

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2回会合議事要旨

1. 日 時

平成18年10月4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)
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) 政府機関における評価の視点について

○ 事務局より説明

(2) 政府機関における取組の状況

○ 満塩委員、山岸委員より説明

(3) 自由討議

- 成熟度評価には、誰が評価するのか、全体の評価の基準やそのレベルをどうするのかの2つの問題点があり、はっきりとした比較評価になりにくい。ただ、その点を除けば、成熟度評価はある意味で有効であると思う。
- 評価の視点のうち、定性的で直接評価結果を取得できない項目については、代替する観点から複数の指標を設定して測る方法がある。
- セキュリティ・マネジメントを管理する際にも IT を利用する観点があった方がよいのではないか。e-learning は容易に受講率や平均点を取得でき、識別や認証もシステム化により、負担を減らし、利用者の努力によらず実施することができる。規程の内容をシステム化することにより、規程を守らないとシステム自体を利用できないことになり、成熟度が上がったことと同等の効果が得られるのではないか。
- IT 利用については賛成。例えば、可搬記憶媒体でデータを持ち出すときには、暗号化するなどの規程があり、教育をしても、実際に対策の実施に結びつかないことが多々あるため、強制的に暗号化したものしか利用できないようにすることも必要ではないか。
- 成熟度の観点でみると、システムでの強制的実施や e-learning 活用が評価に繋がるが、これは最終的な評価に IT を反映させることであり、直接 IT の利用そのものを評価することは難しいのではないか。
- 実装を IT で強制することは、政府における業務が文書での管理を前提とされており、すぐに実現できるかは疑問である。ただ、省内からの持ち出し等については IT で強制するか、少なくとも警告やモニタリングするシステムは必要ではないか。
- システムで強制する方法は、システム的に制限が無ければやってもよいとの意識になりやすいので、IT だけに頼り過ぎず、職員に対する教育の方も重視すべき。
- 教育は当然行った上で、それでも対策を忘れる者がいるので、完全に守るためにはシステムによる強制も必要だと考える。ただ、IT に制限をかけて仕事ができなくなるのは本末転倒なので、実務的に有効な範囲を検討すべき。
- 評価指標とするにあたり、セキュリティ対策を IT でオートメーション化したかの観点は、予算の確保状況や実装の進捗状況に直結するので慎重にすべき。
- IT 利用について整理をすると、既存のシステムに追加して IT 化するとなると予算上で厳しいだろう。セキュリティ対策は職員にとって業務と二律背反する取組であるが、これを解決するのが IT 利用であるため、評価の一側面となるのではとの考えに基づくが、これは将来的な議論である。
- 成熟度については、企業など一般に広く比較する場合には有効であるが、政府機

