資料３－１

【下村委員御意見】

意見書

2008 年 5 月 17 日

下村正洋

＝重点政策　政府機関・地方公共団体について＝

○　政府機関における情報セキュリティ対策の目標・枠組み設定、推進体制について

・政府機関統一基準とそれに基づく＜中略＞政府全体のＰＤＣＡが前面に出すぎたために、各府省庁におけるリスク分析や自己評価などの自主性や自立性を損なっていないか。

（意見）

営利活動を行っている組織（つまり、非独占的企業など）はそれ自身が置かれている状況から組織の存亡や発展が構成員の待遇に直接的に関与することから、情報セキュリティのようなコスト的側面を強く持っているものについても自主性を期待できるが、情報セキュリティが組織の基本的な存続を脅かさないような場合（つまり、非営利組織や権益に守られた独占企業など）には、その自主性に任せるのではなく、第三者からのある程度の強制は必要であると考える。

○　政府機関におけるチェック機能の必要性について

○　各府省庁の評価について

○　独立行政法人等及び外部委託のセキュリティ対策について

（意見）

上記３つについては、前回資料３－６和貝委員の意見に同意する

○　政府機関における人材育成について

（意見）

情報セキュリティの専門知識を有する人材を各政府機関に配置することは必要であるが、その資質をある程度同質にしなければ政府機関内での意思疎通や連携などに齟齬が生じる可能性がある。したがって、人材育成においてその目標となるものを提示することは考えられないか。

＝重点政策　重要インフラについて＝

○　重要インフラにおける情報セキュリティ対策の視点

（意見）

指摘にあるように重要インフラにおいて一律の基準を示すことは不可能であると考える。したがって、それぞれの分野ごとに基準を作るべきと考えるが、その策定の方法は各分野で自主的に作ることを後押しするような施策をとるべきと考える。このようにして策定した基準を広く一般に公開し、その理解を求めることにより、その分野に残るリスクを社会的に許容することができれば望ましいと思える。

○　安全基準等の整備

（意見）

それぞれの分野の特性に応じて適切な「安全基準等」を示すことは上述したと同じく進めるべきと考えるが、その遵守状況を定期的に確認する必要があると考える。この方法として情報セキュリティ監査を適当な期間をおいて実施し、その結果を公開することは有効ではないか。

○　情報共有体制の強化

・整備された体制の下での情報共有を阻害する要因があるのであれば、それはどういったものであると考えられるか？また阻害要因を除去するためにどのような取り組みが必要か？

（意見）

阻害する要因として考えられるのは、組織としての機密防衛とメンツがあると考える。機密防衛については情報を出すことによってその組織のシステムや運用に関わる情報が漏洩または類推されること、メンツにこだわるとは、情報（脅威情報や脆弱性情報など）を発信することでその情報の発信自体を他社に評価され、自信の実力を推量され、それが劣っていると判断されることをおそれることである。前者については、組織間の協定などを締結することによりある程度は緩和されると考えられるが、後者については組織だけでなく、それに従事する人の思惑も働くので簡単に除去できないものであると考える。

これを解決するには組織を越えてコミュニケーションできる環境を作るしか方法はなく、各組織のセキュリティオペレーションに従事する人々の Face to Face の関係を作り上げることを考えるのはどうか。

＝重点政策　企業について＝

○　対策推進全般

・情報セキュリティ対策によって確保すべきセキュリティの水準は企業一律でよいか？

（意見）

セキュリティの水準が企業一律であることはなく、それぞれの業種や業態によって、または、守るべき情報資産によって水準が変化することは明らかである。したがった、様々な状況によってセキュリティ水準ならびにそれを決定づけるセキュリティ対策があっても仕方が無く、このようなことを積極的に推し進める政策が必要と考える。具体的には業界団体等を後押しして、それぞれの業界において個別の情報セキュリティ基準を、（それもできるだけ具体的な対策まで踏み込んだ、）自主的に作り上げることを支援する政策を考えてはいかがか。あえて記述するが、このような踏み込んだ基準を作り上げるときにＩＳＭＳ等の情報セキュリティマネジメントシステムが有効に機能していることは大前提である。

・情報セキュリティ対策が、企業にコストであると思われないようどのようなメリットをどのように作って行くべきか？

（意見）

「企業にコストである」ではなく、「企業に過剰なまたは不必要なコストである」とすべきであると考える。情報セキュリティ対策に掛かる費用は企業にとってコストであることは変わりなく、これをコストでなくビジネスにおいてプラス方向（単純すぎるかもしれないが、つまり、セキュリティ対策をやると儲かるということ）に作用させるようなことは政策レベルでは無理であると考える。したがって、前述のように個々の状況により具備すべきセキュリティ対策を策定し、それを遵守することによってその企業の最低限の取り組みを実証することである。これ以上のことは市場の原理に委ねることで十分だと考える。

・対策を推進してもリスクがゼロになる訳ではない（以下略）

（意見）

対策疲れに対しては、上述の方策により具体的なゴールを提示することができると考える。疲れるとは何処までやればいいのか判らない、つまり、見えないゴールに向かって進まなければならないことに対して発生することだと考えられ、具体的な対策を提示することは対策疲れに対して有効と考える。具体的対策を考える場合において、予防策より事後対策が有効かつコストが掛からないならば事後対策重視に重点を置くことも有効である。ただし、極端にこの方向に触れることは結果的に対策（予防策）を怠ってもいいとのメッセージになることも懸念されることから、個々の業種や業態でセキュリティ対策基準を積極的に公開し、社会からの合意を取り付ける必要がある。

○　中小企業関連

・「中小企業」には様々な業種、規模が含まれることから、対策を検討するとしてどのように対象の整理を行うか？

（意見）

前述してきたように業種、業態などにより個別に具体的なセキュリティ対策基準を作ることが有効と考える。また、中小企業にある下請け業態については、その委託元と共同して対策基準を作ることが有効ではないかと考える。

・限られたリソースの中で、中小企業向けの対策として効果的なであるのはどのような対策か？

（意見）

中小企業の問題はセキュリティ対策の核となる IT システムのコストとセキュリティ人材不足であると考える。IT システムのコストについては、必要となるセキュリティ対策用の IT システムの共同利用基盤（ビジネス）の創出を促すことがあるのではないか。また、人材については中小企業にそれぞれ専門家を作ることは難しいと考えられ、セキュリティコンサルティング（人及び業）の拡大を促進することが必要と考える。