資料５－１

【富永委員御意見】

２００８年8月6日

情報セキュリティ基本計画「政府機関＆重要インフラ」への意見

富永 新（日本銀行）

先に行われた「政府機関」と「重要インフラ」に関する議論を踏まえ、次回の「両者を跨る議論」に向けて、改めて考えを整理しましたので提示します。

１．政府機関と重要インフラを跨ぐ全体整合的なリスク評価の必要性

「政府機関」と「重要インフラ」を跨った全体整合的なリスク評価が必要。組織単位で別個に評価した重要度を単純に足し上げると、以下の２リスクあり。

① ある組織の最重要業務は他組織の一般業務より低いなど、不適切

② 全体として経営資源以上の対応計画となり、実現が困難

一度、内閣官房主導で、政府機関と重要インフラ（１分野として「行政サービス」を含む）全体での重要業務のランキング（リスク評定）を実施したうえで、全体のバランスを考えた具体的施策を考えていくのが得策。

―― 地方公共団体は、地方自治原則がある以上、上記選別の結果「最重要」と認定し得る業務のみ、特別立法等により遵守を求めるのが筋か。

―― 政府機関も、「金融界に比べシステムの位置付けが低く、可用性が求められるシステムは少ない」説が正しければ、無理に高いレベルを求める必要はなく、機密性先行の現対策もある程度まで正当化が可能。

２．オールＪＡＰＡＮ的な人材の活用

情報セキュリティに関する人材難が問題となっているが、オールＪＡＰＡＮで考えると、例えば大手銀行を中心とする金融機関やIT ベンダーには、システム系のベテランを中心に監査人足り得る人材が、他の業界よりは多く存在。

この際、業界の垣根を取り払い、こうした人材を何らか組成して権限を与え、わが国公共的システムの最適化の検討や、統一・横断的な目線での対策推進・監査等（チェック）に活用していく方策が有効。

３．ＢＣＰの総合テスト推進によるＢＣＭ確立

システムのテストは単体テストから総合運用テストまで徹底的に実施される一方で、ＢＣＰのテスト（訓練のうち「習熟」と並ぶ意義である「確認」）が殆ど行われていない不均衡こそが、危機対応上の大きな問題。

諸外国と比べても、ストリート・ワイド・エクササイズ（ＳＷＥ）が不足している。わが国は「準備が整ってから、上手く回ることを確認したい」国民性であるが、この際「やってみて、如何に上手く行かないかを思い知る」ことが大事。そのうえで、実効的なBCM を確立していくアプローチが有意義。

こうした面で、政府（ＮＩＳＣ）が音頭を取って取り組む意義は大きく、一段アクセルを踏み込んだ推進を期待したい。

以　上