関においては一定程度の業務が共通であるとの認識に基づき統一基準を策定しているはずなので、政府機関における評価の軸足は統一基準の項目別ではないか。

- 「仕組み」の評価と「結果」の評価の2通りがあるが、成熟度は「仕組み」の評価である。例えば、事業継続の観点でダウンタイムや稼働率などは、たとえ政府であっても業務によって重要性が異なるために、結果について客観的指標は設定できず、仕組みを評価するしかないのではと考える。
- 政府機関統一基準は状況が変化すれば見直しされるため、既に政府機関の成熟度がある程度加味されているのではないか。2005年版の基本遵守事項については、リスクに関係なく全て実施し、政府機関統一基準に対して評価指標を設定していけば、成熟度も吸収することができるのではないか。
- 政府機関統一基準の策定意図は、政府機関にはある程度の業務の汎用性があると想定し、多くの省庁が抱えているリスクに対して最低限実施すべきというものを定めている。そして、政府機関統一基準の主な役割は、ハードルを徐々に上げていくことで最も歩みが遅いところを押し上げていくことである。
- PDCA サイクルについて、各府省庁で個別に PDCA サイクルを完全に備えるのではなく、政府全体で PDCA サイクルを構築し、Plan として政府機関統一基準を作り、Do を各府省庁が担い、Check は内閣官房と各府省庁に役割があると考えて、各府省庁にとっては Do が最も大きなミッションであるとの理解でいいのか。
- 政府の情報システム管理・運用の基本認識は、“federation of kingdoms”とたとえられる。各府省庁 (kingdom) が個別に PDCA サイクルを持ち、それを前提として、政府全体では federation として最低限レベルを確保していくため、PDCA サイクルの出来が悪いところを改善するようにしていく仕掛けである。これが情報セキュリティ政策会議の決定であり、運用状況に対する勧告であり、検査として重点検査を実施していくことである。
- PDCA サイクルをどの大きさに設定するかにより、評価のスタンスは変わるだろう。統一基準ありきであれば、各項目をどのようにチェックしていくかが重要になるが、各府省庁で PDCA サイクルを持つのであれば、成熟度の観点も割合を大きくすべきかと思う。
- 政府機関統一基準は最低限であり、その上で各府省庁の業務を踏まえた足し込みが必要であり、それは、各府省庁側に PDCA がないと実現できない。特に、機微情報を保有しているような組織では自ら PDCA を回しているべきである。そのため、政府機関統一基準の基本デザインとしては、各府省庁には PDCA サイクルが一応あるとの考えにしている。ただ、PDCA サイクルができていない府省庁にとっては、このルール通りに動かし、Do を頑張れば回るようにと、PDCA のテンプレートとして提示している。自ら PDCA を回していた府省庁は、対策が十分であるかのチェッ

クシートとしての利用を想定している。

- 府省庁ごとの違いとして、地方支分部局がある大規模な官庁かどうかを観点として考慮しなければならないのではないか。
- 自組織独自のPDCAサイクルと政府全体のPDCAサイクルの中で複数の改善すべき課題がある場合に、限られた資源をどこに配分するか悩ましい。各府省庁の組織・規模、扱う情報の種類もあるので、各府省庁の意見を聞く機会を設けて欲しい。
- 役所は評価・監査などが増えており、全体に評価疲れが見える。その後のActに直接結びつく評価項目であると実効性が上がるのではないか。
- 本委員会では、独立行政法人、地方公共団体は直接の対象範囲とはしていない。ただし、政府機関における対策の標準と評価指標を作ると、独立行政法人及び地方公共団体に参考として影響を与えることは事実なので、実際に現場に展開したときに不具合となる場所はどこか、また、地方公共団体等は政府機関よりも大きなリスクに直面して対応しているのでその知見を入れ込んで行きたい。
- 地方公共団体には大量の個人情報があり、機微にわたるものもある。総務省のガイドラインを基に、セキュリティポリシーを精査するとしても、様々な業務に従事している者がおり、どのように徹底させるかが課題である。
- 地方公共団体から独立行政法人まで本委員会の範囲とすると大変な議論になる。実際には影響するが、地方公共団体や独立行政法人は状況が違うので、分野別の観点がある程度入れざるを得ないと思う。
- 「予算」の観点で、「予算が確保されているか」、「予算の執行は機動性が確保されているか」については、予算と執行の乖離を是正すべきという指摘があり、各府省庁で対応できるものなのか疑問。また、「遵守度合」を測るために、実際にどれだけの調査が必要なのかが懸念である。
また、評価の運用の仕方について、内部監査等の内部チェックの構造や地方支分部局の取扱いについても検討が必要。さらに、これらの調査を一遍に全部訊くのか、重点的に訊くのかがあり、重点的に訊くのであれば、予定を示して欲しい。
- 政府機関においても、行政事務を行うグループとオペレーションをしているグループがあり、業務業態が大きく違っていたり、組織が非常に特異であったりする場合にどのように整理するかは議論が必要。
調査の仕方は、現実に作業量と各府省庁の実効性や確実性等を踏まえると、重点的に成らざるを得ないだろう。予定は難しいがなるべく対応する方向で検討したい。基本的には、最大の効果で最小の評価コストが重要である。
- リスクによって優先的にやるべき対策が事実上は異なるはずだが、その観点をこ

