資料３－４

【富永委員御意見】

２００８年5月１２日

情報セキュリティ基本計画「検討論点」への意見

富永 新（日本銀行）

これまでの議論の中で主張してきた「一定のリスクを許容しつつ適切なコントロールの下でＩＴ利用を図ることや、リスクが顕現化した場合の影響を最小限に抑え迅速に復旧（事業継続）することの重要性」を採り入れて頂き、現行計画の理想主義色から現実に基づくバランス感が増しているものと認識します。

また、先に意見表明したベースライン（基本原則）＝１．自己責任原則（前提としての情報開示）、２．市場原理優先（必要最低限の行政介入）、３．費用対効果重視（経営的視座からの考察）も、引き続き意識しながら議論を進めて頂くことが適当と考えます。

そのうえで、これまでの議論を踏まえ、改めて考えを整理してみると、以下の通りです。

１．先ずは政府機関が率先垂範する（背中を見せる）重要性

本計画の対象者は、中小企業・地域・個人など、幅広いものとなっているが、これらの方々に、具体的に「何々しろ」と強制することは難しいと思われる。教育・啓蒙的な活動も重要だが、「手の届く範囲」「実際の効果」という観点からは限界感が否めない。

そうした中で、優先度が高いのは、重要インフラや大企業になると思われる。これらの主体に相応の社会的責任意識に基づく対応を促すことは可能としても、自発的な対応を動機付けるためには、先ず政府機関が「ここまでやっている」「こうすれば（低負担で？）できる」といったお手本を示し「背中を見せ、追わせる」姿が適切。そうしないままお題目を唱えても「怒られない程度に適当に付き合っておくか」程度の推進力しか働かない可能性が高い。

―― 重要インフラの定義が現状のまま（高抽象度）であれば、個別企業側が「模様眺め」感覚になっても致し方ないか。

政府機関の対策は、情報セキュリティの機密性・完全性・可用性（ＣＩＡ）のうち、先ずは機密性中心に対策が進んでいる模様だが、今後完全性や可用性を含めた、全体的な姿として国民の信頼を獲得できるような取組み強化が期待される。

そうした対策推進の実効性を確保し、納得性を高めるためには、ＮＩＳＣの位置付けをより強化する、ないし新組織を立ち上げるなどにより、コントロールタワー（権限ある主体）を明確にするとともに、各省庁の自主点検モードを脱し、第３者による立入監査の実施までを含むＰＤＣＡ体制の整備・確立が必要ではないか。

２．具体的な取組みの進展に向けた体制強化と選球眼

現論点案は、「具体的な取組みを機能させていく」と謳う割には、実現のために必要となる強い動機付けと実践的な体制のイメージが弱く、また具体策の洗い出しも不十分なため、このままでは「一次計画比、手抜きを許容しただけ」との批判を招きかねない印象がある。

「利益提示型の奨励」と言っても、現実にはそう簡単でないことを踏まえると、リスクベースで真に重要な分野（対象）に関しては「枠組みを一段と強化する」方策を考えていくことが現実的ではないか。

具体策の抽出は悩み所で、これまでの議論でも広範な問題提起がなされているが、優先すべき切り口は、「政府（ＮＩＳＣ）が本当にやりたいことは何か」「そのうち当面できることは何か」になると考える。野球に喩えれば、どんなコース・球種を狙って打つのかを、事務局側でも詰めて議論し直し、整理・提示する必要があるのではないか。

先ずは「できること」「手が届く範囲」に真剣に取組み、そこでの成功体験（ないし教訓）を基に、他の対象範囲や課題解決に繋げていく漸進的なアプローチが有効と思われる。

―― 「（すぐに）できないこと」や理想論的な夢を書き込む場合には、その性格が分かるように分類し、「中長期的な課題」等として取り扱うことが適当。

３．アウトソーサーを取り込んだ協働体制の構築

わが国のＩＴ化の現状を直視すれば、最大の特徴点は「外部委託（アウトソーシング）が進展し、責任の所在が不明確になっている」点にあると整理可能ではないか。殆どのＩＴ化は、外部委託（パッケージ利用を含む）を前提に進んでおり、共同システム（センター）の隆盛もあって、実質的な当事者はＩＴベンダーに移転している度合いが高い。

