資料2

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２回会合議事要旨

１．日　時

平成 18 年９月７日（木）　17 時 00 分～19 時 00 分

２．場　所

内閣府別館会議室

３．出席者

【委　員】

井上　克至　委員（エヌ・ティ・ティ・データ・セキュリティ株式会社取締役）
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）
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）
中尾　康二　委員（KDDI㈱技術開発本部情報セキュリティ技術部長）
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長
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

○　事務局から説明

(2) 討議

○ 先ほどの事務局からの説明では、2009年の姿の書き方として、

① ISO/IEC 17799（JIS Q 27002）等を基準にして2009年の姿を書き、それを評価指標にして2009年のセキュリティレベルを評価する、行政評価でいうとアウトカムの評価に関わるもの。

② セキュア・ジャパン2006に掲載された133個の施策が実現した状態を2009年の姿とし、それに基づいて評価指標を設定し評価する、アウトプット評価に関わるもの。

の二つの書き方を御提示いただいたが、どちらを主にしてやるのか、あるいは両方やるのか。両方やるとした場合、両者の関係はどうなのかという問題がある。

○ 前回、政府の取組みが企業のモデルなのではないかと言ったまでで、企業が政府統一基準を参照すべきと言ったわけではない。

○ JIS Q 27002等はセキュリティ・マネジメントに関するものであって技術も含めた情報セキュリティ全体の一部でしかないと認識しているので、全体をカバーする②に①の大括りの要素を一部盛り込んでいくのが良いのではないか。

○ 政府機関や重要インフラは別として、企業とか個人には、強制力をもって強いることは考えるべきではなく、自主判断に基づいて自己責任で行動をするということに委ねるべきであるという基本スタンスで臨むべき。

○ 株式公開企業はJ-SOX法に基づき必要な施策に取り組み始めており、その一環で情報セキュリティも重要だと言われている。こうした観点から各企業は業務プロセスをチェックしているところであり、その状況を見守るべき。

○ 非上場企業は、IPAが実施している情報セキュリティ対策ベンチマークなどの普及により、セキュリティの重要性の認識を与えること、「気付き」を与えることが重要ではないか。

○ 自主判断・自己責任という観点からは、個人・企業については、①の規範によるアプローチではなく、②のプロセス・アプローチが正しいのではないか。政府機関、重要インフラは、場合によっては、規範によるアプローチが良いかも知れないが。

○ ①のようにJIS Q 27002をスタートポイントにすると、いろんな疑問に到達すると予想していた。企業・個人については、政策・施策の観点から指標を作るのでも良いと思う。

○　ただ、JIS Q 27002は、セキュリティのいろいろな観点に関する部品が全部揃っているので、政策・施策の裏に規範のうち使える部品が関係するという形かも知れない。

○　理想論的には、まず、個人とか社会がそれぞれどういう目的を持っているか、あるいは思いをもっているかについて展開し、他方、ある程度定量化でき、かつ政策の方からコントロール性があるものを評価指標として選択する。
　最終的には、政策と評価指標、それから評価指標と目的要素のそれぞれのマトリクスみたいなものを用意して考えていくのがオーソドックスな姿ではないか。

○　企業に強制をしてはならないという意見に賛成である。非公開企業についても、公開企業との取引を介して間接的にJ-SOX法にさらされており、対応しているので、強制せずにやっていってもらいたい。

○　規範は重要だが、環境によって異なるので、これを一つに決めるのは不可。様々な規範が出てきて、それが評価指標に結びついて様々な議論がされていくような、柔軟性を保つようになっているのが良い。

○　②の政策・施策からのアプローチの方が良いのではないか。そして、そこをもう少しかみ砕いて表現する中で、規範が例示としてあるのは良いと思う。

○　②のアプローチの中で例示されている「企業評価」の部分については、潤沢な評価指標が出てくるのかが気になる。

○　規範を大括りのものとし施策の評価と連動させれば、もう少し説得力が出るのではないかと思う。

○　JIS Q 27002の中の項目をそのまま引いてきて、それを基に指標にするというのではなく、もっとマクロな形で根本にある考え方の部分を取り出してくるのが良いと思う。

○　大枠は政策・施策からのアプローチをするとしても、実際に企業がセキュリティのレベルを上げるには、JIS Q 27002のようなマネジメントシステムの考え方を入れてやるしか今のところないので、具体的なところに話を落とすときには、規範を利用したアプローチになると思うが、具体的に何かを測定するといったときには、そのままでは使えないだろう。

○　目標を中心に書くべきかそれとも政策を中心に書くべきかというと、

やはり両方で、その書き方を工夫すれば良いと思う。

○　情報セキュリティが保たれている社会の姿を初めに出し、それを幾つかの領域に分けたのち、その下に個々の政策・施策をぶら下げるという作業により、指標がでてくると思う。

