情報システムにおけるリスクマネジメント

－システム安定稼動におけるリスクの可視化－

アブストラクト

２００２年春に発生した銀行のシステム障害は、企業の経営層には少なからずショックを与え、情報システム障害が発生した場合の影響は、経営の悪化に直結していることを改めて認識させられることになった。情報システムについては、コストパフォーマンスを最優先にとらえていた経営者も、リスクマネジメントの重要性を真剣に考え始めた。情報システムを担当している部門にとっては、ＩＴ基盤を安定稼動させるためにリスクの内容と影響を明らかにし、それらに対して適切な対応をとるとともに、サービスレベルを維持管理することが非常に重要になってきた。

1. 研究の目的

企業において、経営層はリスクに対する対策の必要性を感じながらも、リスクとして具体的にどのようなものが存在しているのか、また、そのリスクに対して、どの程度の対応を行うことが妥当なのかが不明確であり、的確な対応をとることができない状態でいる。また、情報システム担当部門では、具体的な費用対効果が明確にできないため、経営層を納得させるリスク対策の提案を行うことができない。

当分科会では、企業の経営層と情報システム担当部門の双方が漠然と感じている不明確さを明らかにし、リスク対策の具体的提案を行える仕組みを考えることを研究の目的とした。

2. 研究の範囲

分科会参加メンバー各社の重要課題として、「システム運用時におけるリスクの低減」という意見が多かった。これは、現場の危機感の現れであるといえる。そこで、当分科会では、『システムの安定稼動』に向けてのリスク対策を経営層が判断するための材料となるリスク評価方法を検討することにした。

一般的にリスクマネジメントは、マネジメントサイクル（ＰＤＣＡ）に従い実施する必要があるが、当分科会では、Ｐ（Plan）工程における、リスク分析，リスク管理に研究の焦点をあてることとした。

3. リスク分析／リスク管理の評価基準

一般論として言われているリスク分析／リスク管理手法を、自社において適用しようとした場合、手法を理解し、適用するためにカスタマイズを行い、手順書等を作成するといった作業が発生する。これらの作業をできるだけ軽減し、誰にでも理解できる手法を簡潔にまとめることができた。

当分科会では、システム利用者が容認できる使用制限の項目（システム停止時間，レスポンスタイム等）とその数値（時間等）を、サービスレベルとサービスレベル許容値という形で定義し、これらを使用することにより問題の解決を行った。

