2008－DD－66 (3)
2008／6／6

内部統制におけるリスクとコントロールの考え方の提案

Proposals on the Selection-Method of Risks and Controls in Internal Control

根岸寛明[1], 梅田伸明[2], 明庭聡[3], 大沼啓希[4]

Hiroaki Negishi, Nobuaki Umeda, Satoshi Akeniwa, Keiki Ohnuma

[1]富士通マイクロエレクトロニクス(株), [2](株)NTTデータ, [3]日揮情報ソフトウエア(株), [4]日本アイ・ビー・エム(株)

Fujitsu Microelectronics Limited, NTT Data Corporation, J-SYS Software Co.,Ltd., IBM Japan,Ltd.
negishi.hiroaki@jp.fujitsu.com , umedan@nttdata.co.jp , akeniwa@jsys-soft.co.jp , KKEY@jp.ibm.com

【要旨】内部統制では組織の主要な活動について,業務プロセス,業務遂行上のリスク,および各リスクのコントロールを明確にし,業務の遂行をモニタリングしていく。統制の前提となる文書の作成において,RCM(Risk Control Matrix)の作成が最も困難である。ここでは,RCM作成の上の課題を解決するため,まず,リスクパターンの提示,次にリスクパターンに基づき,リスクの列挙⇒リスク発生原因の分析⇒対応策立案⇒コントロールの立案というプロセスを経ることによってリスクとコントロールを導き出す方法を提案し,その効果を検証する。

【Abstract】In the process of internal control, the business process is monitored based on the process flows and the risk control matrices. The risk control matrix development is the most difficult process in the internal control preparation step. We propose a simplified method to prepare the list of controls from the list of risks through the table of risk causes, countermeasures.

1. はじめに

内部統制[1]とは企業などの組織活動において,組織が健全かつ有効・効率的に運営されるよう業務のフローを定め,それに基づいて管理・監視・保証を行うことを指す。内部統制では組織の主要な活動について,業務プロセスおよび業務遂行上のリスクと各リスクのコントロールを明確にし,業務の遂行をモニタリングしていく。内部統制は,「業務の有効性・効率性」,「財務諸表の信頼性」,「関連法規の遵守」,および「資産の保全」の目的を達成するために,合理的な保証を提供することを意図した,企業・組織の全員によって遂行される1つのプロセスである。

日本では,財務会計分野において,金融商品取引法(俗称「日本版SOX法」)が2006年6月に成立,2009年3月期の決算から内部統制報告書の提出と公認会計士によるチェックが上場企業に義務付けられている。現在,2008年度から開始される財務会計分野における金融商品取引法対応の実運用を控え,運用の準備を済ませたところであり,99%の企業が財務会計分野における内部統制対応に着手済みといわれている。

内部統制対応では,上記の目的のため,まず業務とその統制内容を文書化する必要がある。文書化では業務活動の重要プロセスを選択し,選択した重要プロセスについて以降の文書を作成する。

- 業務と担当部署の流れを記述した「業務フロー図」
- 各業務の詳細を記述した「業務記述書」
- プロセスのリスクと各リスクのコントロールを記述した「RCM(リスクコントロールマトリックス)」

現在の内部統制対応は, 著者らも実業務を担当しているが,抽象的なガイドラインに基づき,試行錯誤で形を整えたもので,内部統制の目的の一部である「財務諸表の信頼性」のみに対応したものである。今後,必要とされる定期的な監査に基づく PDCA サイクルの運用,また,目的の一つである「業務の有効性・効率性」を果たしていくために,今回の試行錯誤の結果として得られたノウハウを内部統制対応の合理的な方法の形にまとめていく必要がある。ここでは, 著者らが実業務を通じて得た経験をもとに,内部統制の文書化で特に困難であった RCM の作成について,直面した課題とその課題を解決する四つの提案をする。

2. 提案

ここでの提案は,著者らが取り組んだ内部統制文書化の経験を持ち寄り,ノウハウとしてまとめたものである。提案はリスクパターンの提示と,以降の 4 つの提案である。

- リスク管理レベルの設定
- リスクパターンに基づくリスク識別
- リスクパターンを活用したコントロール検討
- 業務フローを利用したコントロール記述

2.1 リスクパターンの活用

リスクのパターン化ができないかと考え,失敗知識データベースを題材にリスク(失敗の原因)を分類した。失敗知識データベース[5] の失敗百選を素材とし,リスクパターンの観点から分析を行った。分析は失敗知識データベースの成果である原因,行動,結果の分析結果を基本にし,「ものづくり」の現場でのリスクの分類という観点から,試行錯誤により,4 人で通算 4 回行っている。

