高度情報通信ネットワーク社会推進戦略本部情報セキュリティ政策会議
政府機関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 10 月 23 日（月）　13 時 15 分～15 時 15 分

２．場　所

内閣府別館会議室

３．出席者

【委　員】

榎木　千昭　委員	（KPMG ビジネスアシュアランス株式会社執行役員）
大木　栄二郎　委員	（工学院大学教授）
多賀谷　一照　委員	（千葉大学教授）
谷口　博一　委員	（監査法人トーマツ代表参与）
冨士原　裕文　委員	（富士通株式会社コーポレートＩＴ推進本部 fujitsu.com 室長）
満塩　尚史　委員	（環境省 CIO 補佐官）
山岡　正輝　委員	（株式会社 NTT データ情報セキュリティ推進室長）
山岸　行弘　委員	（金融庁 CIO 補佐官）
山田　真貴子　委員	（世田谷区助役）

（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
警察庁情報通信局情報管理課長
防衛庁運用企画局情報通信・研究課情報保証室長
総務省大臣官房企画課情報システム室長
総務省行政管理局管理官（情報担当）
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)　政府機関における情報セキュリティ対策の評価指標について

○　事務局より説明

(2)　自由討議

○　前回の説明では Act に対する評価の視点とあったが、今回の説明では Check の

ところの指標となっているのは、どのような経緯なのか。

○　Act とは Check で出た結果がアクションに繋がるかであり、その部分がきちんと回っているかを見るためにマネジメント指標を取り入れた。Check の部分は、定量的な対策実施指標で見て、Act の部分はマネジメント指標で見ていく。

○　マネジメント指標として、やるべきことがやられているのか、組織があるのかなどが挙がっているが、肝心のリスク認識が変化したのかをどう評価するのか。

OECD のセキュリティガイドラインの design and implementation の視点でいくと、政府機関統一基準の要求に応じて、どのように設計し、実装したかを見る指標が必要ではないか。

政府機関から外に出る取組の評価が見やすいので、例えば外部委託を見るとわかりやすいのではないか。

○　各府省庁には、自主的に情報セキュリティ対策を設計し、実装するだけの能力や時間、人員に余裕がない。そこで、多くの場合は、府省庁間で業務及びリスク認識の点である程度の共通部分があると考え、すぐに現場で適用できるよう統一的な方法を内閣官房から示して対策を実施させている状況がある。

主体間の取組を測ることは、個人・企業評価指標専門委員会でも議論があり、外部委託も含めて、事務局として検討をしていきたい。

○　もし、政府機関が民間企業にとって模範にすべきセキュリティ管理のレベルまで出来ていると考えるならば、政府機関は、３年後を視野に入れて、新しい技術等でシステムについて民間企業が目指すべきレベルに向かっていくような評価指標が必要でないか。

○　政府機関統一基準は各府省庁の最低限を規定し、底上げを図るための基準であるが、これが徹底されて一定水準まで来さえすれば、新しい取組を少しずつ基準の中に入れていくことで底上げをしていくということが可能になる。現状を考えると、一番高いものを指定する基準ではなく、必ずやらなければならないレベルを規定する基準になっているので、今は評価指標もそれに合わせ、最低限のチェックにならざるを得ない。

○　各府省庁が独自に PDCA を回す視点と政府全体で PDCA を回す視点があり、各府省庁は今の統一基準を基にチェックすると思うが、政府全体の評価指標としたときには、現在の統一基準しか見ていない評価指標でよいのか。

○　政府全体の指標設定として、電子政府を安全に利用するとの達成目標に対して、実際に具体的な評価をどうしていくかと言うと、非常にギャップが大きい。実際に取組を促進していくには、具体的に道具がないと動いていかないので、道具と