そうした状況下でのリスク管理の基本は、「原機関による適切な委託先管理」になるが、こうした意識向上を啓蒙していくことは当然として、現実の情報セキュリティ対策を向上させる（リスクを軽減する）近道（効果的な方策）は、政府が「主要なＩＴベンダーに直接働きかける」ことにより、ＩＴベンダーを

取り込んだ協働体制をいかに構築していくか、ということに尽きるのではないか。

具体的なアプローチとしては、

１．真に重要なシステムのＩＴ主導権は原機関に復帰させ（任せ切りをなくし）、ＩＴベンダーの役割と責任を明確にする方向での真摯な取組み

２．民間企業同士の取引に任せるべきものは、両者間で適切なパートナーシップが養成される各種ガイドライン類の整備と啓蒙による後押し（環境整備）

３．零細企業など弱者対策としてＳａａＳ（やＡＳＰ）を推進する場合には、（原機関による委託先管理には無理があると割り切ったうえでの）ＩＴベンダーに対する行政からの監督・指導

を組み合わせていくことが一案かと思量。

さらに発展させるならば（各種の制約が想定されるが）、一定の責任を負い基準を満たす者だけを、政府機関や重要インフラのＩＴ提供者に選別（それを忌避する主体は撤退）する方向で考える、といった対応も展望し得るのではないか。

――　ただし、これらの方策は、上記「市場原理優先」方針に反する行政介入感が否めず、必要性の見極めや実際の方法は慎重であるべき。

４．基準作成は、その必要性と基本的考え方の提示が主軸

基準作成の必要性が何度か論じられているが、改めて見回すと、既に各種の基準やガイドラインは存在しており、しかしこれに沿った具体的な取組みが進んでいない、という状況が多いのではないか。

従って、新基準の必要性を真に見極め、屋上屋を重ねるような基準作りは行わないスタンスが適当と考える。

また、「基本計画」として踏み込む適正範囲としても「こういう考え方の下で、この（各々の立場に応じた）水準の基準が必要ではないか」と問題提起したうえで、

１．未だ無い業界等があるなら

・「先ずは基準を自分たちで作ることから始めよう」

２．既に存在する業界等に対しては

・「今の基準が、上記の考え方を充足しているか見直したうえで、それが守られているかを検証することが重要」

と呼びかけること、が妥当ではないか。

５．障害原因の共有と再発防止策の横展開

障害抑制のために情報の共有を進めることの有用性は論を俟たないが、現在の情報共有はＷｅｂを中心とする機密性分野に偏りがちで、実際に国民に影響

することの多い可用性（システムダウン等）の事例共有は遅れていると認識。

私ども（日銀・システム関連考査担当）では、０７年３月に、
「事例からみたコンピュータ・システム・リスク管理の具体策」
http://www.boj.or.jp/type/ronbun/ron/research07/ron0703a.htm
を公表した。
これは、過去数年間に全国の金融機関で発生した障害事例等を普遍化し整理・紹介したものであり、金融界のみならず全ての機関・企業等で「他山の石」として参照し対応策を打てば、障害の防止に役立つものと考えられる。

今後、こうした取組みを、他の指導・監督機関やＩＴベンダーならびに関係団体でも推進し、有益な情報提供と共有が進展することを期待する。特に、オープン系システムが普及する中で、サーバーやミドルウエア、データベースなど汎用的に（組み合わせて）使われる機会の多い製品の不具合情報の共有は、優先度が高いと見られる。

さらに、事業継続関係についても、今般（５月９日）、
「業務継続体制の実効性確保に向けた確認項目と具体的な取組事例――先進事例を中心に」
http://www.boj.or.jp/type/ronbun/ron/research07/ron0805a.htm
を公表した。
これも、障害発生後の対応等に関し、幅広い関係機関、企業のメルクマールになり得るものと思われる。

６．その他

（１）議論の前提となる要件設定

・先に意見した諸条件明示のうち、次期基本計画の対象期間だけでも、議論の前提として早めに決めることが適当ではないか。

（２）各論の補強

・検討論点のうち、「推進体制」以下＝「具体部分」は、丸投げ的なオープン･クエスチョンが多く、「何を目指すのか、どんなアイデアがあるのか」や「現行計画で何ができていないのか、その際何がネック（問題点）だったのか」など、問題意識の中身がイメージしにくい（この結果、触発された意見も浮かび難い）印象が否めない。
今回提示される各委員の意見のほか、現計画の達成度評価、他の委員会等を含む議論の洗い直し等により拡充したうえで、再提示されることを望みたい。

以　上