の評価の視点に入れるかどうか。

- 対策基準が求められるレベルにあるかどうかを評価するというのであれば、各府省庁独自のリスク認識に基づいて対策しているかの観点はどこかにあるべきだが、リスクに基づく対策の中身の違いについてはそれを統一基準の中に持ち込むべきではなく、統一基準のレベルで評価すればよいのではないかと思う。
リスクの中身としては、既存のシステムに対策するのは大変であるが、これから構築するシステムではセキュリティが考慮された基盤の上に共通的に構築されると考えられるので、3年間でその進行状況が見えるとよい。
- 基本的に、異なるリスクに対応しなければならないために政府機関統一基準から逸脱するというシステムは非常に限定的であると想定している。それは、経験的にも言われており、米国の FISMA や SP 800 の構造からも明らかである。そのため、政府機関統一基準におけるリスク認定も非常に汎用的であると認識している。
また、NISC が各府省庁の実装にまで直接チェックをするかについては議論がある。各府省庁には一応監査組織があり、NISC のキャパシティとしてもそこまでの余力はないため、実装の確認については現時点では各府省庁に任せることとしたい。
- 監査について、民間企業の場合でも監査部が現場を直接チェックしている訳ではない。監査部は執行組織を監査し、執行組織は自主監査の名目で現場をみる。あくまで執行組織が自主監査したものを監査部が確認したものを内部監査としており、政府機関の場合と非常に似ている。
- 地方支分部局や外部委託先などで責任が不明確な場合があり、その観点がどこかに盛り込まれているべき。
- 次回までに何をするのか、具体的なイメージを教えて欲しい。
- 今回で評価の視点について議論し、次回までに事務局でまとめる。そして、次回には、今回の議論から具体的な評価指標をどう考えるか整理したい。また、全体のリスクと受容の関係や政府においてどのような水準を考えていくのかのたたき台、指標が出てきたときの指標の運用の仕方について提示する予定である。
- NISC が各府省庁の対策のあり方や PDCA サイクルを検査・評価する際に、政府機関統一基準に合わないところを強制的にやらせたり、それをやらせるために公表したりすることまでは考えていない。内閣法の趣旨からそこまでの権限はなく、責任は各府省庁にあるので、その前提を踏まえて検討をお願いしたい。
- 基本的に各府省庁に責任があるが、NISC としては PDCA が回っていないところや最低基準が守られていないところについては、当該府省庁にその情報を伝えてセキュリティ対策の改善を促すことは役割ではないかと思う。

- 各府省庁で独自に PDCA をもち、その中で Check をし、それを府省庁全体で俯瞰して評価する指標であるとする、各府省庁で PDCA をどのように回しているかを測るものであり、同時に各府省庁内で評価されるときにも利用されることを想定して指標を作ることではないか。
- これまでは各府省庁任せであり、政府全体としてどうなっているのかを把握できていない。今回の評価指標は、政府全体の基本計画に基づくものであるが、政府機関における対策の実施度合は各府省庁の取組に落とすことができ、これをみれば政府機関における対策の進捗度、成長度をみることができるとの仮説に基づき、各府省庁の対策を見るテンプレート的な評価指標の提示が必要。
- 各府省庁がある程度評価しているなら、全体の評価指標は大枠でよいだろうし、一方で、各府省庁内や地方公共団体などで規範となる評価指標が無い状況であれば、具体的なレベルまで書くことも必要だろう。その2つを分けて、各府省庁での評価のガイドを示し、政府全体としての評価という二重構造でもよいかもしれない。

(9) 今後のスケジュール

- 事務局より説明