○　今どの状態にあるのか、目標とどのくらい違うのかというところが見えるための指標を付ける必要がある。

○　社会指標を見て、各主体が世の中の状況と自分がやるべきことが見えるような指標を提示する必要がある。また、どの施策を変えて行かなければいけないのかが見える指標にすることも必要である。

○　恐らくJIS等は、主体の規範ではあるが、社会全体の規範ではないと思う。

○　リスクをどう扱うのかは書いておかないと、リスクがこういう形で軽減しました等につながらないと思う。

○　リスクについては、外的要因が多く悩ましいところ。
　リスクに影響を与える脅威は３年間大きく変わらないという仮説の下に進めるというのが唯一できることと思うが、皆さんの御意見を聞きたい。

○　個人・企業共通に言えることとして、どんな情報があればいざというときに対応出来るか、というような環境整備が出来ることが第一なのではないか。つまり、規範ではなくプロセスによるアプローチだと思う。

○　リスクについては、定量化するのではなく、社会なり日本という国家が許容できるリスクはどの程度かを考えるのではないか。

○　セキュリティというものを企業という主体で考えると、大きく三つに分けるのが分かりやすいのではないか。一番目はガバナンス、経営者をどう律するか。二番目がマネジメント、トップが決めたことをどのように実現するかという仕組み。三番目はテクノロジー、技術でマネジメントなりガバナンスを如何にやりやすくするか。

○　ある分類を考えた後、あるべき姿もそれを達成するための政策系もその分類で描くというような考え方を導入すると、少し全体構成がやりやすいのではないか。

○　133個の施策というのは、恐らく考えに考えて作られた体系だと思う

が、それで2009年の理想的な姿が完全に満たされるということは考えにくい。どこまで満たされそうなのか自己評価するという考え方がなければいけない。やはり規範により望ましい姿のイメージを提示するというのは、絶対いるのではないか、その規範がJIS Q 27002かどうかは別にして。

○　①と②を無理にマージさせるのではなく、その二つをやるという考え方が絶対に必要。

○ 規範をベースにした「あるべき姿」を示すのが良いのではないか。JIS Q 27002ならばISO/IEC 17799に源泉があるので、世界最高水準か否かを測定でき、内容的にも大きくは外れない。COSOやCOBITの考え方も重ねていく必要があるとは思うが。
　他方、その「あるべき姿」とは別に、これは最低限やるべきである、というのをミニマムレベルとして立ててはどうか。そして、その間に三段階か四段階の区分が出来れば、それがそのまま評価指標になり、尺度にもなりうると思う。

○　レベル区分をするというのは、最高水準でないといけないというわけではなく、例えば、レベル３で良いと思っている会社はそれでもよい。マーケットからは五段階のレベル３であると見られるが。

○　施策の指標については133個の具体的なものがあるが、それをそのまま使えばよいというものでもないので、もう少しカテゴライゼーションをやって行く。

○　①と②、両方のアプローチでやってもらうということでどうか。

○　企業というのは色々な条件がある中で活動をしており、企業にとっては適切なセキュリティレベルであれば良いわけだが、その「適切だ」というのは、業種や事業規模ではなく、それぞれの企業が持っているセキュリティに対する価値観に基づいて決まるものだと思う。ゆえに、一般的に高ければ高いほどよいのかというと、そういうものではない。

○　規範という考え方はわかるが、それが一般論的な意味での「望ましいレベル」とかを適切に示せるかというと、非常に難しいと思う。

○　一つのイメージとして、JIS Q 27002に基づく項目が幾つかあり、高水準企業なら全部マル、その他企業なら10個程度マル、相応企業ならその中間、という尺度が出来ればよいのではないか。

○　相応企業か否かを誰が判断するのか。

○　常識的に自己判断することになるが、おそらくは業種別に出てくることになるのではないか。
　これは、経営者の判断を尊重する指標の体系になるのではないか。

○　多分無理だと思う。一握りの会社だけがそれをやり、他は無視することになる。

○　「企業はこうあるべき。」ということは一切言わない。2009年の望ましい姿、高水準企業はこういう姿で、ミニマムレベルはこういう姿であるというものも作れないということか。

○　やはり、高水準企業、相応企業を誰が決めるかという問題に帰結する。一律には言い難い。
　例えば、ある企業が相対でＡ社とだけビジネスをやっていた場合、Ａ社が言われるセキュリティをやっていれば、それで「高水準企業」である、JIS Q 27002の項目では２つしかマルがついていないとしても。

○　その場合、マルが二つという状態が相応ということで、企業としては整理すればよい。
　この方法を用いれば、今現在のグローバルな常識と比較して日本はこの水準にある、と言うようなものが書けるだろう。