さらに,各リスク分類に,主な要因と対応策を対応させ,リスクパターンを作成した。対応策は,第 1 版として,失敗知識データベースの対応策の記述の他,内部統制対応の入門書として定評のある「内部統制の入門と実践」[6]から抜き出している。

分析結果のリスクの分類(運用時のリスクと設計時のリスクの２種類)とリスクパターンを以降に示す。

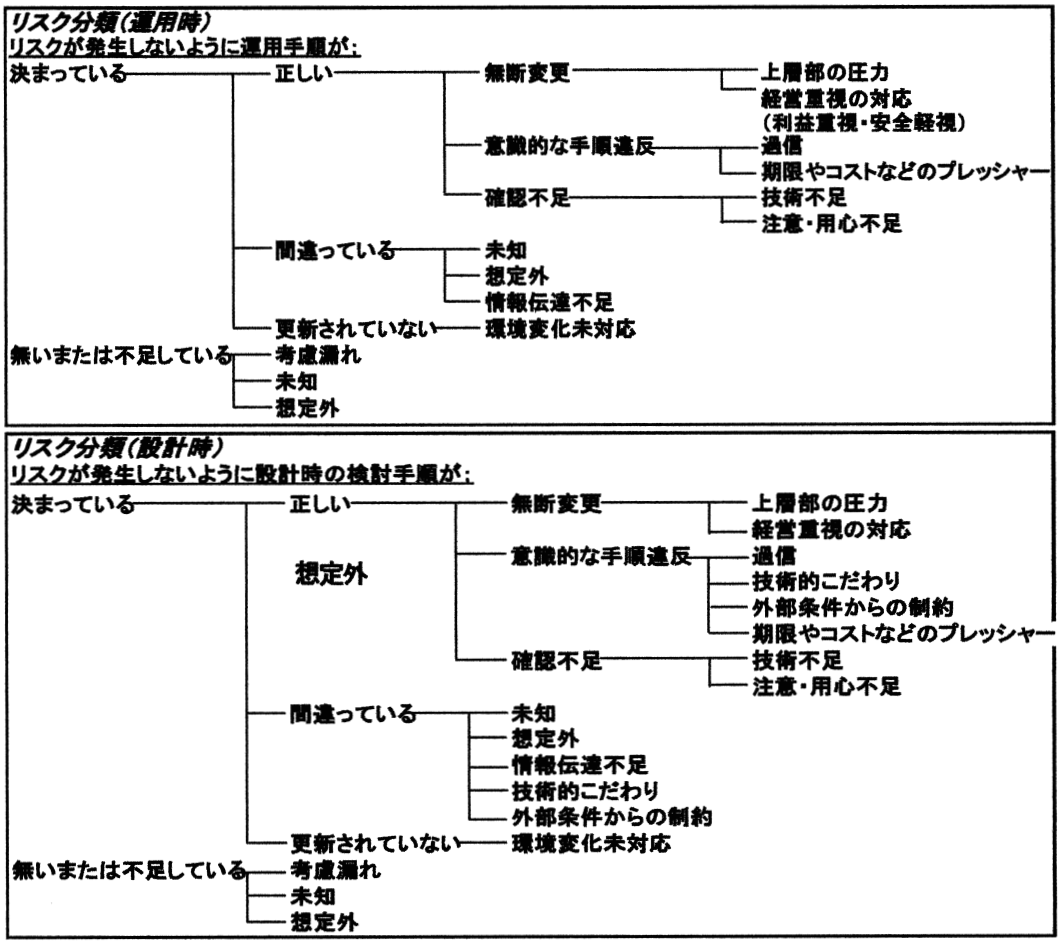

図1 リスク分類

表1 リスクパターン

リスク分類	主な要因	対応策		
		内部統制の入門と実践より	失敗百選より(設計)	失敗百選より(運用)
手順が無いまたは不足している	・考慮漏れ ・未知 ・想定外	・規程,マニュアルの整備	・設計基準の整備 ・過酷な条件,最悪シナリオの想定 ・関連情報,類似事例,過去の欠陥や問題点の収集・解析と手順への反映 ・仮想演習によるチェックの実施 ・不確定要素があれば余裕を持たせる ・技術者の専門領域間の情報伝達	・過酷な条件,最悪シナリオの想定 ・関連情報,類似事例,過去の欠陥や問題点の収集・解析と手順への反映 ・仮想演習によるチェックの実施 ・人事異動時の情報共有 ・設計基準を超えた場合の対処の想定

