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４回会合議事要旨

１．日　時

平成 18 年 10 月 19 日（木）　９時 00 分～11 時 00 分

２．場　所

内閣府会議室

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）
牧野　二郎　委員（弁護士）
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)　「第１次情報セキュリティ基本計画等に基づく各種施策の評価の全体枠組みについて（案）」及び「情報セキュリティの観点から見た2009年のあるべき「姿」と情報セキュリティ政策の評価指標（内閣官房素案）について

○　事務局から説明

(2)　討議

○　事務局の考え方は非常によくわかるが、2006年のリスクが2009年に受容出来るレベルにな

っているかをチェックするというだけでは、企業にとっては余り意味がない。新しいリスクがどんどん出てくるが、それをどう考えるかが重要ではないか。

○　事務局としては、指標については、新しいリスクに対応する形で適宜組み替えて行くことを考えている。

○　新しいリスクに対し直接対策を取れる政府機関と、間接的な環境整備で対応する企業・個人とでは異なるとの認識のもと、指標の運用に際しては、それぞれの適用領域に応じ、柔軟に運用出来るようにする必要があると事務局としては考えている。

○　「’06のリスクが’09に除去・低減」との記述が資料にあるが、違和感がある。

○　2009年時の日本の「姿」各論について、政府機関、重要インフラ、企業、個人の横の関係がきちんと議論されるのかが気になる。

○　政府機関、重要インフラ、企業、個人の横の関係については、委員会の成果を事務局で一旦集約するので、そこで考えていく。

○　資料中、「2009年の姿各論」と「各論に係る指標」を導くものとして、「基盤のモデル」というものが示されているが、これはどのように理解すればよいのか。

○　「基盤のモデル」とあるのは、今回の議論の出発点であり、政府機関、重要インフラ、企業・個人でそれぞれ異なる。しかし、最終的にこの部分は「評価指標」と「姿」に収れんするので、最終的な論点整理では消えるものとして理解していただきたい。あくまでも検討していくためのモデルである。

(3)　「企業・個人の対策実施領域における情報セキュリティの評価指標（案）」について

○　事務局から説明

(4)　討議

○　企業の情報セキュリティ評価指標の一つとして、「セキュリティ監視ソフトの導入状況」というものがあるが、監視サービスを利用している企業も結構あるので、これが含まれるような指標があると良いのではないか。

○　企業の情報セキュリティ評価指標として、インターネットにさらされている情報システムはセキュリティパッチの適用を怠らないなど、「常識」とされている運用のレベルを満たしているか否かがわかる指標が考えられる。

○　実際にどういうシステムの運用をしているか聞いても仕方がない。機能的に悪いところが見つかれば、それで当然治すはずなので、「定期的又は随時（専門家等による）セキュリティ診断を受診しているか」を回答させるのがよい。

○　セキュリティ診断の実施主体について、外部の第三者の監査・診断に限定する必要はない

と思う。

○　「情報セキュリティ教育の実施内容の充実度」という評価指標とあるが、内容の充実とは、カリキュラムなどの充実か。あるいは、受講対象者の範囲が広がるということか。どちらを指しているのかが明確ではないと思う。

○　「個人が負担感なく情報関連製品・サービスを利用出来る環境整備」に関する評価指標として、「ISP事業者が提供しているウィルス検査サービスや迷惑メールフィルタサービス等の利用者数又は各事業者毎の全加入者中にしめる利用者の割合」を取ることは、工夫をすれば可能ではないか。

○　「インターネット安全教室」に関する評価指標については、単なる参加者数だけではなく、地域人口比率のようなものも取れば、浸透状況を考えられるのではないか。

○　「情報セキュリティを含む情報モラル教育実施の教員存在率」という評価指標があるが、「情報セキュリティ教育に関する（教員向け）研修実施率」も入れた方がよいのではないか。

○　教員に対する研修の実施については、大学の教員養成課程で必修の時間を設けているほか、初任者研修でも情報化への対応ということで時間を設けている。また、10年経った後の研修でも、情報教育を選択研修の一つとしている。

○　ただし、研修内容の実施主体は、大学であり、あるいは都道府県又は政令指定都市であるため、情報教育のなかで情報セキュリティに関する事項がどの程度取り上げられているのかということは、把握していない。

○　教員の情報教育に関する研修経験の有無については、毎年調査をしている。これによると、全公立学校教員の先生方の52.3%が情報教育に関する研修を何らかの形で受けているが、多くは校内研修という形態である。