リスク明確化のポイントは以下の２点である。

① サービスレベル許容値を超える状態をリスクと定義し可視化すること

② 脆弱性は脅威の要素として含めること

この考え方から、リスク値を以下のように計算することとした。

リスク値＝Ｔ×（Ｄ－Ｒ）

（Ｔ：脅威の発生頻度，Ｄ：脅威発生時におきる被害の値，Ｒ：サービスレベルの許容値

※　（Ｄ－Ｒ）は被害の大きさを示す　）

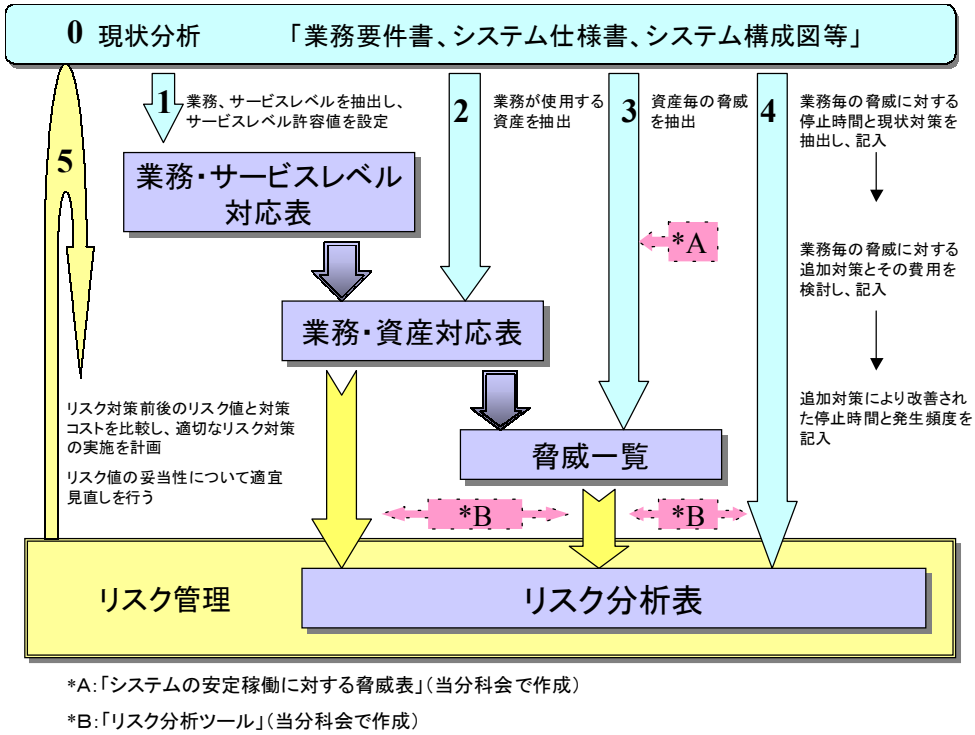
この式の意味は、以下のように捉えることができる。

① ‘Ｔ×’は被害が小さい場合でも頻発する脅威はリスクが高いことを意味している。

② ‘Ｄ－Ｒ’は、サービスレベル許容値以内の被害値であれば、
リスクとはしないことを意味している。

4. リスク分析／リスク管理の手法

リスクを可視化するために、現状分析からリスク管理に至るプロセスを策定した。リスクを数値化するために必要な情報（サービスレベルの決定、業務・資産・脅威の一覧）を整備しリスク分析表を導き出す。リスク管理を容易に行うためのツールを当分科会で独自に作成した。概要は下図のようになる。

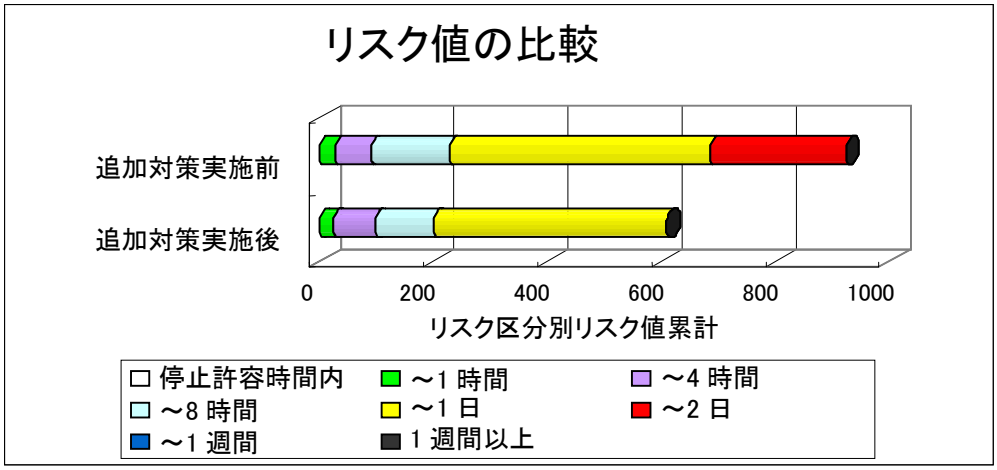


*A:「システムの安定稼働に対する脅威表」（当分科会で作成）

*B:「リスク分析ツール」（当分科会で作成）

5. 適用事例（架空会社）

リスク分析／リスク管理の手法を実際に架空会社に適用した。業務分析を行い、業務・サービスレベル対応表、業務・資産対応表、脅威一覧を分科会メンバーの実務経験を反映しながら作成した。リスク評価作業として、この基礎資料をもとに適用する対策とそのコストおよび効果の組合せにより複数のリスク分析表を作成した。リスク管理として、リスク分析表の結果から最適なリスク対策を選択した。リスク管理にて、選択した対策の効果を表したのが下図である。



近年、情報システムにおけるリスクマネジメントは、企業経営のリスクマネジメントの一要素として考えられてきている。全社的なリスクマネジメントシステムのポリシーにしたがって、情報システムのリスクマネジメントも行われていくことになる。方針の策定、対策の選択基準、実施対策のチェック体制、経営によるレビューなどは、生産や販売に関わるリスクマネジメントとベクトルを合わせて遂行していくことになるであろう。