情報セキュリティ政策会議　企業・個人評価指標専門委員会
第３回会合議事要旨

１．日　時

平成 18 年９月 25 日（月）　９時 00 分～11 時 00 分

２．場　所

内閣府会議室

３．出席者

【委　員】

大木　栄二郎　委員（工学院大学教授）
佐々木　良一　委員（東京電機大学教授）
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／株式会社ディアイティ代表取締役社長）
妹尾　堅一郎　委員（東京大学先端科学技術研究センター特任教授）
棚橋　康郎　委員（新日鉄ソリューションズ㈱代表取締役会長）
田辺　国昭　委員（東京大学教授）
滑川　恵理子　委員(㈱サンケイリビング新聞社マーケティング戦略室編集企画部長）
村上　輝康　委員（株式会社野村総合研究所理事長）

（五十音順）

【政　府】

内閣官房情報セキュリティセンター副センター長
内閣官房情報セキュリティセンター情報セキュリティ補佐官
内閣官房情報セキュリティセンター内閣参事官
警察庁生活安全局情報技術犯罪対策課長
防衛庁運用企画局情報通信・研究課情報保証室長
総務省情報通信政策局情報通信政策課情報セキュリティ対策室長
文部科学省大臣官房政策課情報化推進室長
経済産業省商務情報政策局情報セキュリティ政策室長

４．議事概要

(1)　セキュア・ジャパンの姿（企業・個人）のイメージ及び評価指標の検討

○　事務局から説明

(2)　討議

○　本日は、最初に政策・施策系から「セキュア・ジャパンの姿（企業・個人）」を検討した後、JIS Q 27002等の規範系から、その姿に追加すべ

き事項がないかを検討して行きたい。

○　個人の情報セキュリティ対策について、学校が情報提供や啓発活動を推進して行く上では重要であるが、広まって行くのに時間がかかる。

○　実際にパソコンを使用している大人の場合、メーカーとかプロバイダのサポートセンターから情報が来るというのが、一番分かりやすいのではないか。また、ウィルス対策ソフトの購入と更新など、企業経由での広報啓発というのも一般的に使われている。

○　情報の流れを大別すると、情報提供・啓発の仕組みと、トラブル時の対応の仕組みに大別される。

○　セキュリティ対策の専門性をどこまで個人に求めるか、個人に何をどこまでやらせるかというところが、一番大きな課題である。企業でも、現場の職員が何もしなくても、専門の部署がセキュリティ対策を実施している。

○　情報センターの様なものが存在し、セキュリティに関する情報がいつでも入手出来る一方、セキュリティに関するトラブル情報が集約されるような仕組みができると、前進して行くのではないか。

○　評価指標としては、プロバイダの契約時に情報セキュリティに関する最新の情報が置かれている場所を教えている率などが考えられる。

○　学校の関係では、セキュリティ教育というものを実際のパソコン教育の中でどのくらい確保しているかなどが考えられる。

○　トラブル時の対応の関係では、サポートセンターの相談件数や消費生活センターの生活者窓口への相談件数が、考えられる。このような相談件数は、啓発が進むと増えると思う。

○　前回、政策・施策というものをベースにして議論をしてゆくことになったと理解しているが、規範系の話が何故でてくるのか。

○　一つの仮説として、情報セキュリティ関係の施策をして行くと、施策の展開が企業に及んだとき、そこにおける今までのリスクマネジメントなり情報セキュリティマネジメントのところでも、施策の展開が図られると考えられるが、その際、どこに影響を与えたかを見るインデックスを作って行くときの柱として、指標を使う。

○　セキュア・ジャパンの姿の方に指標を展開しようという話ではないが、社会的な影響を見て行くところで書けるものがあるのであれば、書

けばよいのではないかと思っている。よって、規範系の作業に関しては、評価指標を作って行くという中の作業のステップストーンだと思っていただければと思う。

○　政府・地方自治体及び重要インフラといった、別の委員会で検討しているものと最終的に一体化するとのことであるが、どういうことを意味するのか。

○　政府機関評価指標検討委員会、企業・個人評価指標専門委員会及び重要インフラ専門委員会で、それぞれの分野における目標点と評価指標をどうするかという議論をしているが、最終的には、これら三つの目標点と評価指標を含めた評価の枠組みをあわせた一冊の文書を作成し、政策会議に報告ないし政策会議で決定することを考えている。

