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４回会合議事要旨

１．日　時

平成 18 年 10 月 31 日（火）　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）

（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

○　「２００９年時のあるべき姿（政府機関）」において、先進的技術導入の観点が入ったことはよい。
　政府機関評価指標（マネジメント指標）において、外部委託には政府機関内部の取組と政府機関と外部の断面の取組とがあり、先端的技術の観点を入れると、政府が外部から調達する機器等についてセキュリティを考慮しているかの指標があるとよい。また、委託先管理の定性的指標について、政府機関統一基準 6.1.2(2)の委託先への徹底が参照されているが、(1)の委託先の選定基準や手続きの整備の視点の方が、客観的な評価がしやすいのではないか。

○　統一基準上は外部委託先に対策を徹底することがあり、その有無を聞き、更にプラスαとして評価するために、個々の取組ではなく府省庁全体の仕組みとして、契約書の雛形等で対策について具体的に含めているかを調べていきたい。

○　外部委託の観点は、マネジメントの基準なので、委託先の管理について、その規程があるかどうかだけでなく、選定の仕組みが実効的になされているかについてみるとすると、政府機関評価指標（マネジメント指標）において「規程」ではなく「組織」に分類されるであろう。

○　調達仕様に記載するとあるので、請負業者に関する要件はそこでみればよく、統一基準の基準項目の方は、6.1.2(1)まで含めておいた方がよいのではないか。
　「２００９年時のあるべき姿（政府機関）」において、ただし書きの中で危機管理対応が記載されているが、PDCA サイクルを考えたときに問題が起こらないとは言い切れないので、そのときの対応までを１項目として書き込むべきである。
　政府機関評価指標（マネジメント指標）のうち、資産管理台帳は PMO 自体が整備するので、その中にセキュリティに関する項目の整備状況が書かれているかとした方がよい。

○　政府機関の緊急時対応能力強化については、第１次情報セキュリティ基本計画に盛り込まれており、「２００９年時のあるべき姿（政府機関）」に書き込むこと考えている。また、政府機関内における人材育成についても、別途専門委員会で検討しており、その姿を書き込むことと考えている。

○　緊急対応能力は、各機関がそれぞれ持つのか、横断的に対応する仕組みを作るということか。

○　各府省庁がそれなりの対応能力をもつこともあるが、政府全体として能力開発ができているかどうか、また緊急対応が起きた場合にその知見が各府省庁にフィードバックされ、政府機関統一基準に反映されるかどうかであり、平時と緊急時の対応が有機的に結合している状態ができあがることが最終的な書きぶりになるだろう。

○　委託管理について、当初はマネジメント指標の中にあり、それが定量的評価の項目で測れるのでないかとの説明でマネジメント指標から消えたが、またマネジメント指標に復活した。対策実施状況の評価では、「基本遵守事項３４６項目の中でも重要な項目に着目」とあるが、どのように重要な項目が決まるのか。

○　外部委託については、政府機関統一基準 6.1.2 にいくつか項目があり、表面的に YES か NO できくことができる。ただし、表面上は規程に盛り込んでいるとしても、どのくらい具体的に実施されているかは分からないので、手順書を見たり、ディスカッションすること等により実態をみることができると考えて、マネジメントの評価ポイントとした。

○　政府全体の PDCA において、政府機関統一基準２００５年１２月版の基本遵守事項が適切かどうかの評価がなされると思うが、その結果をどのように反映していくのか。

○　政府全体のサイクルとしては、情報セキュリティ対策マネジメントのサイクルと政策・施策のサイクルがある。対策については、評価結果と外部要件の変化を踏まえて、政府機関統一基準の見直しを緊急時も含めて最低年１回はすることになっている。施策について、小さい流れとしては、実施計画であるセキュア・ジャパン２００７を作るときに２００６年度の実施上の評価を基に NISC でとりまとめ、大きな流れとしては、３年間の基本計画を定めているので、その中で戦略を変えていくこととなる。その大小のサイクルを複合的に回していく際に、この評価指標を使っていく。

○　「２００９年時のあるべき姿（政府機関）」では、まだ十分であると言えない部分が存在しているとして２つ挙げたうち、「政府機関統一基準よりも高い対策水準が求められる情報システム」は、文脈からすると、２００９年に世界最高水準に至っていないと読めるので、誤解のないように表現を修正すべき。

