資料４

第２次情報セキュリティ基本計画策定にあたっての意見

３月１９日の会議において示された「検討の範囲」や基本的なスタンスに関して追加的にコメントを送ります。

■ 第２次基本計画として特徴を出すべき

・ 第１次計画では、全体の枠組みに重点が置かれたことと思うが、第２次で内容をより進展させるに当たって、第１次とは違った明確な目標設定のようなものがあるといいのではないか。
・ 世界の中で日本の存在感が薄れていくなか、せめて「アジアでの情報セキュリティのリーダーになる」というようなレベル目標がモチベーションとして必要なのではないか。「情報セキュリティ」という言葉自体が、一般には親しみがなく、まして CAI（機密性、完全性、可用性）などと解説すればより疎遠な印象を与える。わかりやすく親しみと訴求力のあるコピーを持つのがいいのではないか。
・ 民間活動で意識高揚を推進している【みんなで「情報セキュリティ」強化宣言！】コミュニティ活動においても、本年度はキャラクターに若い層に再び人気がでている「なめ猫」を採用して興味を引く活動をしている。

■ リスクマネジメントとして捉えることの強調

・ 行政においても経営活動においても市民の社会生活においても、ICT がインフラとなっている事実を強く認識し、ICT の利活用によって豊かな社会と安全な社会を形成するという【リターン】のために、【リスク】を正しく理解してそのコントロールをする必要性を強くメッセージにすることが重要である。
・ リスクコントロールはリターンを得るための知恵であって、前向きに捉える必要がある。ややもするとコストが掛かる、担当者だけの問題にされている、理解者が少ないなど後ろ向きの話が多いので、２次計画ではそれを払拭していくような内容のまとめ方が望ましい。
・ 利便性＝社会・経済の活性というリターンを得るには、ある程度のリスクコントロールコストが掛かることは避けられないが、リスク ZERO はありえないので過度になることを防ぎ、回避・低減・移転・受容の対策を正しく理解されるように努める必要がある。

■ 対策としての方向性と具体

・ 実際の現場では、「具体的に何をすればいいのか？」が正直な感想であり、体系的な枠

組みとともに対応の具体に触れる必要があるかと思われる。

- リスク管理の観点からは「予防措置」と「事後処理」があるが、モニタリングのような「情報セキュリティの見える化」をどう低コストで実現していくかも重要な予防措置を思われる。事後処理にしても、過去の同様事例がうまく生かされないことが多く、知識ベースを整備も必要である。
- このたび海上自衛隊がシンクライアント（Sun-Ray）を大量導入するという報道があったが、これは十分なリスク分析もないまま「技術的対応」に依存した事例であると思われる。その前に「教育的対応」、「オペレーションやマネジメント対応」でやるべきことが山積しているはずで、安易な技術的対応がコスト問題を強調する結果にも繋がる。
- 基本計画では、リスクの正しい理解、分析、対応の手順について具体を示していく必要があるのではないか。

2008/03/27

大成建設株式会社
木内里美