○　評価指標としていろいろと示されているが、これと2009年のあるべき「姿」とはどういう関係になるのか。

○　評価指標について、予め目標値を設定するのか。目標値を設定しない場合、指標がどうなればどういう評価になるのか、考え方をまとめる必要がある。

○　現在把握している統計に基づいて評価指標を設定するという方針に賛成であるが、個人等のところで、調査を全く実施せずに設計するのは難しいのではないか。

○　大きな枠組みでは、2009年の「姿」と評価指標はほぼ大体マッピングするような関係を事務局では考えている。

○　目標設定については、その必要があれば、総論部分でまとめて触れる。運用に際し、どの指標に設定するべきか御意見があれば、事務局で検討したい。

○　新しい指標については、関係者と調整する必要があるが、幾つかの調査に新しい調査項目を混ぜていただくことを検討している。それでも足りない部分については、指標を拾う範囲を公的な統計調査以外に広めるか、調査を実施することになるが、これについても御議論いただきたいと事務局では考えている。

○　必要ならば、遠慮することなく調査をしても良いのではないか。

○　アウトカムの指標については、社会の状況というものを測定する指標なので、安易に書いてしまって良いのか疑問。

○　例えば、死亡事故とシートベルトの相関関係で言えば、シートベルトを着用することで死亡していた人が怪我にとどまるようになったから死亡事故が減少したのか、シートベルトの着用が安全意識を喚起し、事故自体が減少したから死亡事故が減少したのか、いろいろ考えられる。PDCAで言うところのＣをきちんと行っているか、という指標が必要ではないか。

○　政府、重要インフラ、企業・個人という三つの領域間の指標のずれの調整はどこでなされるのか。企業・個人の方で決めた指標で、政府の方では取っていないものが無いよう、調整する必要がある。

○　目標値の設定については、勇気をもってやらなければならない反面、雑にやると社会に混乱が起こるので、2009年までに値を決めて行けば良いくらいの考えに基づいて決めて行くべきではないか。

○　相関を取ることについて、どのように考えて行くかについては、研究しなければならないところもあるので、事務局に考えさせて欲しい。

○　指標のずれの問題については、事務局として、なるべくそれが無いようにする。
　なお、政府機関との関係では、政府機関がかなり詳細に取れるので、これとの比較を真面目に見て行くと、企業・個人に重すぎる内容となる。また、重要インフラとの関係では、行動計画という形で政策パッケージが組まれているため、進捗管理系の項目が中心になる。そのため、指標のずれが結構出てしまうが、そこは各省庁が的確に関与して行くという前提で動かざるを得ないと事務局では考えている。

○　「インターネットを利用して感じる不安や不満、利用しない理由」がアウトプット指標として指摘されているが、これはアウトカム指標ではないか。

○　外部委託先での情報セキュリティ対策実施状況について、これを特出しして指標を取る必要はないのではないか。

○　アウトカム指標と2009年の「姿」は、かなり密接な関係にあると思う。そうしてみた場合、今回提示されたアウトカム指標は、インシデントや犯罪被害という、特定の側面しか見ていないという気がする。

企業・個人が2009年にどうなっているか、ということについても、アウトカム指標で見るべきではないか。

○　企業や個人等の社会の構成要素が、お互い活動している中でどうなっているのかを見るのが重要ではないか。すなわち、企業間の取引や企業と個人の間の取引が安全に行われるということが「姿」として描かれ、アウトカム指標で評価出来なければいけない。

○　アウトプット指標とアウトカム指標の整理の仕方については、再度整理した方が良いのではないか。

○　外部委託先での情報セキュリティ対策実施状況について、これを特出しして指標を取る必要はないのではないかとの御意見があったが、一つの企業間取引とか、政府と企業間の取引という側面で情報セキュリティを見るという観点からは、必要ではないかと思う。

○　個々の企業や個人がどうなっているかというのと、主体相互間のやりとりの中でどうなっているというのは、別の指標として見るのが良いのではないかと思う。

○　ここで示されている評価指標は、本当に測定したい指標や本来の評価指標を見ることが出来ないので代替的に見るという指標のように、幾つかの種類に分かれる。企業・個人で評価指標とし、政府機関で評価指標としない部分については、どういう理由で評価指標としないのかも含め、指標の位置づけを整理した内容があってもよいのではないか。

○　今回示された評価指標案を基にするのは良いが、網羅性、全体としてこうあるべきで、故にこの評価指標があるべきだというのが必要ではないか。

○　定量化することの出来ない評価指標について、わかるように残しておく必要があるのではないか。

○　目標を定めるべきではないかとの議論があるが、政策目標である世界トップクラスの水準というのはどういう水準なのか、一義にはわからない以上、決められないのではないか。

○　重要インフラは、行動計画という形で政策パッケージが組まれているため、進捗管理系の項目が中心になるとのことであったが、指標の目標値を定めることが非常に難しいことを考えると、企業についても、この方法の方が適しているのではないか。

