資料３－６

【和貝委員御意見】

2008/04/17
和貝

スライド 13p について：
〇政府機関におけるチェック機能の必要性について
・各府省庁の自らの情報セキュリティに関するチェック機能（特に監査的な機能と指導的な機能）をどのように実効性を 確保した上で埋め込んでいくかについて検討すべきではないか。

←チェックを実施するためには、チェックの基となる基準が必要となる。この基準は統一的な規準（クライテリア）として準備されたものに基づき、各府省庁が自らの規準を各府省情報セキュリティ管理規準として策定し、これに基づきチェックがなされることになることが望ましい。
　各府省庁が自ら策定した規準を遵守する活動を導入し推進することが，「指導的な機能」と位置づけられ、導入運営されている状況をチェックする機能が「監査的な機能」と位置づけられる。制度の当初にあっては、指導的機能が重視され、制度がある程度成熟した後、監査的機能を発揮することが有効である。監査は本来良好な実施状況の確認としてなされるべきであり、合理的な水準を定めた規準を遵守する活動こそが重要だからである。
　規範性の観点からは、統一的な規準を遵守すべき規定を法律として定め、統一的な規準は府省令とするなどの措置が考えられないか。

・監査的な機能について、その客観性の確保はどうあるべきか。

←監査的な機能は、上記のように自らの「情報セキュリティ管理規準」への準拠の状況を示す「準拠性監査」として実現できるのではないか。準拠性監査は年一回等、定期的に実施されるべきである。
　監査の客観性は、情報セキュリティ管理規準の策定と独立の監査人を指定することで達成できるのではないか。
　情報セキュリティ管理規準が非公開とされる場合でも、独立の監査人として社会的信頼を得た適格性を有した者が、情報セキュリティ管理規準への準拠性を証明すれば、監査の客観性は、保たれるのではないか。独立の監査人については現行の各種監査人資格制度の監査人がその候補となろう。

←「監査」の観点が、「政府機関」についてのみ議論されているのはバランスを欠かないか。
　本スライドに続く、「重要インフラ」、「企業」についても、レベルの差はあれ何らかの規準に基づく合理的セキュリティ水準の達成維持を目指し、その社会的評価を期待するのであれば、セキュリティ管理規準および監査が議論されるべきではないか。

〇各府省庁の評価について

←NISC によるような評価は継続すべである。ただし、評価主体については今後適当な別の機関

ないし者によることを検討すべきではないか。規準を明確にして「評価」を「監査」として制度化することについては先述の通り。
評価の結果が良好でなければ　*気にすべき* であって、対応期間や予算を勘案の上、当然に改善すべきである。
←評価結果の改善を推進するための仕組みとして、セキュリティ人材の育成・採用や、「セキュリティ担当」を特定設置した、「規準」遵守活動等の施策が考えられる。

スライド 14p　について
・政府機関が外部に委託している業務のセキュリティ対策を政府機関はどのように担保するのか。
←当該政府機関内に「セキュリティ監査担当」を設置して、外部委託先の監査(評価)を実施するか、またはこの機能を専門とする外部機関・業者に独立的監査を委託するなどにより、外部に委託している業務のセキュリティ対策の導入・状況を担保するのが適当ではないか。

スライド 19p 「企業」について
〇対策推進全般
〇一般ユーザー企業関連

←大括りの業態別、規模別の「情報セキュリティポリシー」の例示を提示し、一定規模以上の企業の「情報セキュリティポリシー」策定の「義務付け」、ないし「推奨」などの措置は実現できないか。
上記で情報セキュリティ依存の企業、あるいは大規模企業については、情報セキュリティポリシー策定を義務付けし、導入・運用状況の監査を推奨することは有用ではないか。
←監査を実施した企業については、監査費用のうち一定金額を税務上の所得控除とするなど優遇策を適用できないか。
情報セキュリティポリシー策定・導入企業の届出、届出の旨一般開示するなどは、制度を推進するものではないか。
←企業の対策疲れは、合理的水準を示す「規準」が明確でないところにある。早期に企業別情報セキュリティ管理規準の基礎となる統一規準を明確にすべきではないか。
セキュリティ事故についての復旧コストは、その事前防止を想定した対策コストに比して大きくなることが多く、事後的対策のみでは経済的合理性の観点からは適切ではなく、事前対策が肝要であることに留意すべきではないか。

〇中小企業関連
←上記、*対策推進全般*　に記載した内容は、中小企業関連にも適用できないか。

スライド 21p 「個人」について

○情報セキュリティ教育、啓発の充実

←企業に従事し業務を通じてある程度の知識経験を持った者を除けば、一般個人にとって情報セキュリティについての関心は依然として低い。個人についてのセキュリティの合理的水準も想定できるはずであり、少なくとも一般個人として了解しておくべき情報セキュリティについては、啓発が必要と考えられる。
「児童」の段階からの教育カリキュラム等体制の準備や、一般個人向けテレビ広報等の検討を基本計画に盛り込むことは可能か。

○個人の責任範囲

←「セキュリティ文化」の中では、個人として負うべき情報セキュリティについても責任範囲を明確にすべきである。しかしながら、現状それを早期に実現することは適当ではない。先述の、個人の情報セキュリティ教育、啓発を前提としてそれらが十分浸透し、個人のセキュリティ意識が個人としての合理的水準に達したときに個人の責任が問えるのではないか。
試験的に個人の責任範囲として実施すべき情報セキュリティ推奨策などを提示して、その運用状況を研究・検討していくなどの措置は採れないか。