○　ご指摘の記載については、底上げの基準として満たしているものが世界最高水準であるが、それよりも高い対策水準が求められる情報システムは存在するので、そこを区別する意図であるが、誤解をされないように書きぶりを検討する。

○　平成１８年度重点検査で利用した指標とその他の候補を挙げ、実現可能な調査方法を含め検討とあるが、どのように重要な項目を拾うのか。

○　重要な項目をどのように拾うかについて、統一基準で様々な項目があるが、評価に当たって、例えば、端末・ウェブ等の技術、物理的な対策の観点は数値を取ることができるが、情報の取扱いなどの職員一人ひとりの取組みをみるようなも

のはどの程度画一的に数値が上がっていくのか難しい面もあり、どのような項目が画一的に数値が上がってくるのかについて考えた上で、その中から重要な項目を候補に挙げていきたい。

○　重要な項目については、時事的なものとスナップショットの２つがある。端末・ウェブの重点検査はスナップショットだが、７月の政策会議で報告した Winny に関する事案に基づく調査は緊急対策的なものもあり、センターの知恵を使ってやっていきたい。

○　「２００９年時のあるべき姿（政府機関）」の他のマネジメント・システムとの整合的な運用については、星３つの評価に該当するとの理解でよいか。また、業務のマネジメント・システムと情報セキュリティのマネジメント・システムでは軸が異なると思うが、評価するに当たり整合的な運用とは具体的にどのような状況なのか。

○　ご指摘のとおり、マネジメント指標が星３つになっている状態を示している。その際に、整合的な運用であるとは、一般に情報セキュリティ対策が向上していくと職員にとっては不便になるが､決まりだからと敢えて対策をするのではなく、仕事のプロセスの中に流れとして情報セキュリティ対策が織り込まれることが理想である。それが、どの部分で実施されているかの事例を集めていきたい。

○　星３つの状態とは、セキュリティ対策をとった場合に、一時的には業務全体の効率性はほっておけばレベルダウンするが、上手く仕組むことにより効率性が対策前と同等に保たれることであると考えるが、これをマネジメント指標で取ることは難しいのではないか。セキュリティ対策は１回対応しただけで終わりではないので、新たなセキュリティ対策をとったときに、業務が止まらないような柔軟なシステムになっているかの評価に繋がるのではないか。

○　マネジメント・システムには、一般的な用語の意味と、品質や環境に関するものの意味の２つがある。民間でマネジメント・システムの統合という場合には、品質とセキュリティをどう統合するかを示すことが多いので、用語の使い方を変えたらどうか。業務との整合性について記載しているのであれば、マネジメント・システムという用語を使わなくてもよいのではないか。

○　政府機関において、ＩＴマネジメント・システムという概念は入ってきている。PMO にも触れられているので意味は通っているが、やや意味する範囲が狭くなる。そこで、業務とＩＴマネジメント・システムと併記するのはいかがか。

○　民間ではプロダクトマネジメントという概念があるが、政府でもコストマネジメントの考えが入ってきており、電子政府の方ではその話が出てきている。政府

機関でも単なる業務だけでなく行政サービスとしての品質管理に段々踏み込んできている。そのため、マネジメント・システムという表現を完全否定することではない。

○　「府省庁内のその他のマネジメント・システム」という記載があるので、その他の中身の例示をいくつか書き込んだらよいのではないか。

○　政府機関評価指標（マネジメント指標）で、「例外の認識」を「意識」の観点に入れているが、ルールが遵守できないときに例外措置として、審査手続きや記録の整備をきいているので、「規程」に入れた方がよいと思う。

○　政府機関評価指標（マネジメント指標）の左側の分類については分かりやすく再考をさせてほしい。

○　各論整理において、ｉ）のマネジメント指標とⅱ）の対策実施指標は、ⅲ）の効果の評価の代替指標ではなく、本来は事故率とか稼働率とか情報セキュリティ水準を評価する指標があるはずだが、本来の状態を計測できないので代替指標として対策やマネジメントをみていると明確に書くべき。

○　一般的に、情報セキュリティ水準の高さは、情報セキュリティマネジメントと情報資産の把握状況と運用状況、それに対する事故・障害の発生状況をみることであり、事故発生率だけが指標ではない。指標全般の観点からは、資産管理の状況、運用の状況を測ることはやり得ることだが、非常に負担であるので、実施のところをみることにしている。

