

個別検討に関するコメント

2008年3月24日

環境省 CIO 補佐官

満塩 尚史

I. (1) 確保すべきセキュリティの検討

- 基本的には、セキュリティの検討の切り口は、CIA であると考えている。特に IT ガバナンスのフレームワークといわれる COBIT の中でも、CIA は、「Information Criteria」の一部と位置づけられており、セキュリティを定義するためには、基本的な切り口であると考えている。BCP 等は、「Information Criteria」を確保するための「IT Process」のひとつであると考えている。

- 「Information Criteria」の一部である CIA で情報セキュリティを定義するのは、妥当であると考えているが、一方、この CIA の確保を実現して（セキュリティを実現して）、政府、重要インフラ、企業、個人に対してどのような影響（もしくは効果）があるか整理しておく必要があると考えている。特に、企業等においては、セキュリティの効果をどのように考えるかで、推進力が大きく異なり、これは、政府、重要インフラ等にも同じことが言えると考えている。

第1次基本計画の段階では、事件、事故等の脅威を感じていたと考えるので、推進することができたかもしれないが、今後も推進していくためには、この影響や効果を整理する必要があると感じている。

- レベルに関しては、企業等が主体的に選択するためのレベルがほしい。イメージとしては、米国 SP800-53 で定義されているレベルである。これらのレベルを定義できれば、企業側や各組織で各組織の業務内容等によって、自組織のレベルを定義できると考える。

また、これらのレベルは、国内における共通言語となることを想定している。（現在、セキュリティ業界においては、各社、各層での言語やレベルが統一されていないと考える。そのためにも、レベルの定義も必要だと個人的には感じている。）

I. (2) 他分野との関係

- 政府機関の他分野との関係を整理していただきたいと考えるのは、個人情報保護、文書管理、BCP、情報公開である。特に、文書管理及び情報公開に関しては、法律等の問題もあるので、企業とは別に政府機関特有の問題として整理していただきたい。

Ⅲ. (1) 政策推進にあたっての基本スタンス

- 「経済・社会、生活・安保」とは、まったく異なるスタンスであるが、第一次基本計画で構築したフレームワークの具体化もしくは導入といったイメージの基本スタンスも必要ではないか。特に、多くの企業が ISMS を取得し、取得件数としては、世界の中でもトップクラスであることは事実であるが、具体的なセキュリティ対策が世界でもトップクラスだという実感はあまりない。問題は、PDCA のライフサイクル管理は、導入されたもののセキュリティの具体的な対策は、まだまだ、これからであると考え。この状況は、政府機関も同様ではないかと考える。
この路線の先には、米国で実施している NIST 活動、SP、FIPS、NIST Security Configuration checklist program 等にもつながると考えている。

Ⅲ. (3) 対策の実施における地域性の観点

- 基本的にはセキュリティの場合も、他の施策、IT 施策等と同じ構造が、都市部と地方部間に存在していると考え。ただし、情報セキュリティに関する知識が、IT から業務、法制度等の広範囲にわたり必要なため、都市部と地方部間の格差が、他の IT 人材等の格差以上に激しいと実感している。

第2次計画検討に際しての“大括りの項目”について

メッセージ

- 上記であげたように「第1次計画で構築したフレームの具体化」というイメージの視点も必要ではないか。

理念・哲学

- 上記であげたように「高品質・高信頼性・安心安全」を実現し、政府機関、重要インフラ、企業、個人は、その先に何を見ればいいのか。「情報セキュリティ先進国」が目的なのか。「情報セキュリティ先進国」を目的とした場合、企業等のこれまで以上の推進力を発揮することができるのか。

推進体制

- 第1次基本計画で構築したフレームワークを実現、具体化する推進体制が必要ではないか。米国の NIST 等の具体的な基準や仕様は、セキュリティ製品や業界でも活用されている。一方、日本においては、セキュリティ業界で活用するような具体的な基準や仕様は、まったく、存在しない。これらの推進をしていかない限り、セキュリティ業界において日本が「情報セキュリティ先進国」に位置づけられるとは思えない。
- 政府機関に関しては、米国事例等やこれまでの会計検査院の活動を考えると会計検査院との連携も考える必要もあるかも。

重点施策

- 政府機関に関しては、統一基準を実施し始めたばかりであると考え。そのため、大枠のフレームワークは構築されてきている。ただし、現実に則したマニュアル等の整備や具体的なセキュリティ対策の実施は、これからも実施する必要があり、これらの具体化が重要なテーマであると考え。
- 日本は、既に ISMS 所得件数が 2000 件を超え、世界でも突出した取得数を誇っている。(2位以下の国での所得件数は、3桁以下である。)とはいえ、日本企業が世界でも有数の「情報セキュリティ先進国」であるという実感は、個人的にはあまりない。そのため、第1次基本計画で、立ち上がった意識を実態に転換していく作業が必要ではないかと考える。企業においては、ISMS 所得することが目的ではなくセキュリティ対策の「質」が問われる時期であると考え。