○　「セキュア・ジャパンの姿」素案中の「情報セキュリティに関するリスクの基本認識」について、犯罪やテロというところからリスクについて言及しているが、ITが悪いもので、不安感があるという非常に短絡的な印象を与えることになり、好ましくない。

○　情報セキュリティの問題は、事故とか脆弱性に基づくIT利用に対する不安から生じているのではなく、情報それ自身が非常に価値を持ち始めたことによるのではないか。

○　「セキュア・ジャパンの姿」素案中の企業の情報セキュリティガバナンスに関する記述は、企業そのものを視点にしているが、企業全体の社会、企業間の取引やそこでのルールに関する内容も必要ではないか。例えば、非常に機微な個人情報について、その取扱方法が決まっている、など。

○　「セキュア・ジャパンの姿」素案中の企業の情報セキュリティ関連製品とサービスに関する記述は、全体的に、ISMS、製品系のISO/IEC 15408、システム開発におけるセキュリティ、脆弱性をつくらない方法とが、書き方として全部混在しており、整理する必要があるのではないか。また、システム開発におけるセキュリティ要件の定義と、開発プロセスにおけるセキュリティチェックというようなところがない。

○　「セキュア・ジャパンの姿」素案中の企業の情報セキュリティ人材に関する記述で、情報セキュリティ人材間における情報交換や交流については、必要なければやる必要はないのだから、情報交換や交流が行われていると断定的に書かなくても良いのではないか。

○　「セキュア・ジャパンの姿」素案中の企業の情報セキュリティインシデント対応に関する記述で、社会全体としてインシデント発生時の対応

メカニズムが確立されている旨の記述があるが、それは厳しいのではないか。

○　個人については、マスコミについて言及する必要があるのではないか。

○　「セキュア・ジャパンの姿」素案中の個人向け情報セキュリティ関連製品とサービスについては、それが提供され、広く浸透しているというのではなく、セキュリティ対策を実施していることを意識していなくても、十分なセキュリティ対策が出来ているべきなのではないか。

○　これは指標確立後の調査方法に関する問題かもしれないが、企業のセキュリティ対策の状況を正確に把握しようとすれば、多くの項目について調査する必要があり、かつ、定期的に調査する必要があるが、調査される企業としては、大変負担が大きい。

○　大規模な調査をやる場合、調査を通じて情報セキュリティ対策の重要性に気付き、自らの責任と判断でセキュリティレベルを上げて行くという動きにつながれば望ましい。加えて、企業が自らのセキュリティ状況を的確に把握出来るというものにしないと、この調査はうまくいかないだろう。

○　経済産業省の情報セキュリティ対策ベンチマークを普及させるのが、企業に情報セキュリティ対策の重要性を気付かせ、企業自身のセキュリティ状況を的確に把握させるうえで非常に意味があるのではないか。

○　十分とされる情報セキュリティ対策は経年で変化するので、調査事項の内容についても、経年で変えて行かなければ意味がないと思う。
　現在のベンチマークの内容を充実させつつ、多くの企業に参加させるということに力をいれるのが望ましいのではないか。

○　事務局としては、内閣官房単独でやる意思はなく、IPAや経済産業省とも御相談させていただきたい。ベンチマークについても、活用させていただければと考えている。

○　「セキュア・ジャパンの姿」素案中でセキュリティガバナンスという言葉を使っているが、ここにある定義でガバナンスという言葉を使っている例を見たことがない。
　また、ISMSや情報セキュリティ監査制度に言及しているが、これらはセキュリティのレベルを評価するものではない。