○　実施率について、対策とはリスクの低減であり、リスクとは確率の問題であるため、１００％と９９％の差の意味は大してないにもかかわらず、ＡとＢに評価が分かれている。例えば、１００％対策したからといって、セキュリティホールは次から次に出てきて、リスクが０になるわけではなく、９９％と分けることの意味が疑問である。
　いずれ各府省庁に意見照会があるとの認識でよいか。

○　最終的には、この指標でやるということを各府省庁に意見照会することにしている。

○　医療でやられているように、重大な事故だけでなくヒヤリ事故をサンプルで集めることにより、対策にどのような欠陥があるかを逆に推計してリスクを低減することが有り得るが、この情報セキュリティ対策の仕組みには組み込まれているのか。

○　それは、政府機関統一基準を決めるプロセスの中で織り込んでいる。行政組織だけでなく一般的な組織から分かっている知見を踏まえていることと、行政組織に特有な部分も盛り込んでいること、最低ラインを提示しているとの３つの条件から、専門家と各府省庁の実態調査のフィードバックによって組み込めると考えている。

○　ヒヤリ事故からの知見は、対策基準の見直しで反映され、その新しい基準でマネジメントを回していくとの仕組みになっている。

○　評価を受ける側は予算に縛られているので、情報セキュリティを際限なく上げられるわけではない。数年間での目標を示してもらい、その達成度で評価することはできないか。調査をする前には客観的な物差しを提示し、どの府省庁も最終的な１００点を取れるロードマップをひいてほしい。また、マネジメント指標の解釈については、各府省庁でマネジメントの考え方いろいろあるので、NISC で一意的に決めずに各府省庁の事情を踏まえてほしい。

○　毎年の評価であれば、経年度的な評価をコメントでもよいので入れることはできないか。マネジメント指標でも伸びたところは評価してもよいのではないか。一律的な指標を明確に示す必要は無いと思うが、経年度的なことを考慮することはあるとよい。

○　予算システムとの関係で、今後どこをやるかのロードマップを示してほしいとの指摘について、理解いただきたい点は、現状は最低水準の遵守事項であり、実施状況の中ですべてをやるべきとの考えに基づいているので、重点検査についてテーマを示すことはあっても、対策を実施していく上で免罪符を与えるような部分を示すことはできない。どのようにマネジメントしていくかは、各府省庁がそれぞれ責任を持って考え方を示してくれたらよいと思う。経年変化のコメントや観察結果は当然出てくるだろう。

○　事故については統計的有意性に難点とあるということだが、「２００９年時のあるべき姿（政府機関）」において、電子政府の安全性・信頼性に大きな疑問が呈されるような事態は特段見られないというのであれば、特段見られていないことをどこかで評価する必要があると考えるが、統計的に把握できないとの整合性を教えてほしい。また、企業・個人の評価指標専門委員会で事故件数をとっているが、こちらも統計的有意性がないのか。

○　統計的有意性については、新聞に出るような大きな事故は外から分かるが、FAX・メールの送信ミスのような細かいレベルのセキュリティ事故までを各府省庁でどのように把握しているかが分からない状況で、外に出てくる結果だけで府省庁間の評価は難しいのではないか。政府全体としてマクロでみてアウトカムの中で

とることは有り得るが、各府省庁で比較のポイントとなるのは適切ではないのではないか。

○　各府省庁の比較を言っているわけではない。細かい事故をどのように把握しているかでバラツキがあるのであれば、データの根っこをみてみる必要があるが、それは企業・個人評価指標専門委員会の検討でも同様の問題があるのではないか。事務局として見解は統一してほしい。

○　経年の議論があったが対策基準の見直しがあり、マネジメント指標と対策指標でも時系列的に食い違いがでるかもしれない。また、府省庁の場合は単年度予算であるため対策が一年遅れになり、頻繁に手直しをする状況に陥るのではないか。

○　安全を管理するとは、ある日やったことがそのまま通用するのではなく、こまめに直していくことで一定の基準を維持することであるため、経常的な見直しが必要である。ただ、予算は１年以上の遅れがあるので、そこは配慮が必要である。
　指標が変化することについて、ある程度許容してもらう面と、ベースでみていく面の両方をみていくことがある。したがって、評価指標を一定にするために、基本遵守事項や検査方法を変えられないというのはよくない。