しての政府機関統一基準に忠実に評価指標を作成している。

○　底上げの道具は重要だが、皆が 80、90 点を取れる指標だけでなく、今年は 50、60 でも 3 年後に 100 点になるような指標があるべきだろう。

○　重点検査の結果報告でも、基本遵守事項以外に強化遵守事項を一部入れただけで、政府機関内で非常に不満があった。政府機関にとっては、やるべきことが 100 点でないことが最も受け入れがたいことである。政府機関統一基準では、今後やるべきことを強化遵守事項として織り込んで、今後徐々に基本遵守事項とすることで、なかなか 100 点にはならない仕組みがあると考えている。ただ、対策実施状況以外にも、マネジメントにおいて様々な見方があるのではないかと考えて、マネジメント指標を入れている。

○　評価指標が暫定版であるとすれば、評価指標の 2007 年度版などとして途中であることを示すことはいかがか。

○　表示するかは悩ましいが、基準が変われば、それに対抗する評価指標は変わらざるを得ない。

○　評価指標の全体枠組みが見えないのでこれで十分かが分からず、これで終わりと一人歩きするのが恐い。統一基準で、評価の方法として「リスクに応じて適切であること」も監査で確認しろとあるが、そことの関係が曖昧になる。

○　7 月報告の重点検査で 100 点でなければとの意識は、職員にもあったが、新聞や世の中の論調としても出ていたのが事実である。そのため、状況をみて段階的に基準を上げていくのが現実的であると考える。

○　評価は、マネジメント指標と対策実施指標を合わせていくことを考えており、対策実施指標は政府機関統一基準に沿って約 300 の遵守事項をいくつにカテゴライズして、いくつかの重要と思われる指標を総合的に用いることを想定している。

○　外部委託はマネジメント指標で出てこなくても対策実施指標に含まれており、マネジメント指標の中にも統一基準の遵守事項が一部含まれているので、バランスを見ないと行けない。

　情報システムの一元的な把握はできていないことが実態の認識であると思うが、PMO が各府省庁で立ち上がって把握できるようになってきているので、そことセキュリティマネジメントの関係を盛り込むべき。

○　各府省庁の規模、職員数、地方部局の有無、持っている文化等により応じていろいろなポイントがあるので、評価する際には、一律に実施の有無だけでなく、

自府省庁では独自の取組でマネジメントを上げているというものがあれば、アンケートかヒアリングなどを通じて収集してよければ評価のポイントとする。また、ここで挙がってきたプラクティスを政府全体でベストプラクティス集として各府省庁にフィードバックすることも想定している。

○　マネジメントを測る際に有効であるかなどはセルフアセスメントでは厳しく、ある程度客観的に評価できる部分があると使いやすい。

○　定性的な指標は、なるべく外から分かるもので整理しているが、具体的に聞かないと効果的であるかどうかわからないものもあるだろう。評価の視点は広げすぎず、まずは絞って該当することがあるかどうか、それに類する取組をしていればどのような努力をしているかを聞いていきたい。

○　府省庁の評価でどのような課題が挙がり、どのような改善を行い、どのくらいよくなったのかを見るような評価指標を含むべき。

○　「組織」の「評価の実施」の観点で、自己点検の回収率や計画の有無、監査報告書を単に提出だけでなく最高情報セキュリティ責任者に説明しているかなどを聞いており、そこで指摘されて事項がちゃんと対応されたかどうかを確認していくことも有り得るのではないか。

○　マネジメント指標の評価に関して、組織が実効的に動いており三つ星であるときに、意識が二つ星になることがあるのか。それぞれ相互の関連性はあるのか。

○　マネジメント指標の評価の観点の関連性は見てはいない。ただ、マネジメントが三つ星でも、対策実施指標がＣという場合も有り得ると思う。この場合、実施は予算の問題等で時間もかかるが、マネジメントができていれば自ずと対策は進むだろうと思う。

○　モニタリング（評価の実施）の項目は「組織」の観点の中に入っていて、教育は「組織」の外で「意識」の観点として出ているので、相互の関連性が気になる。「組織」に自己点検を含むか、それともにシンプルに組織の事だけ聞くのかの整理が必要ではないか。

○　各指標が適正であるにもかかわらず、まだ達成していないと見えると困るので、星幾つではなく、評価主旨を文章で付けるものではないかと考える。

○　記号をどうするかもあるが、評価の内容について、前回は結果の表だけが一人歩きしたように見えたので、プレスリリース等も含めてちゃんと説明していくことが重要ではないか。また、全部が 100 点でなければならないというのはセキュ

