資料２－１

情報セキュリティ政策会議　基本計画検討委員会
第２回会合議事要旨

１．日　時

平成 20 年２月 14 日（木）　15 時 00 分～18 時 00 分

２．場　所

内閣府本府　地下講堂

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
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
神保　謙　委員　慶應義塾大学総合政策学部専任講師
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) 基本計画策定に向けた、関係者ヒアリング①：日本弁護士連合会

日本弁護士連合会から、資料４に沿って説明がなされた後、下記内容の討議が行われた。

○　今回、日弁連の過去からの取り組みを初めて伺ったが、「国家による民間規制反対」、「リスクマネジメントであってコンプラでない」「全分野横断的な基準反対」などのご意見について、共感を覚える。特に「第三者監査機関を作るべき」との主張については、有効な具体策と考える。

○　「先ずは何のためのセキュリティか議論した方が良い」という意見については、正論だとは思うが、組織や人によって立場や意見が異なることを考慮すると、これを議論して全員が納得する一つの結論を導くことは、実質不可能ではないかと思う。「多様な考え方の中でどこまでを共通の認識として認め合うのか」といった問題設定にした方が良いのではないか。

→　委員指摘のとおり、実際、世界のプライバシー保護の考え方を見ると、国によって相当な開きがある。その「開き」を認識した上で、日本はどの辺りかを考えた方が良いと考える。どこの国と同じような感覚のプライバシー保護のあり方か、何となくでもある程度イメージしておいた方が、問題が起こったときに「これはプライバシーとして保護するものではない。」あるいは「プライバシーとして保護すべきものであり、こうしなければいけないと思う。」という説明が、割と迅速に出来ると思う。問題が起こったときに、議論していて対策がなかなか立てられないというのは良くないので、あらかじめ一定の議論をしておいた方が良い。また、考え方により、どこにどれだけ予算をかけるかというのが違ってくるので、「こういう目的があるので、ここに予算を使います。」という議論にもつながると思う。

→　情報の取扱いに関する本人の同意について議論しているが、かなりセンシティブな情報であっても個人の同意なしに扱わざるを得ないこともあれば、簡単な問題であっても本人の了解を得た方がよいというような場合もある。そこには、個人の自己決定権やプライバシーの考え方が根本的にあるので、一旦議論で決まってしまうと動かせないものという意味ではなく、流動的であっても構わないとは思っている。

○　情報通信技術が発達していない段階での制度・規制の枠組みを考えれば、こういう議論をしていても良いが、技術進歩が早い分野であるので、技術に関する議論を取り入れながら考えていかないと間に合わないのではと感じている。

○　これだけ情報通信技術が発達すると、今まで人類がほとんど対応したことがないような事態が発生している。情報の伝搬送量だけをみても、10 年前・20 年前には想像できなかった速度・分量で伝搬している。そのような状況において、今までの法制度や規制の制度にない、新しい枠組みを考える必要があるのではないかとの印象を受けている。

○　情報セキュリティ基本法について、資料中、「必要」と主張している部分と「不要」と主張している部分があるが、結局のところどちらなのか。

→　ここに提示した「情報セキュリティ基本法」の案文は、2002 年の段階で、その当時の状況を考えて作成したものである。そのため、全ての事項が今日的なものに対応しているか再度検討の余地はあるが、特別基本的な内容と、監査制度をつくるということが、基本法案の概要であると考えている。

→　「情報セキュリティ基本法」の案文を具体的に提案した後の状況を言うと、例えば、個人情報保護法のなかで「個人情報取扱事業者」について罰則を強化すべきではないかとの議論が与党からでたが、そのときには、特にプライバシーの保護のため、個人情報保護法のなかで今直ちに個人情報取扱事業者への罰則を適用することは必要ないという意見をまとめている。すなわち、「情報セキュリティ基本法」は作って欲しいが、罰則を全分野横断的にかけることは問題があるだろうと現在認識しており、具体的案文としては、先ほどの案文から罰則を除いたものを考えている。

○　先般、「原田ウィルス」の作成者が逮捕されていたが、ある程度規制を強化しないと人権を守れない事態になっている、すなわち、被害を受ける側のことも考えないといけないのではないかと思っている。サイバー犯罪条約担保法を含む一連の法案に反対の立場を示されているが、「こことここは反対であるが、ここは早急にやらなくてはならない」というように、もう少し具体的に考え方を整理した方が良いのではないか。意見書では「早急な結論を導くことは望ましくない」、「具体的に十分検討」と書いてあるが、早急にやらなければならないこともあるのではないか。