○　非常に微に入り細に入った指標で評価することにどういう意味があるのか。重要なのは「気付き」を与えて、実際の個々の企業のセキュリティレベルを適切なものにすることではないか。

○　JIS Q 27002等を基にした指標は「気付き」のベースにはならないか。

○　各業種を高水準企業、相応企業、その他企業に分類するという試みは、昨年、経産省でも延べ40～50人の協力の下、長期間議論したが、結局、そのような分類は不可能であるという結論になり、自らの「気付き」を促進するような形態に落ち着いた。
　この専門委員会で議論するのは構わないが、昨年の経験では半年以上議論しても不可能だったので、結論を出すのは無理だと思う。

○　クラシフィケーションが難しいということは世界的にも言われている。情報セキュリティに関するリスクの評価は企業によってまちまちであり、評点をつけること、または三段階にわけるということも難しいものではないかと思う。

○　JIS Q 27002に基づく指標は、国全体としてどうであるか、政策の結

果がどうであるかということには使えると思う。ただ、個々の主体、個々の企業がこの後何をすれば良いのかということを判断するために使うのは難しいのではないか。

○　広い意味での規範と施策の両方から検討する必要があると考えている。
　今問題になっているのは、具体的な評価指標というものはどういうものにするのかということだと思うが、統計データに近いものがある程度ないと、指標を作っても評価に使えないと思う。

○　政策側のほうは、少なくともベースのたたき台にはなるが、政策の進捗度が本当にどれだけ社会に影響を与えたかというところの指標に何を使うかというのが悩ましい。いくら政策をうっても社会が変わらないと言うこともある。

○　「望ましい姿」にどのくらい近づいているかという評価がないと、「その施策が2009年によくできました」という評価しかできない。「望ましい姿」からの距離を測れるようなものが必要ではないか。

○　「望ましい」という言葉をつけるから良くないのではないか。

○　データを取るときの負担を軽減するためには既存データの活用が重要だが、その場合、統計データなど、相応の母集団からなるデータを取らないといけないことに留意する必要がある。

○　JIS Q 27002を基にした項目には、人的資源のセキュリティに関する項目もあるが、このようなデータは国際的にも見たことはなく、日本で議論したこともない。

○　段取りについて、事務局から提案したい。
　まず、2009年で政策が目標としていることは何かということをカテゴリわけしながら書き下しを始めたい。その際、見ていくときのファクターとして、まずJIS Q 27002を利用し、2009年の政策が目標とするところというマーキングと、それは何を見ているのかというところの叩き台を作ろうと思う。
　他方、社会指標の方は、「あるべき姿」から議論をしていくとまとまらないので、逆に指標側から作業を進め、どこまで見えるかということのリストを作り、それを見て「セキュア・ジャパンの姿」というものに展開をするというところを考える。

○　基本的には事務局の提案が一番効率的と思うが、2009年をみるのであれば、やはり本来あるべき姿というか、どうなりたいのかということも

必要ではないか。

○　本来あるべき姿と目標設定に関しては、作業の中から見えてくるものが出てきた段階で順次意見を聞いて行きたいと考えている。

○　本来あるべき姿ということであるが、アプリオリに規範というものがあるのかという点については、疑問を持って欲しい。

○　企業の「世界トップクラスの水準」とは、社会のしなやかな構造、セキュリティ事故が起こっても復元する、そういう状況のことであると思う。また、個人の「不安を限りなくゼロ」とは、個人に対し限りなく優しい社会であり、個人を取り巻く環境が評価指標になるのではないか、いつでもアンチウィルスのソフトが買えるなど。

○　結果系の指標も組み込んでほしい。それを入れないと、結局、単に自己満足で終わりかねない。

○　事務局からの説明で、セキュリティ・インシデントに関する紹介もあったが、統計はとれるのか。

○　発生ベースでとれるものは、統計量としてあるものはとれる。要するに、犯罪になっているものについては、統計が公的にある。IT障害とか幾つかのトラブル系のものに関しては、報道ベースでの統計量は一応とれることはとれる。
　問題は、見つかったものはわかるが、トータルとしてはどれだけ大きいかというのはわからない。例えば、迷惑メールとか違法有害情報とか犯罪への利用というところになると、水面上に出てくるものは見えるが、そうでないところは想像するしかない。

○　迷惑メールとか有害情報は、セキュア・ジャパンにおける情報セキュリティ・インシデントの範疇なのか。

○　今回、この委員会の所掌を超えた部分も提示しているのは事実。この点については、議論の材料提供をするという話であって、ここをどうしようという話ではない。

(3)　今後の予定について
○　事務局から説明