

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1回会合議事要旨

1. 日 時

平成18年9月20日(水) 10時00分～12時00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)
富士原 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)
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. 議事要旨

(1) 内閣官房情報セキュリティセンター長挨拶

(2) 各委員の紹介と委員長を選出

○ 多賀谷委員を委員長に選出

- (3) 多賀谷委員長挨拶
- (4) 会議の公開等について
 - 事務局より資料3について説明、案のとおり了承
- (5) 政府機関の情報セキュリティ対策の枠組み
 - 事務局より資料4に沿って説明
- (6) 政府機関の情報セキュリティ対策の現状と課題
 - 事務局より資料5に沿って説明
- (7) 民間企業の取組紹介
 - 山岡委員、富士原委員より説明
- (8) 自由討議
 - まず今回の専門委員会で検討するに当たり、その目標を確認したい。政府機関は、2009年に世界最高水準の情報セキュリティ対策を行うことをチャレンジ目標としているが、世界最高水準になっているかどうかをどうやって評価するかが一番大きな命題ではないか。
 - 今回の説明では、組織における情報セキュリティマネジメントに関する内容が中心であったが、そもそも政府機関の対策水準がいいのかどうか、政府機関の幹部が国民や利害関係者にきちんと説明できるのかどうか、情報セキュリティ対策の水準が諸外国と比較して妥当なのか、中で使われている技術が有効かなど、評価の対象を広げるべきではないかと考える。
 - 政府機関は企業や個人に対して模範として、取り組むべき形を示すべきである。
 - これまでの情報セキュリティ対策は、欧米を見習っていくキャッチアップ型であったが、日本が世界最高水準を目指すのであれば、今後はリーダーとなるような観点が必要ではないか。
 - 既に政府機関統一基準があるところで、各省庁はどのように実施しているのかの仕組みを評価するのか、あるいは、基準の内容そのものや、もっと大上段の政府全体の取り組みの評価と捉えるべきか、評価の対象をどこにするのか。
 - 評価には、対策実施の仕組みやマネジメントそのものを評価することと、マネジメントシステムや情報セキュリティ対策が有効なのかどうかという有効性を評

価することの2つがあるが、どちらかはっきりすべき。

個人的には、対策の有効性そのものの評価は非常に難しいので、仕組みの評価を細かくやっていたら、有効性もその中に見えてくるのではないかと。

- まずは政府機関統一基準のマネジメントのうち Act の議論を行いつつ、政府機関として2009年の姿としてどうなっていくべきかについても、次のステップとして議論をしたい。
- 対策基準の水準の妥当性を検討すべきという意見もあると思うが、今回の検討の対象は、政府機関統一基準に関する具体的な評価指標の部分としたい。
- 対策の有効性については、議論をしたいところだが非常に難しいので、まずはマネジメントの部分を精緻に攻めてみることを今回考えている。なお、有効性を測るいい手法なり、いい経験があるのであれば、活用したい。
- 有効性の評価というのはアウトカムをどうするかという話であり、マネジメントの中でも政府機関統一基準を全て横並びで網羅的にみるのではなく、その中でもメリハリをつけてみるべきポイントを絞る作業が必要ではないか。
- 対策の実施率を前提に考えているようだが、100%であればよいのか、全部やっ
ていなくても、やっている内容が良ければよくて、いろんな形の評価もありうる
のではないかと。政府の中でどういう対策ができていけば世界最高水準なのか見な
がら、Act を見ていくべきではないか。
- 実施率は最初の評価の取っ掛かりとして有効なものであり、次のステップとし
てマネジメントシステムの視点での評価をこれから取り入れようとしているとい
うことだと考える。例えば、教育であれば、どういう教育をやっていけば有効性
を高めることができるについて、e-learning 活用とか時間数という形で分解してい
き、他の視点のところでもそういう形でやっていけば、有効性も推論できると考
える。
- 政府機関の現状としては、能力のある人材が不足しているために、単純な指標
を定めればそれに応じて頑張れるが、各府省庁でカスタマイズしてやりなさいと
言ってもできないので、入り口はシンプルな形でやりたい。今のところ実施率で
見ているが、これがベストとは思っていない。本来、世界最高水準に合うように
指標をはめていくのが一番いいわけで、有効性を高めるためのラウンドをどうや
って回していくかということであり、その意味で実施率は平板な指標であるとは
認識している。