→　日弁連としては、時代状況に応じながら考えており、旧来型の枠組みを一つ一つチェックしてきたという経過も踏まえると、政府の方で何らかの形の法案のようなものを考えているのであれば、それを受け、旧来の法案について日弁連の各分野で用意してきた案文を調整し意見を述べさせていただく。

○　参考配布されている第 45 回人権大会の宣言と本日の意見書を比較すると、本日の意見書は、基本的に人権大会の宣言の精神を踏まえられているようであるが、トーンはかなり異なる。人権宣言が出た 2002 年以降の情報化の流れ、推移を見た上で書かれているのだと思うのだが、どのように理解したらよいか。

→　2002 年から今日までの間に法制度が変わっていることが影響している。適正管理ということについて、2002 年の頃までは「努力義務」だったが、現在では「義務」になっている。努力義務というのは、法的にいうと、努力していれば良いという意味であり、問題が発生しても、「努力している」ということが言えればよい。それが「適正管理義務」ということになると、適正管理しているかと言うことが端的に問題となり、法的には非常に重いものとなる。このような状況を踏まえ、日弁連からも努力義務ではなく端的に適正管理義務にすべきだということを言ってきており、その結果、現在の個人情報保護

法、行政機関個人情報保護法、あるいは全国の自治体の個人情報保護条例は、恐らくほとんど全てが適正管理義務に変わっている。このように、適正に管理しなければいけないという状況が出来ており、個人データを様々な形で利用する条件整備が揃ってきている、変化が出てきていると考えている。

→　一部の人だけが情報セキュリティに関する仕組みを作ってしまうのではなくて、もちろん、できる人は限られているかもしれないが、国民から寄せられる「自分はこういう問題意識を持っている」「こういう被害を受けている」という意見が仕組みに反映されていかなければいけないと思う。その場合、データ管理について言えば、「私の情報がこうなっているのは、おかしいのではないか。」ということに対して、技術的に仕組みを変えるなどの議論が出来ないといけないと思う。そのときのポイントとして、プライバシーというものを日本社会でどう位置づけるかという議論は、固定もせず将来的に定まることもないと思うが、法律家としては、そこを考えつつ、この問題に取り組まなければならないと考えており、情報セキュリティを進める方向については、積極的な考え方である。

(2) 基本計画策定に向けた、関係者ヒアリング②：全国市長会（神奈川県藤沢市）

神奈川県藤沢市から、資料５に沿って説明がなされた後、下記内容の討議が行われた。

○　地域金融機関の場合は、日銀や金融庁の指針類およびFISC（金融情報システムセンター）から出ている基準がかなり明確であり、それをチェックしながら対策を進めている例が多い。地方公共団体についても、内閣官房なり総務省が一律の基準や均一のセキュリティポリシーを策定し、それを遵守させるという方法も有り得るかとは思うが、そもそも、首長が「安全性より利便性・効率性重視」を公約して当選した場合など、民主主義や地方自治との関係でどの程度まで指導が可能なのか疑問がある。

→　情報セキュリティについては、総務省からガイドラインが出ているが、基本的な考え方や基本的な対応について定められているだけである。実際に、予算的なことも含め、どのようにどこまで対策を実施するかは、主にそれぞれの首長の判断、それぞれの自治体の政策に任されている。

○　資料中、業務継続計画について言及がなされている。現在、内閣府の防災担当で業務継続計画に関するガイドラインを策定されていて、情報セキュリティ関連の内容も含まれているが、その内容を充実させた方が良いというお考えか。また、藤沢市では業務継続計画を策定されているのか。

→　業務継続計画は必要であると認識している。なお、全国の自治体を見ると、いまだほとんどの自治体が業務継続計画を策定していないが、策定しようという動き自体は、いろいろな所で行われており、藤沢市でも策定作業を進めているところである。

○　セキュリティ保険の創設について言及がなされている。自治体の場合、保険が使われない場合は税金を捨てていることになる、保険が活用される事態が発生しないようにするべきであり保険をかけると無責任になる恐れがある、損害に対する賠償などが必要な事態が発生したときは予算措置をすれば良いだけである、と思うのだが。

→　指摘のとおり、保険に逃げるということになると意味が全然ないが、いろいろな手当をしても、どうしても低減できないリスクが存在するので、保険という考え方自体はあっても良いのではないか。例えば、病院などの医療事業についても、保険は存在している。