○　「セキュア・ジャパンの姿」素案中で言及されているリスクの関係では、企業が現在持っているITインフラが今の基本構造のままで、2009年

に許容リスク量まで下げられるかというのが大きな問題提起としてあるのではないか。その意味では、現在企業が依存しているITの中にどういうリスクがあるのか、きちんと評価する必要があるのではないか。

○　ガバナンスという言葉には、内部的な認識を超えて、企業の経営者が外部から自分の行動を評価されるかということなども含まれる。

○　情報セキュリティ報告書のようなもので、自分たちのリスク認識やそれに対する活動計画が示されていることが、「望ましい姿」にあるのではないか。

○　具体的に重要情報を取り扱う企業間あるいは企業と政府間の取引の中で、情報セキュリティの確保がどのように実施されているのかというのも、一つの大きなテーマである。

○　個人のところは、国民一般のリスクの意識がどの程度のレベルにあるのかというのも、一つの大きな要素ではないか。

○　情報セキュリティに関するリスクの大きさを国民が理解し、リスクを受容できる程度がわかるようになる施策をやって行く必要があるのではないか。

○　評価指標を考えて行く上で考慮すべき要因として、指標の網羅性、経年的に数値を把握出来るか否か（定量性）及び施策との関連性の三点があるが、これらは相反する場合がある。その場合、施策との関連性や網羅性をある程度明確にした後に、定量化を図って行くという段階を経る必要がある。

○　評価指標の網羅性を確保するためには、規範系から見て、どういう評価指標が抜けているのかを見る必要があるのではないか。

○　定量化の際は、最終的には何らかの形で判断が容易になって行かなくてはならない。相互比較できるようにして行く必要があるのではないか。

○　「セキュア・ジャパンの姿」素案中で示されている、IT関係の利用率が上昇するが、IT関連の犯罪や事故が減少することはなく、IT利用に対する不安は引き続き存在するという基本認識には違和感がある。ここ数年で社会全体の状況自体が大きく変わるのではないかと予測している。

○　企業については、全てのビジネスがIT抜きには考えられなくなっている、ITを抜きにしてはマネジメントが成り立たない、企業が持つ個人あるいは他企業に関する情報が急増しているという事情がある。とすれば、情報セキュリティリスクは、増大することはあっても、現状維持ではな

いと思う。

○　個人については、個人間の相互関与の度合いが非常に増加しており、個人が関与しているITの内容と頻度ないしは量が急増しているため、情報セキュリティリスクは増大しており。それを見越した政策や評価を行って行くのが基本認識ではないか。

○　企業における情報セキュリティ人材について、経営者や専門家の話だけであり、企業人一般の底上げの話がない。情報セキュリティについては、企業人一般の底上げが重要であるので、これは良くないのではないか。

○　情報セキュリティ人材というのは、実は企業における全体の力の状態だという認識になった方が良いのではないか。

○　個人については、少し大げさに言うと、「民度」という概念で捉えるとよいのではないか。つまり、先進国における市民社会の品格という意味での民度。情報セキュリティに関して、先進国としての安全と安心を保てる民度レベルがあるのだと思う。

○　情報化社会においては、自分のサーバを勝手に踏み台に使われて犯罪に使われる等、間接的あるいは非意図的な加害者になりうる可能性があるが、この部分についても考える必要がある。

○　情報セキュリティ教育に関する記述で、大学・大学院に関する記述がないが、先端科学技術に関する情報等が流出することは非常に危険なことであるので、大学・大学院についても言及する必要がある。

○　個人の家庭での普及啓発については、企業に勤めている方が家庭に戻ったときの波及効果によるところが大きい。つまり、企業内で教育されていれば、それが家庭にも移転される。こうした波及効果を重視した方が、現実的には効果があがるのではないか。

○　「セキュア・ジャパンの姿」として、全体の社会状況を示す目標がどこかに出てこないと、社会全体としての姿がまとめにくいのではないか。

○　個人については、教育と情報と商品から「セキュア・ジャパンの姿」に言及しているが、何かが足りないように思える。例えば、教育により情報を得たとしても、行動を変えないと意味がないが、その行動に関する言及がない。

