社会システムにおけるリスクマネジメント考
ソフトウェア製品及びシステム製品におけるリスクマネジメントの場合

文教大学大学院情報学研究科 講師 (兼任) 夏目 武†

Takeshi Natsume†

あらまし リスクマネジメントの一般的動向とソフトウェア製品及びシステム製品に関するリスクマネジメントのあり方の現状を解説し，内在する諸問題の解決としての課題を考察する．

キーワード：リスクマネジメント，ハザード，ビジネスリスク，安全リスク，プロジェクトリスク

近年，リスクという用語が新聞や雑誌等に頻繁に現れる．不利益を被る発生の予想を強調する場合と，損害としての大きさを予想し話が進展する場合があり，いずれもあいまいな事象の発生を想定した将来への危惧を記述している．実践的リスク管理，リスク開示，リスク情報，資産リスク，投資リスク，貸し出しリスク，倒産リスク，焦げ付きリスク，投機リスク，戦略的リスク，不安要因リスク，司法リスク，暖冬リスク，自然災害リスク等いろいろな表現として飛び交う．本来，工学的には両者を合わせた 2 次元量のベクトル量の大きさとして定義されている．現状はこの 2 要素の 1 要素のみが強調され，管理目標や予防行動の指標等として取り扱われている．

用語，リスクマネジメントは 1960 年代に現れる．1980 年代に現在に近い概念と手法が確立している．又，ソフトウェア製品及びシステム製品の分野のみならず，金融，社会科学等の分野においてリスクマネジメントが何らかの形態で導入されている．

工業製品やシステムにおけるリスクは ISO/IEC Guide 51(1995) : Safety aspects –Guidelines for their inclusion of standards[1] により概念整理が行われた．製品の使用時における，製品安全の概念がある．すべて可能性のあるリスクの特定とそれらの要因となる関連要素の削減，排除，最小限の残存リスクの容認とその為の予防対策を保証することで，消費者は安心して安全製品として保証された製品やシステムを規定の使用環境と条件の下に使用することが出来るようになる．又，故障の伝播とそれに伴う組織を含む人間系要素や環境要素の変動等の外部要因により障害発生と損害の大きさとして算出するモデル化が整備されつつある．これは信頼性工学と安全性工学の統合化を意味する境界領域の問題として整備が進められている [2]．

一方，ISO/IEC Guide 73 (2002): Risk management –Vocabulary– Guidelines for use in standards[3] が発刊された．ここでは広義にリスクの意味を展開し，リスクを事象の発生確率とその結果の組み合わせと定義している．その結果 (consequence) には負の期待値のみならず正の期待値もあるという展開である [4]．これは従来の信頼性，安全性工学の分野からすれば，あり得ない事であり，背反である．RISK の本来の意味の言葉として 3 百年続いた概念の変更への挑戦である．しかし，金融工学を主体とした投機リスクの場面では可能であり，この拡張概念のほうが取り扱いやすいと主張するのである．現在の特にこの社会経済情勢不安の時機に至って生じた混乱である．一般リスク，ビジネスリスク，安全リスク，プロジェクトリスク等，適用場面のキーワードを付加してその場を凌いでいる [5]．

ソフトウェアに特化した系統的なリスクマネジメントは 1980 年 MIL STD におけるソフトウェアの安全性管理プログラムに始まる．ソフトウェアとその関連システム環境要素が主たる観察される要因でシステムを危険な状況に陥ると思われるプロセスを分析し，特定して対策を事前に行うプログラムである．同等の手法は ISO/IEC 15026 (1998) : System and software integrity level[6] として国際規格のもとにまとめられている．先頃は，IEEE Std. 1540-2001: Standard for software life cycle process – Risk management[7] として学会規格が出版された．同時にこれは ISO/IEC JTC1 SC7 –Information Technology のもとに国際規格として準備が進められている．いまさら何を考えているのかという向きもあるが，大切なことは時代の要請であることを認識したい．近年の急速な IT 技術の発展と社会構造の変化は社会システムのみならず技術環境

2005 年 10 月 6 日受付
† 〒 253–8550 神奈川県茅ヶ崎市行谷 1100
natsume@shonan.bunkyo.ac.jp
† Graduate School of Information and Communication, Bunkyo University
1100 Namegaya, Chigasaki, Kanagawa 253–8550, Japan

文教大学大学院情報学研究科 IT News Letter Vol. 1, No. 1, pp. 6〜7 (2005)