○　地方公共団体間の格差が非常に大きいという指摘があった。民間企業でもそうだが、人に依存している部分が大きいのが原因であり、何らかのルールとそれを監査する仕組みがないと、中々平準化しないと思われる。民間企業の場合、内部統制報告書制度、いわゆる J-SOX の導入がきっかけになっているが、地方公共団体についても、これに該当する内容を基本計画に盛り込む必要があるのではないか。

→　民間企業で言うところの J-SOX に該当するものが、地方公共団体に存在しないのは事実である。結局のところ、住民の判断が最終的な政策判断につながるのであり、その点で民間企業とは異なるのではないかと考えている。

○　資料の４頁目に「各地方公共団体の情報セキュリティ対策に「差」があってはならず、取り扱いも含め全国均一な対応が必要で、独立して取り扱うべき重要な領域ではないだろうか。」と記載されているが、ガイドラインレベルの話か。それとも、システムの共同利用を進め、１つのシステムにするということか。

→　「全国均一」のとらえ方であるが、同じようなレベルに保つということであれば、方法については、いろいろあるのではないかと考えている。

○　人材について言及があった。藤沢市では情報セキュリティ担当者が充分配置できていると思うが、特に東京から離れた地方公共団体では、情報セキュリティの専門家を確保できているのか。

→　藤沢市でも、専任の常勤職員を置いている訳ではなく、専門的な知識経験を持っている外部の人間を非常勤職員として採用している。人材については、地方に行くともっと厳しい状況である。情報システムの運営担当者自体が１～２人であり、情報セキュリティまで手が回らないという地方公共団体もあると聞いている。

○　資料の５頁目に「市町村の情報セキュリティポリシー策定率と情報セキュリティ研修実施率」が掲載されているが、この表を見る限り、「情報セキュリティポリシー」の策定率自体は高い。先ほど、各地方公共団体で保有する情報資産自体は基本的に近い反面、脆弱性などがだいぶ異なるなど、情報セキュリティのレベルには格差があるとのお話があったが、情報セキュリティポリシーは、組織の情報セキュリティに関するリスク、脆弱性などを洗い出しで策定するところ、様々な「情報セキュリティポリシー」が存在していると理解してよいか。

→　推測を含めてお話をすると、情報セキュリティポリシーについては、何をすべきかという基準・文言を定める話と、実際に普段実行しているのかという話は、別の話と思われる。

○　資料の５頁目の表にある「監査」について。ISMS などでは外部監査をやることになるが、ここで言う「監査」には、外部監査を含むという意味か、あるいは外部監査のみを指すのか。

→　監査については、内部監査と外部監査の両方を含む。外部監査だけを抽出すると、非常に少なくなるのが実情である。

○　情報セキュリティ研修について実施率が急激に高まっているのは、LASDEC で e-learning による研修システムを開発したことによることが大きい。LASDEC を通じた政策と自治体への対応が、広く行き渡っているということは言える。

○　監査の問題については、金銭的な問題がかなり関わってくる。外部監査になると、相当な費用を計上しなければならないが、議会の了承を得るのが大変だと思われる。本日の説明にもあったが、議会や首長をはじめとする幹部職員に御理解いただく努力が必要になるだろう。

(3) 基本計画策定に向けた、関係者ヒアリング③：日本経済団体連合会

日本経済団体連合会から、資料６に沿って説明がなされた後、下記内容の討議が行われた。

○　資料の６頁目に中小企業について言及があり、中小企業にとって取引相手ごとに個別のセキュリティ基準に従って対応することは負担が重いため、何らかの対策を講じる必要があるとのことであるが、具体的にはどのような対策をお考えか。

→　根本的には、発注側である大企業自身が、何をどこまでやっても良いのかという基準を定められないのが問題であると考えるので、発注側を揃えることが第一の問題であると考える。

→　６頁に記載のある「一定の共通セキュリティの目安の整備」が、政府が考え、大企業に要請して欲しい一番根本のことである。

○　民間企業の団体が、「国に基準を決めてもらい一斉に揃えたい」というのは、俄かには信じがたい。民間企業が自らの経営の一環である情報セキュリティ対策の整理を国に要望し揃える、というのは筋が大きく違っているのではないか。

→　政府が策定した基準に従うというような自立性のない話ではなく、企業自身も努力しているが、なかなか努力しきれないところがある。官民双方で一緒にやることが必要なのではないかと考えている。