○　交通事故対策で言うところの高齢者のような、情報セキュリティをよく知らないがITをよく利用しているという集団を把握し、当該集団の情

報セキュリティ意識をどうやって向上させるのかという目標が、「セキュア・ジャパンの姿」素案からは見えてこない。

○　「セキュア・ジャパンの姿」素案の個人に関する部分について、教育に関する部分については明確に言及されているが、物理的な対策や取締に関する部分が言及されていない。

○　今回示された調査項目について、全部を実施することは負担が多いので、既存のものを活用できる項目と新たに調査しないといけない項目を仕分けをし、提示して頂きたい。

○　情報セキュリティ対策実施率への言及があるが、情報サービスに該当するところとソフトウェアに該当するところは分けて考える必要がある。

○　評価指標の案として、業界基準・推奨業界基準という言葉が出てくるが、経済産業省のベンチマークを議論した時に、業種を捉えても意味がないという結論になっている。
　これに限らず、既に他の委員会等で議論された結論のうち、意味のある内容についてはどんどん取り入れ、この委員会ではそこを超えた議論をしていかないといけないのではないか。

○　現在の学校教育について説明させていただくと、情報セキュリティ教育が重要であるとの認識のもと、情報教育の一部として、高等学校・中学校では必修科目としている。しかし、小学校では、総合的な学習の時間の中に位置づけられているため、学校によってその取り組みに差があるのが実情であり、今後の課題であると認識している。

○　情報セキュリティ教育に関連して、教員の存在率という指標案が示されているが、主に小学校の児童を対象とした情報セキュリティ教育を含む情報モラル教育の実施をする知識、指導力のある教員が存在するかという観点で指標を設定していただくと、小学校における情報セキュリティ教育も確実に進むと考えている。

○　教材の所持率という指標案があるが、教材を持っているか否かではなく、先生方がその教材を教えられるか否かが重要であるので、この観点から指標を設定した方が適切ではないか。

○　評価指標案については、詳細な部分で精査した方が良いと思われる部分があると思うので、さらに議論すべき。

○　事務局としても、今回示した「セキュア・ジャパンの姿」素案のうち、リスクのところについては「たたき台」であり、考え方の書き直しが必

要であると考えている。

○　ISMSや情報セキュリティ監査制度が混在しているとの指摘については、わざと混在させたところもあるが、事務局としてもう少し整理したい。

○　情報セキュリティ人材に関する記述については、他の議論との並びのなかで、もう少し加筆しようと事務局としては考えている。

○　マスメディアについては、事務局も重要な役割であることは認識しているものの、どのように記述するかについては、非常に難しい問題であると認識している。

○　３年後の社会での個人の状況をどのように書くか、本当に書ききれるかは事務局としても非常に悩んでおり、もう少し御議論いただきたい。

○　個人については、引き続き個人に具体的なスキルを求めて行かないといけないのか、あるいは、スキルを上げなくてもカバー出来るようになるのではないか、という問題があり、非常に難しい問題であると事務局では認識している。

○　評価指標案で技術基準の適合認定に関連し、技術基準適合マーク添付を確認したか否かという記述があるが、現実には、販売店で買うと必ずついているという合理的期待から確認していないのではないか。
　これに限らず、一つ一つの項目の精査を重ねていった方が良いと考える。

○　評価指標案に関する議論については、検討の時間をいただきたい。また、既存の資料を活用出来るか否かなどがわかるような資料にしていただきたいという意見に賛成である。

○　マスコミの関係については、マスコミに期待するというよりも、個人に何らかの形で気付いてもらう、突発的な情報を伝える仕組みが必要であるという言及で良いのではないか。インターネット等の代替手段が存在するのであり、マスコミがやらないのであれば、やらなければよいと思う。ただし、インターネット等の代替手段は、それを見ない人たちが存在するので、これに依存するのは問題である