ティの専門の立場からは望ましくないと考えている。

○　まず、評価結果を外部にどう公開していくのか、リスクはどこまでオープンにしていくのか。単純化しすぎても意味がないのではないか。また、各指標間の連関性はあるのでないか。これが駄目だと意味がないとか、指標の重み付けはされるのか。更に、ベタープラクティスも併せて公表すれば、より生産的な評価になるのではないか。

○　まず、公表のルールだが、7 月 25 日の重点検査の公表は、リスクが高まる方向の情報は開示しないこと、比較性とわかりやすさを維持すること、事前の評価の構造を十分に説明することを考慮している。プレスには別途説明の場を設け、説明している。細かい中身に関しても、各府省庁に対して一方的な評価ではなく、やりとりして評価した。

○　ご参考だが、企業に対する情報セキュリティガバナンスのときも似たような議論があり、しっかりやっているものを 4 点とする 4 点満点で当初考えていたが、他の模範となる取組やっているものを 5 点とした。委員から指摘があったのは、そのようにしておかないと対策が先に進まないのではないかということであった。

○　国民が見てどう思うか。評価 A を受けた後に事故があると、期待が裏切られた感じがある。国家目標を併せて指標として入れていくべき。

○　対策実施指標の組み方は、容易には 100 点満点をとれるようには作られていない。マネジメント側については、プラクティスの高いものとして取り出せるものをやっているところを褒めていきたい。マネジメント指標は、普通だと一つ星しかとれないが、頑張っているところには三つ星つけてあげたいと思って作っている。高みを狙っていくという意味では、例えば、必須以外のプラスαの部分をどこまでやっているかを評価していくことになるが、現実は難しいと考える。

○　リスクに応じてやりなさいと言っているのであれば、それをどの程度やっているかを評価すべき。

○　なかなか悩ましい話だが、国土交通省において、河川などの営造物の管理をする際には、リスクを前提とする。５０年に１度、１００年に１度、１０００年に１度、どの程度のリスクを目標として、どの程度投資するか。どういうリスクに対して 100 点なのかある程度示す必要がある。

○　リスク評価の観点は考慮いただきたい。例えば、スタンドアローンとネットワークのパソコンで、パッチ当て等について同じような評価をされているのが現状

である。

○　スタンドアローンだからリスクが低いというわけではない。運用状況によって決まってくると考える。

○　各府省庁の評価に加えて、更に政府全体の改善の中で評価して外に説明していくべき。各府省庁の評価と政府全体としての評価の指標は少し違う。政府全体としてレベルをどう上げていくかは、政府全体としての改善に含めるべきである。
　強化遵守事項等は、評価の対象ではなく調査の対象であり、政府全体的な評価でフォローすべきではないか。地方支分部局等は、本省と含めた単純な１つの評価ではなく、分けて考えていくことでよいと思うが、府省庁側で作業する時間が問題である。

○　強化遵守事項については、将来、統一基準を見直しする際に各省の状況を把握する観点で調べる必要はあると思うが、評価という観点から対象とするのはなじまないのではないか。項目をどこまでとるかは時間を踏まえて考えたい。

○　強化遵守事項の実装は、各府省庁で判断すべきと思う。現場で必要でないと判断したのか、必要と判断していないからやっていないのかが問題で、それを把握することを何かの形で取り組んでほしい。

○　セキュリティポリシーや手順書をつくる際に、それぞれのシステムのセキュリティ度合いをちゃんと検討した上で入れているのであれば、規程に検討した上で入れているかの結果でわかるだろう。ただ、個々のシステムにどの対策を入れているかまでの調査は難しい。

○　強化遵守事項については、各府省庁で判断。仮に事故が起きた時の責任は、各府省庁にあり、NISC としても間接的に疑義がある場合に、再考を求めるような仕組みになると考える。

○　評価のところでも、監査の結果に基づいて、改善計画をたてて、リンクさせているかなど、改善に繋がる指標は入れてもいいかと考える。評価に留まらず、改善にどうつなげているかを評価したらよい。