や条件の変化をもたらし，システムの形態を変えつつある．

システムの一つの機能要素としてのソフトウェアも当然影響を受ける．特に生産性の高いこの機能単位は無制限に近い応用が展開される．当然，システムのハザードへと移行する大きなリスク要因を潜在させることになる．ハザード (Hazard) は国際規格で共通に potential source of harm と定義されている [8]．即ち，それは一つのシステムを考えた場合，系，構成機器類，稼働環境，関連人的要素として開発と設計と製造及びこれらに伴う総てに関する技術支援，運転と保守及び保守管理，系を取り巻く諸資源等に対して，危害や損害の発生する可能性のある要因であり，ハザードがあることはシステムの危険な状況を意味する．それは本来の論理機能の完全性からの逸脱もしくは欠点及び他のシステム構成要素からの機能的影響もしくは機能環境の変異による重大機能障害への移行の可能性を示唆している．

移行状態の可逆的な場合は従来の総合的な信頼性工学の領域で解けるが不可逆状況に陥った場合は安全性工学を含む総合的な工学手法で解くことになる．現社会の中で稼動するシステム群はかっての独立系の中の構成要素として安定した系の要素に収束していくプロセスとは異なる技術環境に移行していることを観察する．障害情報と分析等の情報に基づくフィードバックとしての継続的改善活動から漸次安定したシステム状態に移行する形態からフィードバックが局部的修復にとどまり，新たな障害発生要因もしくは条件の生成要因を形成し，定常的にはある残存リスクとしての系が擬似的平衡状態を保つことになる．系は外部のある条件の変化に依存的に偏重し，ハザード状態へ移行するプロセスを取ることになる．この状態に新たな特定の内的もしくは外的要素が付加することによりシステムは回復可能なシステム障害から系の制御機能を越えた状態に移行し，系は機能不能の障害に止まらず何らかの損失被害状況に移行する過程を取ることになる．この一連の過程の可能な限りの場合を分析し，評価することで事前にシステムの被害を避け，発生する損害を最小限にする諸活動がリスクマネジメントの基本である．危機管理との混同は避けるべきである [9]．

これらを支える工学的手法と問題解決の方法は総て信頼性工学の資産を適用することが有効である．データ収集方法，データ分析と統計確率的手法，リスク予知のための諸モデル化とそのモデルを用いた予測評価，段階的プロジェクト/プロダクト管理，安全設計と評価及び保証，構成管理と保全支援などの工学的諸技術が適用可能である．しかし，本来の諸リスクの問題解決の確立には至っていないのが現状である．それは実データのデータベース化が出来ていないことである．確率的リスク評価 –Probabilistic Risk Assessment (PRA) の提案は 1991 年の PSAM-1 シンポジュウム [10] 以来，繰り返し提唱されているか一般的モデルとしての手法は確立していない．実データを基本とした確率プロセスモデルが特定できないのである．国際規格では現在，例えば発生確率を 5 段階，被害の大きさを 4 段階に区分しリスクの大きさを 4x5 の枠に当てはめて特定する方法が推奨されている．系を安心して使用する安全なシステムの構築を目指したリスク マネジメントのこれからの課題は総合的な信頼性-Dependability と Risk 評価を結合したより精度の高い理論的モデル化 (PRA model)，モデル確率過程の計算と予測手法，それに伴うデータ収集と公的データベース整備である．金融リスクと安全リスクとの概念不一致の問題は適用分野が異なり，事象の場合を確率過程に置き換えられるならば，特に並存したとしても特に大きな問題ではない．これは自然に淘汰される一時的問題であろう．

〔文　献〕

1）ISO/IEC Guide 51(1996): Safety aspects – Guidelines for their inclusion in standards
2）渡辺，平尾，中村，斉藤：安全性技術の定量的費用か方法に関する考察，信学技法，vol.101(2001) No.505.
3）ISO/IEC Guide 73(2002): Risk management – Vocabulary – Guidelines for use in standards
4）向井康晴: リスク バジェッティングとオルタナティブ投資の実践 野村證券グループ応用金融工学研究部門 (加藤康之) 講義録 2005/07/02
5）IEC 62198(2001): Project risk management – Application guidelines
6）ISO/IEC 15026(1998): System and software integrity level
7）IEEE Std. 1540-2001: Standard for software life cycle process – Risk Management
8）IEC 61882(2001): Hazard and operability studies (HAZOP studies) – Application guide
9）JIS Q 2001(2001): リスクマネジメントシステム構築のための指針 日本工業標準調査会 日本規格協会
10）Proceedings of PSAM-1(1991) Elsevier, NY.

夏目（なつめ）　武（たけし） 山梨県出身．1961 年立教大学理学部物理学科卒．独立法人国立筑波技術短期大学名誉教授，IEC/TC56-Dependability 委員会委員，電子情報通信学会，同　安全性研究専門委員会委員，日本信頼性学会評議委員，同 LCC 研究会主査を務める．2005 年 4 月より，文教大学大学院情報学研究科情報学専攻講師を兼ねる．情報学研究科では「ソフトウェア工学特論」を担当．専門研究領域は複合システム/ソフトウェアの信頼性安全性評価，解析，保証技術．