→　努力をしていても、どこかで一回でも情報セキュリティに関する事故を起こすと、努力が全然顧みられないという問題がある。

○　大企業は、各々の創意工夫により先進的・先端的な情報セキュリティ対策を採用していけば良いが、それを中小企業に対し一律に押し付けるといった過度に厳しい大企業があれば、

いずれ評判が落ち市場で淘汰される、という市場原理が当然働く筋合いではないか。

→　例えば、個人情報保護法に関連してガイドラインがあり、委託先の監督責任について記載されているが、大企業は、どちらかというとかなり厳しい水準を維持しようとするので、自ずと委託先にもそれを求める傾向にある。情報セキュリティ推進の目安のようなものがあれば、かなり厳しい水準を求める傾向が改善されるので、コンセンサスを取っていただきたい。

○　中小企業の立場からすると、経団連の意見はもっともな意見であると感じている。各取引先からの要望に対応していかなければならず、苦慮している。

○　経団連の下部組織に経営者協会というのがあるが、各地域の経営者協会に対し、情報セキュリティに対する対策等を指示しているのか。

→　各県の経営者協会に対しては、多少言う機会はあるが、具体的な指示まではできていないのが実態である。

○　「監査を導入する」と資料にあるが、監査制度を導入する場合、そのための基準等もあわせて導入することが必要である。経団連として、基準等の導入もすすめていくということか。

→　指摘のとおり、外部監査のためには監査の基準が必要であるので、その辺りも整理することになると思われる。

○　外部監査を受け認証を受けた組織でも不祥事や事故が発生しているという実態を見ると、外部監査をすれば物事がうまくいく訳ではなく、自ら PDCA サイクルをしっかりと回すことが必要なのではないか。また、資料の５頁目に「企業努力を顧みられることなく一様に非難の対象」とあるが、トラブルが起きた際には、どういう体制と原因で起きたのか、きちんと検証し公表することで理解を求めていくという活動しか方法がないのではないか。

→　まず自分たちが取り組まなければいけないと言うことは、もちろん認識している。まずセキュリティを確保しないと、体制自体の存続が危なくなるのであり、セキュリティを強化すると仕事がやりづらいというレベルの話と同列には扱えないことは、言うまでもない。その上で、外部からの視点を加えるとよいのではないかと考えており、要望したい。

→　第三者監査については、政府機関の取り組みに対する要望である。現在は基本的に自己評価に近い形だと聞いているので、これを客観的に第三者が評価指定はどうかと考える。

→　第三者監査については、例えば NISC が各府省庁の状況を直接把握するといった方法もあると思う。

○　経団連御指摘のとおり、情報セキュリティに関するトラブルを完全に防止することは不可能であり、事後処理は絶対に必要。航空事故に事故調査委員会があるように、情報セキュリティに関しても、事故で起こったことを経験に、他の組織・企業が同じ事故を起こさないために情報を共有化していく委員会があるべきではないかと思っているが、内部的な機密

事項などをうまく隠した形で事故の情報を開示・共有できるのか。

→　官民を含めた事故情報を共有するシステムを作り上げることは、非常に重要であると考えている。

○　企業努力を評価してもらうようにするには、「見える」化しないといけない。情報システムないしITの利活用システムのセキュリティレベル、信頼性レベルそのものについて、ある程度明示的に把握し、どういうものにはどういうレベルの対策をするのか検討していかないといけない。経団連で具体的に取り組まれるのであれば、このようなレベルの議論まで、是非踏み込んでいただきたい。日本の国民感情からすると議論しにくいが、国際的にはやらざるを得ないと思っているので、是非御検討いただきたい。

→　指摘のとおり、精神論だけ言っていても話が進まない。最終的には、具体的なレベルの議論を検討することが大切であると認識しているので、我々も進めていきたい。

○　資料の６頁目に税制面の優遇措置の話があるが、現在でもIT設備投資税制などで優遇措置が存在する。これとは違うものを想定しているのか。

→　税制については、例えばSaaSを利用した際の優遇措置などが議論に上っているが。セキュリティを担保するには結構お金がかかるので、優遇措置については、できれば広い範囲であればありがたいと考えている。

○　優遇税制については、屋上屋を重ねるような税制にならないようにする必要があると思う。

○　トラブル発生時に企業努力が顧みられないことの原因の一つとして、報道の問題もあるのではないか。いろいろな障害が起きたときの報道を見ると、芸能ニュースに近いような（皮相的で大袈裟な）報道をしているケースが多いように感じる。障害を起こした企業がメディアに対して充分説明することは前提だが、それをメディアが良く学習することを通じ、メディアのITに対するリテラシーを高めることも必要なのではないか。

