事業継続に必要な情報システムの継続性確保を目的とした情報システムリスクマネジメントに関する考察

Discussions on information system risk management with the purpose of IT continuity assurance for business continuity

渡辺　研司
Kenji Watanabe

長岡技術科学大学大学院技術経営研究科
Management of Technology, Graduate School, Nagaoka University of Technology

要旨

現代社会・経済がますます依存性を高める情報システムの継続性を脅かす要因群を、事業継続マネジメント（BCM）の観点から情報システムリスクマネジメントを通じて、IT 継続性を確保するあり方についての議論を展開する。その過程において、情報システムリスクの定義・モニタリング・シミュレーション・評価をする枠組み（フレームワーク）の構築や、早期警戒指標の開発を通じた動的（ダイナミック）なマネジメントの可能性などについての論点も提供する。

1. はじめに

情報処理やネットワーク技術の発達と低コスト化により、企業活動においてもその商品・サービスの提供や、外部との取引、事務処理などに積極的にそれらの技術を投入し続けている。これに伴い、企業活動におけるデータ処理のスピードと取扱量は急増し、情報システムへの依存性も高くなってきている。一方、情報システムの障害による業務中断などで、予想以上に有形無形の損失を被るケースも散見されるようになり、経済活動を支える情報システム関連のインフラストラクチャの脆弱性は増加していると言える。本発表では、このような企業活動における情報システムに係るリスクを定義し、そのビジネスへの影響を評価する手法を検討し、マネジメント体制としてあるべき姿を、概念的なフレームワークとして提示することを目的とした。従来の情報システムリスクのマネジメントに関する研究は、技術面で解決を試みるアプローチが主流で、実際の対応に必要な運用やオペレーション、組織といった観点からのアプローチは極めて限定的かつ、単発的であったことから、本発表はその部分についての統合アプローチを提示することを試みたものである。

2. 情報システム障害の伝播速度の高速化と到達範囲の広域化

ここ数年で発生したシステム大規模障害とそのビジネスへの影響を分析すると、情報システムの導入以前のシステム開発前後の問題として、（1）マルチベンダー管理能力の欠如、（2）２００７年問題（業務・システム経験の欠如）、（3）ＩＴオフショアリングと優秀な人材不足、（4）ユーザー検収における責任体制の欠如の４点などが抽出できる。その他全体にかかわる構造的な問題として、社会インフラを支えるような大規模システムの設計を、そのシステム思想の定義から実際の構築を経て導入・運用に至るまでのプロジェクトを一気通貫でマネジメントできるような人材（PM: Project Manager-プロジェクト・マネジャー）が極め不足している現状も確認される。また、個別システムにおけるマネジメントもさることながら、個別企業は保有しているシステム群を個別のオペレーションシステム、ハードウェア、ソフトウェア、ネットワークのバージョン、技術的な寿命、相互依存性、品質などをベースに全体ポートフォリオとして統合管理するようなシステム企画・管理体制の構築も経営上の大きな課題と言える。[１]このような経営課題への取組みは、「障害伝播速度の高速化」、「障害伝播到達範囲の広域化」、「他者からの影響の可能性」といった傾向が強くなる状況を勘案すれば、個別企業のレベルに留まらず、サプ

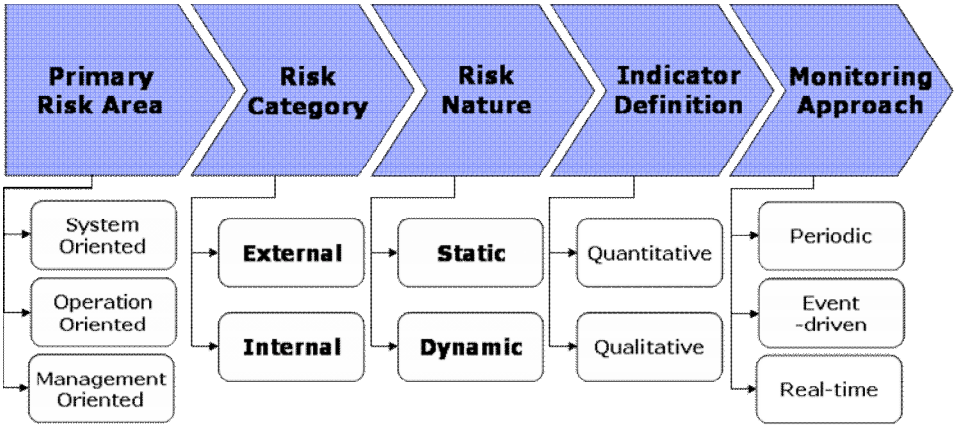
ライ・チェーン全体や業界レベルで議論すべきタイミングを迎えたということが言える。

3. 情報システム運用の多様化に伴う新たな情報システムリスク要因

企業を取り巻く経営環境の厳しさが増す中、専門性を有する外部企業への業務委託により、業務の高度化・効率化を図り、業務運用コストの削減を目的として導入を推進している新しいオペレーション形態に注目する必要性が高まっている。［2］ＩＴアウトソーシングについては、企業の情報システム関連業務のうち、企画の一部、開発・導入、運用・保守が、外部のシステム・ベンダーほかにアウトソースされ始めている。企業活動におけるＩＴ関連業務のアウトソーシングに係わる潜在リスクとして、サービス提供における可用性、安定性、安全性の観点から、アウトソーサーへの依存度増加に伴い、サービス可用性・サービス・レベル（品質）・セキュリティ・信用（アウトソーサー自体の）といった分野において諸リスクが増大する可能性が出てきている。特に昨今のＩＴ、システム、ネットワークの不具合に起因する諸事故を考慮すると、有事（自然災害、人的災害といったディザスター）の際に、アウトソースを実施している業務の可逆性を如何に確保できるか、ということが、今後、重要になってくると思われる。[３]具体的な対応として、アウトソーサー選定基準の強化、ユーザーグループの組成に加え、業界内における業務プロセスやデータの標準化による相互補完体制の導入等の施策を検討する必要がある。