○　ここで示されている評価指標の数値は、恐らく上昇して行くだけであるので、数値を分析するための考え方がないと、この数値からは何も見えないのではないか。

○　企業が自己採点出来るような分かりやすい指標を立てるべき。余り精緻になってしまうと、企業にはわかりにくいのではないか。

○　政府と企業の関係をみる評価指標は、数値を取ることが出来るかもしれないが、企業間については、データがないという問題がある。政府が持っていないデータまで調べればあるか

もしれないが、どこまで活用して良いのかについては、事務局として御意見を伺いたい。

○　直接指標、代替指標、間接指標といった考え方を明示することについては、事務局として検討する。

○　定量化することの出来ない評価指標について、わかるように残しておく必要があるのではないかということについては、事務局として検討させて欲しい。

○　評価指標の運用に関する議論が出ていないが、事務局の方で分析を実施することを考えている。

ただし、企業・個人の分野については、政府機関ほど詳細なデータがなく、公的な調査結果から本当に知りたい情報を手に入れることが難しい。とすれば、調査を行うか、公的ではない調査結果を用いることになるが、調査を実施することによる企業への負担の問題もあり、事務局としてはためらいがある。

○　政府の企業に対する行動につながる調査であれば、それなりに理解するが、行動につながらない調査では、理解を得られないのではないか。

○　今回の評価指標は、政府の情報セキュリティに関する計画の組み直しに活用する指標であるので、政府の行動に対して影響を及ぼすものである。しかし、企業・個人に対して、政府がどこまで関与出来るかというと、環境整備が中心にならざるを得ない。とすれば、この指標がどこまで政府の企業に対する行動に影響しうるかということに関しては、期待出来ないと事務局では考えている。

○　政府機関については、直接評価指標の数値を取りうるところがあるので、それに基づいて幾つか見て行くのが一つのやり方ではないかと、事務局では考えている。

○　現在、各省庁で取っておられる統計は、情報セキュリティが重要になる前の時代に、行政としてどのような統計を取るかということで考えられたものであるが、これだけ情報セキュリティが重要になってきたことを考えると、統計項目を改め、セキュリティ指標のようなものを入れるくらいの気持ちでやる必要があるのではないか。

○　公的な調査結果から手に入れることが難しい部分は、公的ではない調査結果を併用して行くべき。

○　闇雲に調査をするのでなければ、必要な項目について調査をしても良いのではないか。

○　民間の調査は、回答率が余り高くないという状況があるので、それをどのように分析するかが重要である。

○　現在政府が採用している方法と母集団・サンプリング方法・継続性で合致していると認証出来る調査を取り込めば、採りうる評価指標の範囲が広まるのではないか。

○　インターネットの調査は機動性があるので、紙による調査と併用して用いることも考えて行くべきではないか。

○　企業・個人については、強制力をもって行動を制御することが出来ないことに留意する必要があり、そこを忘れた議論に意味はないと思う。指標を詳細に取れれば良いのかもしれないが、政府の行うべきは、企業・個人が自らセキュリティ対策を取って行くように促すことではないか。
　とすれば、いたずらに指標を取ることは、意味がないのではないか。

○　分析した結果をどのように行動に結びつけるのか、対象が企業の場合、分析と行動の間に溝があるように思う。

○　統計については、政府統計に固執する必要はない。一定の水準に達している統計であれば、取り入れても構わないのではないか。

○　大学については、企業と同じように考えた方が、評価指標となる統計などもあるのではないか。

○　経済産業省の情報処理実態調査では、教育機関も対象に含まれているが、国公立は除かれている。また、日本標準産業分類に基づいているので、「教育機関（国公立を除く）及び学習支援業」で一つのカテゴリとなっている。

○　国立大学については、調査が度々来ているので、統計は存在すると思う。公立大学については、多分わからないのではないか。

○　「質の高い情報セキュリティ関連製品及びサービスの提供促進」に関連し、例えば、情報セキュリティ対策装置又は情報セキュリティが確保された情報システム投資に対する税制優遇措置適用状況等について、取れるような指標がないか、事務局として悩んでいる。

○　「コンピュータウィルスや脆弱性等に早期に対応するための体制の強化」については、JPCERT/CCや早期警戒パートナーシップ体制に参加している組織数くらいなら出せると思うが、その他の評価指標が何かないか。

○　アウトプット指標とアウトカム指標の整理に関連して、例えば「個人が負担感なく情報関連製品・サービスを利用できる環境整備」について、セキュア・ジャパン2006では、IPv6に関する事業などが施策として盛り込まれているが、例えばそういう施策をやっている中味を書くのがアウトプットだと割り切り、その結果として世の中がどうなったのかというのをアウトカムだとして行くのも一つの方法だと思う。そうしないと、なかなか答えにくい。
　そのような観点で、アウトプット指標とアウトカム指標を整理して欲しい。

(5)　今後の予定について

○　事務局から説明