○　政府機関の評価については、自己申告に基づく評価だけでは実態を把握し切れないのではないか。最初（１・２年目）は自己申告でも良いが、徐々に第三者監査を導入してチェックしないと、評価結果が本当に実態を表しているかは疑わしいと思う。

○　市場に任せるべきという意見も多いが、欧米の状況を見てみると、情報セキュリティ対策の推進のため、低金利融資・税制面の優遇措置・補助金の交付を政府が行っている。環境や農業の安全保障と同様に、市場原理だけではうまく行かないと思われるので、政府が積極的に取り組んでも良いのではないか。地方の企業では、利益に直接結びつかない情報セキュリティ対策に1,000万円投資することなどは不可能である。

○　事故の対応に関するデータベースをつくり、学習するという方法は、非常に重要だと思う。事故直後の緊急的な対策と、事故発生後長期にわたって分析するデータの確保を通じた長期

的な予防体制のレベルアップは必要であり、産官連携でやるべき。

(4) 基本計画策定に向けた、関係者ヒアリング④：重要インフラ専門委員会

重要インフラ専門委員会浅野委員長から、資料７に沿って説明がなされた後、下記内容の討議が行われた。

○　重要インフラ分野横断的演習については、もう少し大規模かつ長期間で行うべきだと考えているが、御意見をうかがいたい。

→　CEPTOAR の整備が進むなど体制面での整備が進展したことなどを受け、今年の訓練についても、参加者の追加やシナリオの作り方の変更を行った。また、参加者同士のコミュニケーションを遮断することにより、実際の行動により近づけた。演習を２日以上行うことはできなかったが、長期間演習を実施し分析することもしてみたかったと考えている。

○　そもそもの話になってしまうが、「重要インフラとは何か」という定義は行っているのか。金融の場合であれば、例えば全銀センターや日銀ネットなどの決済系システム、メガバンクのシステムに限らず、信用金庫など個別金融機関のシステムも全部がそれぞれ重要インフラに該当するのか。

→　「重要インフラ」として、現在 10 分野が指定されている。また、業種の中において、システムの規模などによって重要インフラか否かを区切ることは行っていない。

→　元々、現在の行動計画の前身である「サイバーテロ対策に係る特別行動計画」では対象分野とシステムを指定していたが、その場合、時代と共に陳腐化するという状況があったので、現在の行動計画では対象分野を指定し、システムについては例示にとどめた。また、所管法との関係もあり、範囲については若干曖昧にしている。

→　所管法は、IT・情報セキュリティの観点からのみ定められるものではないため、IT・情報セキュリティの観点から策定された行動計画との間では、当然、温度差がある。そのため、所管法に何らかの影響を与えることは、なかなか難しい面がある。

○　今回の計画策定議論を通じ、重要インフラの定義について何らかの基準を示す必要があるのではないか。漠然と「重要インフラだからこうだ」ということでは、実際の行動に落とす段階で上手くいかない可能性があり、そうならないようにすることが適当である。

○　重要インフラの情報セキュリティ対策については、各企業あるいは事業分野における CSR、ボランタリーな気持ちで参加していただく前提でお願いしている。これは、所管法との関係、体制が何もない段階で情報セキュリティ対策を促進させる必要性、限られた時間の中で行動計画を作らなければならない必要性などを勘案し、重要インフラの自主性と社会的責任を感じている中での情報セキュリティに係る取り組みへの協力というところで、今の行動計画は成立している。

○　今後の対策の進め方については、重要インフラ専門委員会の中でも議論がなされており、

例えば、何らかの強い参加を求めるのであれば、同時に費用など何らかの形の手当をする必要があるのではないか、という議論が実際に過去の委員会でなされた。所管法との関係、国民保護法制や防災との関係をどうしていくかという問題提起もなされている。これに関しては、今のところ、強く踏み込んで解決するのではなく、問題として認識し、事務局の方で回答を探っている段階である。

○　米国ではこの点、人々の生活にとって不可欠な分野について、当初、重点領域インフラ８分野と定め、所管は各省庁だが DHS がチェックをかける役割を負う形で対策が始まっている。そして、その米国とパラレルな形で日本の重要インフラの概念は出来ている。

