IT資産のリスクマネジメント

松本健吾

システムリスクが単に災害・障害リスクを意味する時代から、システムリスクがビジネスリスクに直結する時代になった今、情報システムを取り巻く環境の不確実性への対応を第一に考えたIT（情報技術）資産のリスクマネジメントが求められている。ビジネス戦略の継続的な実行を可能にするためには、経営の主導のもとで、人的資産、知的資産を含む6つのIT資産について、戦略リスク、情報セキュリティリスクなど8つのシステムリスクの有無とその影響を評価し、リスクに事前に対応する必要がある。

システムリスク・マネジメントの重要性

昨今、「競合会社が新しいサービスを開始したことに対抗するため、早急に新サービスを追加しなければならない」とか、「電撃的に事業買収がなされたため、取引先や扱い品目が増え、計画を大幅に上回る取引が発生することになった」など、経営環境の変化は急激になってきている。

今や、ビジネス基盤として欠かせないものとなった情報システムは、業務面での仕組みづくりを支援することと併せて、急激な経営環境の変化にスピーディーに対応できるものでなければならない。

かといって、ビジネススピードの低下を招かないよう、期限に間に合わせるために、突貫工事でシステム構築を行えば、障害発生の危険性を有する脆弱な情報システムになる。このような情報システムは、ビジネスの足かせとなり、「不良資産」という烙印を押されてしまう。

こうした事態を回避するために、CIO（最高情報責任者）をはじめ、情報システムの運営を担う者は、情報システムを取り巻く環境の不確実性と、情報システム自体が持っている脆弱性とを共に「システムリスク」としてとらえ、その評価をCEO（最高経営責任者）をはじめとする関係者に説明すると同時に、リスクに対して事前に手を打ち続けることが求められる。

これが、いわゆるシステムリスク・マネジメントである。特に環境の不確実性への対応が、これまで以上に重要になっている。

システムリスクの再定義

システムリスク・マネジメントを行うためには、まずシステムリスクの対象となるIT資産とはどういうものかを整理しておく必要がある。NRI野村総合研究所では、情報システムの運営を担う者が中長期的に経営の観点でマネジメントすべきIT資産は、表1に示す6つであると考えている。

従来、システムリスクとして考えられてきたのは、主にファシリティ資産に関するリスクで、地震、

表1　6つのIT（情報技術）資産

IT資産	概要
業務システム資産	ソフトウェア、データ、設計書などのドキュメント
システム基盤資産	ハードウェア、ミドルウェア、ネットワーク
人的資産	IT関連組織の人材、構成、スキル
関係資産	ベンダーとの関係、経営・利用者との関係
知的資産	新技術の研究開発、ITサービスプロセスの知識、製品の評価
ファシリティ資産	コンピュータセンター、サーバー設置ルーム

表2　8つのシステムリスク

システムリスク	概要
災害・障害リスク	地震、火災、停電、運用トラブルなどによるシステムダウン
情報セキュリティリスク	情報漏洩やデータ改ざん
戦略リスク	経営環境の変化に業務システムの対応が遅れる
プロジェクトリスク	採用しているシステム基盤技術が業界標準から外れる
人材リスク	IT部門における人材のスキルのミスマッチや、中核人材の退社
契約リスク	運用委託先の企業体の変化や技術力の低下
定着リスク	導入した情報システムが活用されていない
知的財産リスク	IT部門の貴重な経験やノウハウが喪失する

火災、停電や、運用トラブル、ソフトウェアバグなどによる災害・障害リスクであった。

しかし昨今では、情報漏洩やデータ改ざんなどが企業に与える損害の大きさから、ファシリティ資産以外の、いわば情報資産に関する情報セキュリティリスクに対する認識が強まっている。また、知的資産の重要性への意識の高まりもあって、ビジネスモデル特許の侵害などもリスクとして認知されている。

そこで、改めてシステムリスクを定義すれば、「ビジネスに何らかの悪影響を与えうるシステム上の問題」ということになる。前述したような各IT資産の有効性、効率性、安全性を不確かにするものが、今日的なシステムリスクである。こうした観点からは、災害リスクや情報セキュリティリスクも含めて、表２に示すようなさまざまなリスクが考えられる。

リスク評価の手順

戦略リスクを例に、リスク評価の手順を述べる。基本的には、災害・障害リスクのそれと大きく変わるものではない。

①目的の明確化（評価の対象と目標の明確化）

ビジネス戦略を遂行する基盤を整備するためには、適切なタイミングで、適切なIT資産を対象に、適切なレベルで投資を行うことが必要である。そのために、まず「業務システム資産」と「システム基盤資産」のなかから、戦略との関連性に基づいて評価の対象を設定していく。

②リスクの発見と確認（リスク洗い出し、現状確認、不確実性の抽出、過去のトレース）

経営中期計画などに盛り込まれた環境変化への対応課題に基づいて、情報システムに影響を与える事象を洗い出す（例えば、出店エリアや数の拡大など）。この際、対応課題に修正、追加などがないかも確認しておく。

③リスクの分析（シナリオ設定、影響測定）

上記のような事象が起きる時期や規模などについて、いくつかのケースを想定し、ビジネス面での取り組みを想定しながら、それぞれの場合のシナリオを設定する。そして、それぞれのシナリオにおいて、ビジネス面と情報システム面へどういう影響があるかを把握する。

システムリスク・マネジメントは、システムの稼働を維持することが目的ではなく、最終的にはビジネス戦略を継続的に実行できるようにするために行われるものである。したがって、リスク評価の一連の活動は、経営の主導のもとで実施されるべきである。

『ITソリューションフロンティア』
2003年４月号より転載

松本健吾（まつもとけんご）
ITマネジメントコンサルティング部上級システムコンサルタント