○　「２００９年時のあるべき姿（政府機関）」において、諸外国の政府機関にとっても模範となるような水準というのであれば、NISC が設定した水準が現在として妥当であったのかの評価を捉えておかないとまずいのではないか。

○　定性的な表現になると思うが、現在の統一基準で何を求めていて、どのようなレベルにあるのかなどの設計コンセプトを示していき、次の改訂のときも何が変わるのかを示し、パブリックコメントを取らざるを得ない領域である。設計コンセプトの見直しと展開という形の文書を NISC としてしっかり出していきたい。

○　評価がどれだけ根拠のあるしっかりしたものであるか、各府省庁が気にするのは当然であるが、NISC は各府省庁の対策の効果について完璧には知り得ないので、便宜的な指標をもってそれに近づくように努力する。それで一応の結論を得て、公表や各府省庁と相談をして今後の対策のために上手く使っていくものであり、評価指標はその趣旨を理解して有効に使っていくことが目的である。

○　ISMS では、最初に情報資産を洗い出し、そのリスク分析をし、評価して、対策を立てることが一つのステップであるが、今回のマネジメント指標ではどのような考え方なのか。

○　各府省庁で基本となるリスクは変わらないと考えて、その共通認識のところは NISC が責任をもって実施し、今の政府間統一基準を作っている。ただ、各府省庁

で特別な業務、事情があり、リスクが変化している場合には、追加的なリスク分析と対応措置が各府省庁で必要な部分についてはおこなわれる。完全に業務や情報の取扱いが異なる場合には、政府機関統一基準に乗らないということも有り得るが、結果的に組織全体として大きく外れているところはない。

○　評価の結果を公表する際には、特に情報セキュリティ対策実施状況の指標において、大きなレベルで公表するのはよいが、どこまで公表されるかによっては、新たな脅威になることもあり得るので、よく配慮していただきたい。

○　政府全体としては情報システムに共通性があるとの考えであるが、それでも個別に特殊なリスクが発生している場合には、そのリスクから対策をどうするかは各府省庁の責任で洗い出すことになる。しかし、その対策は NISC が全体としてとる情報セキュリティ対策とは衝突しないと思う。今後問題となるのは、ヒヤリ事故的なものを府省庁間で情報交換して、それに対する対策をとれるかがこの基準やシステムの実効性にかかってくると思う。ある程度共通と考えて、情報の相互提供をしていかないと上手くいかないのではと考えている。

○　ヒヤリ事故の反映については、各府省庁間で直接情報流通していく方法と、NISC が情報を集約して基準等に展開していく方法があり、後者の方がハードルが低く現実的なので頑張っていきたい。
　各府省庁で特殊性があるところについては、より高い情報セキュリティマネジメントレベルが求められる状況にあり、政府機関統一基準で要求している対策が、やり方は別として、意味としては矛盾することはかなり少ないと考えており、独自の追加的な対応を実施し、説明責任が果たせるのであればよいのではないか。

○　NISC がおこなったリスク分析や政府機関統一基準の作成は、各府省庁が負うべきリスク対応責任を NISC が変わって背負ったのではなく、想定したリスク分析をした統一基準でよいかどうか、主体的に判断するのは各府省庁の責任である。だから、府省庁の異なるリスクについては、府省庁の責任において個別にリスク分析を行なえばよいというのが基本的スタンスであると思う。

○　１点危惧しているのは、そのときの説明責任を果たすメカニズムを各府省庁が用意して、説明責任を果たせるかどうかである。統一基準から離脱するのは構わないが、きちんと説明責任を果たすということを決めておかないと、これは実効性がない取組になってしまい、再び、各府省庁で何が起こっているか分からない状況に戻ってしまう。

○　国全体のリスクマネジメントや効率性の観点から、一つの府省庁が全部丸抱えで NISC とは別の基準でやるより、できるだけ特殊性のある部門を絞って、十分な説明責任を果たした上で特別扱いをし、それ以外の一般事務的な部分について

は統一基準で行くべきであると思う。

(3)今後のスケジュール

○　事務局より説明