(5) 自由討議

本日のヒアリングの内容などを踏まえ、自由討議を行った。

○　先ほど、メディアが学習することを通じ、メディアの IT に対するリテラシーを高めることが必要との指摘があった。もっともな指摘ではあるが、なかなか難しい面があるのも事実。ただし、メディアが変なとらえ方をした結果、規制強化・厳罰化一辺倒に陥らないようにすることは必要。行政は本来的に、規制と誘導の両面が大事で、その線引きをどうするのかが一番重要である。その基本的な考え方を第２次基本計画のなかで出していく必要があるのではないか。

○　ボランティアベースで重要インフラの情報セキュリティ対策に取り組んでいるとのことであったが、誘導策を次々考え出すことにより、我々の考える方向でガイドラインを作り出していくことが必要である。

○　安全、安心というキーワードを考えたとき、通常やっておくべきこともたくさんあるが、それは各組織が行うのが当然だと思う。しかし、何か起きたときに迅速にかつ妥当に動ける仕組み、体制・環境・法制度などを用意しておかないと、結局、通常のルールでは何も出来ないケースが出てくる。今度の計画では、何か起きたとき、それをきちんと統括して対応できる体制をどうやったら作れるか、ということをきちんと盛り込んでおくべきではないか。各省庁間で利害関係が対立することもあると思うので、平常時までする必要はないと思うが、何か起きたときには、ある程度の統括的な権限なり指揮権を集めないと対応出来ないと思う。

○　一般に民間でコンサルティングなどをする場合、最初は一般的な対策から始まるが、それが一段落したら、インシデント対応や対策強化のためのチェック機能の検討の話になる。「第１次情報セキュリティ基本計画」に基づく取組みにより、最初の第一歩は進んだという感想をもっており、その意味では、今度の基本計画では、インシデント対応や対策強化のためのチェック機能の確立が到達すべきところであると思う。

○　チェック機能というのは、第三者監査に限られないと思っている。勿論、第三者監査も含まれるが、内部監査や自己点検なども含まれると思う。勿論、第三者監査も意味があると思うので、検討することは否定しないが。

○　情報漏えいが発生した企業の事後対応のための委員会に参加し原因追及をした際の経験から言わせてもらうと、技術的な話や企業組織のステートメントなどが比較できるデータベースが必要であると思っているので、情報セキュリティ事故に関する事故調査委員会のようなものは有益であり、そういった取り組みを通じてトラブルは克服出来ると思う。

○　第三者監査を行うためには、監査の基準が必要であるが、それは、抽象的な精神論レベルではなく、ミニマムスタンダード的な具体的なものである。そうすると、「ミニマムスタンダードを設定し得るのか」という話になるが、恐らく、国から個人に至るまで、全部に共通したミニマムスタンダードを設定することはあり得ないと思う。国や地方公共団体（後者については地方自治との関係で許されるのであればだが）については可能かもしれないが、重要インフラ辺りで線引きがなされると思う。中小企業や個人については、正直、ミニマムスタンダードの設定までは時期尚早で、暫く時間がかかると思われる。どこまで設定できるのか、またすべきなのか、次回以降きちんと議論し、狙いを定めていくべきだと思う。

○　先ほど意見のあった、「何か起きたときの迅速かつ妥当に動ける仕組みの構築」は、非常に重要であると思うので、私も賛成である。

○　情報の有害性に関する「何か悪い情報を流すと少年が人を殺すかもしれない」的な話は、優先順位を低く置かざるを得ないのではないか。ただ、委員それぞれ立場や価値観が様々なので、議論の優先順位については、次回以降に向けて、事務局を中心に交通整理を行っていただきたい。

○　交通整理については事務局と相談したい。なお、ブレストをオフィシャルな会議だけで行うのは困難であり、会議と並行して、インフォーマルな形で意見交換する場が必要ではないかと考えている。協力願える委員は協力していただきたい。

○　法学の分野では、情報セキュリティについて正面から取り組む議論がほとんどない。「将来何かが起こったときに法はどう対応すればよいか」というのではなく、「何かが起こったときに今ある法制度を使ってどう解決すればよいか」という発想がある。技術が急速に発展する状況にあって、情報セキュリティについて議論することは、法学会も法曹界もなかなか難しい。情報セキュリティ政策の議論を詰めて、それぞれの政策官庁が具体的な立法を提案する必要があるのではないかと思う。事件が発生したので解決するという考え方では十分でない。法学の分野とその他の分野の発想の違い、宿命のようなものかという気もするが、進歩する社会の中で、法の果たす役割を変えないといけないと感じた。

○　法学は最悪の事態を想定して考えることがあると思うと、法の分野の姿勢が理解出来ると思う。

⑹ 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。