○　個人については、実はセキュリティの問題ではなくて、IT利用の問題なのではないか。セキュリティ製品が入っているから良いというものではなく、ITを円滑安全に利用できるというのがセキュリティだと思う。
　個人に対する支援策は、ウィルス対策ソフトを入れているかなどの話ではない。

○　様々な評価モデルとISO/IEC 17799の対照表が提示されており、経済産業省の情報セキュリティ対策ベンチマークについて、ISO/IEC 17799の全部をカバーしていないという結果が示されているが、このベンチマークは、ISO/IEC 17799の全部を基本的にカバーする形で作っていることは補足させていただきたい。

○　評価指標案で、CC認証を一件以上取得している会社の率を示しているが、これを数えても意味はないと思う。

○　評価指標案中、自社製品の脆弱性等対処率については、偶々脆弱性が見つからなかった企業は良いのか。この部分については、企業として情報を出しにくいのではないか、などの問題がある。

○　ISO/IEC 17799の評価項目は106あるが、そのまま用いるとすれば多すぎると思う。実際に活用する段階では、出来るだけ集約するのが良いのではないか。

○　マスコミとの関連では、政府公報の活用という考え方はどうか。

○　例えばペイオフの解禁などは、政府公報がその認知率をあげたというよりは、むしろ銀行に貼りだしているポスターなどによる効果が大きかったと思う。マスメディアに該当するかは別として、政府公報以外の情報の提供、PR系は考えて行かざるを得ない。

○　情報セキュリティに関して注意喚起して行くという点では、メディアは確かに重要であるとしても、企業による情報の提供もかなり重要であることは否定出来ない。

○　情報セキュリティの教育については、単に「知る」だけでは不十分で、「知って対応出来る」というところまで行かなければならない。しかし、全ての人がそこまで到達出来るかというと、それは不可能である。
　そこで、セキュリティ教育について、ある種の階層関係を持たせて、その中で地域的あるいはバーチャルなグループの中で相互に教えあう、あるいは、グループ内に教えられる人と教える人がいて、その教える人を教える仕組みを考えて行かないと、多分うまく行かないのではないか。

○　「セキュア・ジャパンの姿」の中で、企業間取引について改めて項をつくり、その断面で見る必要はないのではないか。

○　個人との関係で、倫理教育の中に情報セキュリティが含まれるという話があったが、やはり情報セキュリティというところが鮮明にわかるような指標で、他との関係がわかるようにする必要がある。

○　メディアにとっては、情報がどういうかたちで、どこから、必ず一本として出てくるかということを重視している。ここに聞けば大体わかる、何かの時に必ずリリースが発信されるというところが拠り所となっていくのではないかと思う。

○　個人がどれだけ情報セキュリティに関するスキルを持つか、モラルを獲得して行くかということのためには、情報が常々、きちんと発信されていることが非常に大切である。

○　今ここまで危機は来ているので、これ以上のことはやるべきではないといった情報がどれだけ流れているか、それはメディアから流れて行くという部分が非常に大きいと思う。

○　企業と個人との関係のところでは、会社で個人のパソコンを使う、家に会社の仕事を持って帰る、この部分の整理が、初歩的ではあるが重要なのではないか。米国などでは、持ち込むことが前提で、そのマネジメントがきちんとしていないのが問題であるという考え方もある。

○　「セキュア・ジャパンの姿」素案の基本認識に書いてあることは、セキュリティを如何に高めるかという視点で書かれているが、やはり、セキュリティを高めるという視点の一方で、情報をいかにうまく使って世の中発達するかという視点も必要である。お互いをどう両立させるかというような指標の考え方が、基本認識の所に触れられておいた方が良いのではないか。

○　資料中、事業継続性計画の話があるが、政府の統一基準の中では、事業継続計画には正面から取り組んでいない。事業継続性計画に関する指標を追加した場合、政府の実施状況は評価しないが、企業の実施状況は評価することになることを参考までに申し上げる。

○　事業継続性計画について、政府については中央防災会議で議論されており、きちんと実施することになっている。政府としてやっていないという話ではない。

(3)　今後の予定について

○　事務局から説明