- 民間企業における「逸脱管理」の例では、部門別管理ではなく、全社内で一括管理をしている。逸脱の申請に対して必ず許可するというわけではなく、許可判断については、アクションプランの有無や妥当性を見ている。更には許可した後、現場をチェックするという体制で管理している。
- 政府の場合、チェックシステムを、各省庁単位でやるのか、NISCが政府全体でやるのか悩ましい。二重性になるのではないかと考えられる。
- 逸脱管理とはリスクの受容と言えるが、リスクが十分に低減するための措置が成されているかの判断が必要であり、責任が現場である各府省庁にあることから、リスクの判断は最終的には各府省庁が行うことになるだろう。
また、幹部の意識とは、資源配分を適切に行うことにあるが、一方で、政府機関統一基準は、現状の資源配分の中でどのように対策するかになっており、そこを整理する必要があるのではないか。
- 政府機関においては、規模の大小や地方支分部局の有無などにより特性が異なっており、その観点をどのように評価に盛り込むべきか。対策のスピード感という意味で、予算のサイクルも年度単位であるため、すぐに指摘をしても対応に関する時間がかかる点がある。緊急を要する対策、新たな脅威が出てきた場合、それにどう対応していけるかを、どのように評価できるか。
また、技術の進歩や脅威の変化により、政府機関統一基準も省庁基準も見直されるので、省庁レベルにおいても組織としてきちんとフォローアップしていかないといけないので、そのような点をどのように評価していくか加味することが必要。
- マネジメントの改善の効果は、トップの理解度・やる気による影響が大きい。社風によっても変わってくる。資源配分もトップの本気度によるので、内部統制（特に、その基本的要素の1つである統制環境）の考え方を評価項目に考慮できないか。
- 組織として適切に資源配分の判断が出来ているかが重要ではあるが、実際は十分に判断されていない。また、外部委託においてやっているはずという思いこみは外れ、問題が起こることが多いので、ほっておいたら、まずできないものだと思っていた方がいい。トップの意志が各部門に伝わっているかが重要。そういうことに対する評価も必要ではないか。
- 内部統制については、政府機関・地方公共団体ではどうなのか。地方公共団体では一部の先進的な市町村があり、それをモデルに他の自治体を促進させるというやり方があるようだが、政府機関の場合、すでに横並び意識が強く、地方公共

団体のようにならないと考える。

政府機関においては、地方支分部局の有無などで指標を分けざるをえないだろう。

- 有効性をみる評価指標として「事故発生件数」が考えられるが、どこまでを事故と見なすか、網羅的に発見できるかなどの課題はあるが、大企業においては活用できるかどうかを各委員に訊いてみたい。組織が大きくない場合、事故件数がそもそも少ないし、分類していくと1件しかないとかで経年比較など評価に使えない。

また、職員の意識が低いせいもあるが、そもそも事故の報告がなかなか上がってこない可能性がある。事故の件数が増えるのは悪くなったせいなのか、意識が上がってよくなったという見方もあって、評価指標にしにくいということもあるので、どのように思っているか聞きたい。

- 事故報告はたくさんある。指標にすることも可能かもしれないが、実際には対策をしても事故は減らないため、対策と事故発生の中に相関があるのか疑問に思っている。いくら教育を受けさせて、駄目なことも理解しているのだけれど、実行に結びつかないところがある。数値化できない部分をどうやって評価するか。教育の受講数・受講率はわかるが、それが実行にまで移せるのかどうかを評価できるものなのか知りたい。

- 事故発生件数を測って、評価指標としている。ただ、事故とは何かとは難しい。何を評価しているかと言えば、全社での件数は意味がないので、事業部毎に集計して比較し、トップの意識に改革を促すために件数を利用している。本当は事故発生数よりもインシデントレスポンスの対応期間の方が、体制の評価にもなり、重視すべき。

- 事故の定義を社外に迷惑をかけるなどとすれば隠せないが、社内的な事故については、申告が挙がらないこともあるのではないか。本当は、対外的に事故が無いという企業よりも、一定の件数の事故の報告が上がって、対処されている企業の方が健全であると考えている。それに対して、事故がないとっていて、時々とんでもない事故が起きる企業はリスクをチェックする体制がないという意味で問題ではないかと思う。国の機関でもやってもらわないといけない。内部のヒヤリ事故の報告をきちんとあげてもらって、事例を活用し教育して、改善される状況が好ましい。

- 事故の見極めについては、例えばシステム停止など可用性の観点で外部に迷惑をかけるものは影響度大ということで評価することができるのではないか。

- 有効性の評価としての事故の計測は、対策をオーバーオールでみている。個々の対策の有効性の評価には使えない。目的に対して、様々な対策が設計されており、そのプロセスの中で適切に行われているかを評価する必要がある。
- 政府において、トップの意識は一般的には高いと思うが、それが予算措置など資源配分にはつながっておらず、何か事故が起こるまで動かないのが現状である。その一方で、府省庁には他より飛び抜けて対策をするよりも横並び重視や決められたことをきちんとやるなどの特性があるので、これらに絡ませて指標を設定すべき。このあたりは、うまくいっている企業とかと状況が違っているところで、そこを逆手に使っていくべき。
- 指標の検討の際には、機密性以外にも、完全性や可用性の観点を入れていくべき。また、業務プロセスの中で考えていくべきだが、政府機関では、省庁ごとに異なり、課室ごとに業務が分かれており、担当も変わるので、その点を配慮することが必要である。

(9) 今後のスケジュール

- 事務局より資料7に沿って説明