、消費者行政ともうまく連動してなければならないという認識は持っているので、調整できる範囲で検討させていただきたい。

○　事故、災害、攻撃とあるが、これは事故前提社会の“事故”を分解して書いているのだと思うが、ＩＴ障害も事故前提社会の“事故”に含まれるのだと思う。この言葉も含められるべきではないか。

⇒表現については、検討させていただきたい。

○　技術開発などに関して、産総研や関連機関が連携して行っているものを統合するといった議論があったと記憶している。米国のＮＩＳＴのようなものを、バーチャルでやるというような話があったが、どうなったのか。

⇒“関係団体などの研究者・実務家の知見を集合的に活用するための仕組みの構築を推進する”という箇所が相当する。

○　事務局側から、「事故前提社会」「事故想定社会」を今日できるだけフィックスしたいとのことである

⇒　一部のＩＴ関係者の中での議論では、「前提」では、いかにも事故があっても仕方がないと最初から諦めているようにとれるという意見もある。我々にはそのような趣旨はないが、そこで敢えて「想定」という新たな言葉を入れたということである。「想定」の方が、“事故は仕方がない”となりにくいのではないかということである。これは語感の問題であるので、「想定」でも同じだとか、「前提」で押し通して欲しいといった意見もあるだろう。我々としては、努力はするが１００％はできないという趣旨を入れたいと思っている。

○　語感で申し上げれば、「前提」では「社会」という言葉との繋がりが悪い気がする。「想定」になるともっと悪い印象がある。

○　「前提」も「想定」もそれほど変わらないのではないか。

⇒　「前提」を諦めていると感じる方のストレートな意見は、我々は前提としてやっていない、事故を起こす気はないというものである。ただし想定してないかと言えば、それは想定して頑張ってやっているという意見であり、「想定」には「万が一」というイメージがあるという声が大きい。

○　「私は事故を起こさない」と言っている人たちが、非現実的で、ＩＴやリスク管理の難しさについて分かっていないのではないか。

○　私は「想定」に一票入れたい。何故かというと、「前提」にしているというのはどうも居心地がわるい。「想定」というのは、何かの訓練のように、起こりえないけれど、こういう「想定」をしましょうというように、起きる「前提」とはあまり言わないのではないか。

○　私は「前提」に一票入れたい。「事故前提」というのはこういう意味だということを知らしめるように事務局ががんばれということで応援したいと思う。

○　政策会議で説明した際に、構成員からネットワーク社会は１００％セキュリティを万全にしなくければならいと言われたが、最悪の事態が確率的には起こりうることを仮定して行動しなければならないと思うので、そういうニュアンスをきちんと説明して使うということを繰り返しておく必要があるのではないか。したがって、今日の委員会では、何らかの概念は使った方がよいという意見が多数としたいと思う。

○　まだ、ご意見がある方は、事務局までお寄せ頂きたい。

**(10)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　－