○　定量的指標で気になる点がいくつかある。セキュリティ委員会の開催回数やセキュリティ担当者の職員数に対する比率、経験年数については適正値をどのように測るのか。単に有無でよいのではないか。自己点検の回収率は規則で実施すれば、病欠・出張者を除き 100％近くなるはず。e-learning は印刷教材で実施している場合はどのように評価されるのか気になる。例外措置の経年変化については、経年で減らない可能性もあり、申請件数と許可件数で見てよいのか。

○　地に足をつけた議論がある一方で、方針としては世界最高水準を達成するということがある。世界最高水準と言っている中身、2009 年に統一基準をそのレベルまで持って行くか、そのレベルが何を表しているかというのが一つの大きな議論。リスクへの対応の仕方なり、プロセスが洗練されているとか、全員に徹底されている網羅性がどうかとか、何のレベルを上げていくのかの考え方を事務局から示して欲しい。

○　世界一レベルをどう捉えるか書けるのか。何を持って一番とするか難しいし、一番をどうやって説明するか非常に難しいので、どうしても書くのだとすれば、「世界の模範となるべき」として、それはどういうのかを書くべきか。

○　全体のフレームワークとして、ここ数年間で、全体の仮説があって、その中でこういうことをやっているとか、わかりやすく説明していくのではないか。

○　情報セキュリティは格好いい施策も大切だが、簡単なことを 100%徹底できるかについてうまく評価できないか。

○　最初から問題になっている世界最高水準の話が気になる。世界最高水準については二つ大きな軸があると考える。一つが、セキュリティレベルで、高いハイレベルなものを実装すること。もう一方は、情報システムの品質であり、すべての情報システムでできているかの観点で世界最高レベルというものもあると考える。政府全体としてハイレベルなものを実装しますというのは違う話と考えるが、品質は、政府全体としては必要だと、姿を書くにあたっては思っている。世界最高水準という表現はやめた方がよい。

　各主体全体をまとめる観点では、政府は政府機関統一基準という道具を作り上げて、底上げをやってきているのに対して、民間では ISMS など違う仕組みで来ているのだから、全体構造として、政府と民間は違った取り扱いをすべき。

○　民間企業にとっては、情報セキュリティというと、顧客の目が気になるように、政府にとっては、国民の目なのだろう。そうすると、評価は、国民にとってわかりやすい指標や、政府機関が情報セキュリティに関してこんなに変わったなどの指標が大事。また、事故に対する分析がきちんとやられているかどうかについて、あまり伝わってこなかったので不安に思っている。

○　全体としては、政府機関統一基準も ISMS も同様の取組であるため、政府、企業・個人がそれぞれ実施するメタ構造として、総合的に日本全体のセキュリティレベルを上げていくというまとめ方はあると思う。

　情報セキュリティでは教育や人の問題が重要。政府機関は、情報システムや予算、地方支部局等に課題はあるが、政府職員の 100 点をとるように頑張るという

ところは、民間の模範となる要素もあるのではないか。模範となるようなセキュリティレベルに 2009 年までに上げると謳ってもいいのでは。

○　ここで提示される指標は、日本における情報セキュリティの一つの目標なり、模範なり、あるいは標準になっていくと考える。自治体は国の動きをウォッチして、自分たちの行動を決めていくところもあり、対策実施状況は機関によって異なると思うが、せめてマネジメント指標については、国がやっているというのがわかるような形でまとめていただきたい。セキュリティレベルを上げる契機になると思うので、地方がやる気が出るような指標にしていただきたい。

○　国のシステムなので、単なる努力目標ではなく、アウトプットは 100%やるべき。一方で、アウトカムというか、どこまでのリスクに耐えうるのかについては、100%やるというのは土台無理な話というのは正直に書かなければならない。アウトカムとしてのリスクに対して、どう迅速に対応するか、脆弱性情報に対して行き渡らせるかなど、対応体制のレベルを上げることによって、世界に誇れるような、一定以上のレベルの体制にしていくべきと思う。

(3) 今後のスケジュール

○　事務局より説明