4. リスク・マネジメントに有効な先行指標の開発と、MIS（経営情報システム）ベースのマネジメント体制の概念フレームワーク

情報システム関連リスクが多様化し、リスク・マネジメントの方法や体制も、物理的・技術的側面のみならず、経営面も含めた新たな諸リスクに則したモデルに変えてゆく必要性が認識されつつあることから、計量化のモデル構築や分析の枠組み、経営判断を支援するための経営情報システムの構築、更には組織内外向けのリスク・コミュニケーションを、正確かつ柔軟性を持って実施できるルールやツールの早急な開発が望まれる。このような仕組みの実効性を確保するためには、継続的な知識・経験の共有（ナレッジ・シェアリング）と、データや計画の継続的なメンテナンスが不可欠であり、また、更にこの仕組みを効果的に運用するためには、リスク要因に係る先行指標の開発が有効であると考え、一連の指標群を整理した。また先行指標の実際の開発には、データの性質（static：静的、dynamic：動的）、レベル表記の方法（定量的、定性的）、またどのような頻度やタイミングでデータを収集するべきか、といった定義が必要となることから整理を試みる。（[図１]、[表１]）



[図1] 情報システム関連リスクに係るマネジメント指標開発のアプローチ

[表1] 情報システム関連リスクに係る先行指標開発（例示）

Category 1	Category 2	Category 3	Potential Risk (Example)	Nature	Indicator	Monitoring Approach
System	Internal	Hardware	Hard disk failure	Static	Qualitative	Event-driven
		Software	Critical bug realization	Dynamic	Quantitative	Periodic
		Network	Network down	Dynamic	Quantitative	Real-time
		Infrastructure	Power failure	Dynamic	Quantitative	Real-time
	External	Hardware	Stop running with overcapacity	Dynamic	Quantitative	Real-time
		Software	Program version unmatch	Static	Qualitative	Event-driven
		Network	Slow communication	Dynamic	Quantitative	Real-time
		Infrastructure	Closed traffic (no access to office)	Dynamic	Qualitative	Event-driven
Operation	Internal	Human resource	Regional -wide epidemics	Dynamic	Quantitative	Event-driven
		Transaction	Unexpected irregular transactions	Dynamic	Quantitative	Real-time
	External	Human resource	Decrease in skill level	Static	Quantitative	Real-time
		Transaction	Unexpected slow performance	Dynamic	Quantitative	Real-time
		Contract	Very limited SLA	Static	Qualitative	Event-driven
Management	Internal	Staff skill	Lack of necessary skills	Static	Qualitative	Periodic
		Staff availability	Unexpected high turnover	Dynamic	Quantitative	Real-time
		Compliance	Criminal fraud	Dynamic	Qualitative	Real-time
	External	Vendor	Multi-vendor management failure	Dynamic	Qualitative	Event-driven
		Project	Project management failure	Dynamic	Qualitative	Periodic
		Other banks	System integration failure	Dynamic	Quantitative	Real-time
		Natural disasters	Earthquake	Dynamic	Quantitative	Real-time
		Human disasters	Terro-attack	Dynamic	Qualitative	Real-time

また、企業経営の運用レベルごとに内在するリスク要因と、それらの連関を勘案したマネジメントが不足した場合、最終的にはリスク要因の認識もれや、過小評価といった結果をもたらすことになるから、リスク要因間の相互依存性の分析も重要なポイントとなる。以上で考察したような経営情報システムをベースとした経営判断とリスク・コミュニケーションの枠組みが確立されれば、システム障害の発生前に障害要因の事前対処や発生時のための事前準備が可能となるのみならず、障害発生後の復旧作業や復旧後の枠組みへのフィードバックについても可能となり、強固な事業継続体制が構築されることとなる。

5. まとめ

本発表では経済・社会活動が情報システムへの依存性を高めつつあり、その一方で急増する脆弱性に関するリスクの定義、計量化の可能性、先行指標の開発について議論を展開する。その背景には、情報システムに係るリスク・マネジメントはもはや個別企業だけの経営努力では完結し得ないレベルが要求されるような状況になっている、ということがあると言える。特に重要社会インフラにおける情報システム関連障害に対する取組みについては、２００５年４月に内閣官房情報セキュリティセンターが設置され、今後は業界毎に脆弱性情報を共有するような仕組み（ISAC: Information Sharing & Analysis Center）が構築されつつある［4］が、そのような活動においてもリスク要因定義の標準化や計量化された指標での議論やモニタリング体制が、効率的な運用には不可欠であると考える。

参考文献

[1] Finne, T., “Information Systems Risk Management: Key Concepts and Business Processes”, *Computers & Security*, 19, pp.234-242, 2002

[2] Earl, M., “The Risk of Outsourcing IT”, *Sloan Management Review*, Volume 37, No.3 , pp.26-32, 1996

[3] Suh, B. and Han, I. “The IS risk analysis based on a business model, *Information & Management* “, 41, pp.149-158, 2003

[4] Watanabe, K., “Economical efficiency of outsourcing at bank operations: consideration with “risk-adjusted” point of view”, *Hitotsubashi Journal of Commerce and Management* 37, pp. 39-55. Hitotsubashi University, 2002

[5] 内閣官房高度情報通信ネットワーク社会推進戦略本部、“ 我が国の重要インフラにおける情報セキュリティ対策の強化に向けて ”（第２次提言）、２００５年