リスク分類	主な要因	対応策		
		内部統制の入門と実践より	失敗百選より(設計)	失敗百選より(運用)
手順が間違っている	・未知 ・想定外 ・情報伝達不足 ・技術的こだわり ・外部条件からの制約	・照合による妥当性の検証 ・証憑による事実の検証 ・業績などの指標の分析 ・異常値把握	・過酷な条件,最悪シナリオの想定 ・関連情報,類似事例,過去の欠陥や問題点の収集・解析と手順への反映 ・仮想演習によるチェックの実施 ・専門家の専門領域間の情報伝達 ・複合因子での発生を考慮し総合的に余裕度を設定 ・外国輸入技術の未消化適用をしない	・過酷な条件,最悪シナリオの想定 ・関連情報,類似事例,過去の欠陥や問題点の収集・解析と手順への反映 ・仮想演習によるチェックの実施 ・専門家の専門領域間の情報伝達
手順が更新されていない	・環境変化未対応	・照合による妥当性の検証 ・証憑による事実の検証 ・業績などの指標の分析 ・異常値把握	・最新技術の設計基準への反映 ・製品変更の際の発生しうる問題点の明確化と対応検討 ・不適切な手順の放置の禁止 ・過去の実績に準拠した基準の最新情報の確認	・不適切な手順の放置の禁止 ・過去の実績に準拠した基準の最新情報の確認
手順書の無断変更	・利益重視 ・安全軽視 ・上層部の圧力	・職務の分離・分掌 ・権限の移譲 ・定期的な配置転換	・安全対策には経費削減をしない ・コスト低減できる部分とできない部分を明確に区別する	・資金不足,人員不足,タイトなスケジュールの回避 ・関係者間の情報共有と責任体制の明確化 ・検査基準の整備
意識的な手順違反	・過信 ・技術的こだわり ・外部条件からの制約 ・期限やコストなどのプレッシャー	・上長による承認 ・照合による妥当性の検証 ・証憑による事実の検証 ・職務の分離・分掌 ・権限の移譲 ・定期的な配置転換 ・業績などの指標の分析・異常値把握 ・IT を利用した自動化 ・セキュリティ管理	・資金不足,人員不足,タイトなスケジュールの回避 ・関係者間の情報共有と責任体制の明確化 ・検査基準の整備	・運用状態を適切に確認できるようにする ・不具合発生を検出する機構の組込み ・検査基準の整備
手順の確認不足	・技術不足 ・注意・用心不足	・上長による承認 ・照合による妥当性の検証 ・証憑による事実の検証 ・業績などの指標の分析・異常値把握 ・IT を利用した自動化 ・セキュリティ管理	・関係者の技術水準の確認 ・検査基準の整備	・分かりやすく誤判断の起こしにくい手順,構造 ・誤操作や誤判断に対する安全対策の組み込み ・不具合発生を検出する機構の組込み ・検査基準の整備

2.2 リスク管理レベルの設定

内部統制文書化における問題点の 1 点目はリスク管理レベルをそろえる考え方が不明なことである。どのレベルに対してリスクの管理をするのかを明確にしておかないと,レベルの違いでリスクの規模と数に大きな差が出る。事前にリスク管理レベルをそろえておく必要がある。後になってからそろえることは困難である。

提案 1:リスク管理レベルの設定

- どのレベルの成果に対してリスクの管理をするのかを明確にする。

- 担当レベル,部門レベル,ビジネスプロセスレベルを一定にする。リスク管理レベルで業務フローを記述する詳細度(業務フローに記述すべきスイムレーンなど)が決まる。
- 業務の目標の裏返しがリスクになる。コントロールは1段下のレベルの業務(例えば, 課の業務は部のリスクに対するコントロール),さらに1段下のレベルのリスクがリスク発生原因になる。

● リスク識別の網羅性を管理目標でチェックする

- 管理目標は成果物と目標の観点の組合せで決まる。目標の観点は,内部統制の視点(業務の有効性及び効率性,財務報告の信頼性,等)や品質,期間/納期,コスト,個人情報保護,等々である。
- 管理目標を達成できない状況がリスクである。

2.3 リスクパターンに基づくリスク識別

内部統制文書化における問題点の2点目はリスクの識別(リスクの洗い出し)の際に何をリスクとして挙げればよいかが不明なことである。

● リスクの識別において,大きな個人差が生じる。同じような業務でも,ある人は100のリスクを,他の人は2のリスクを識別するということが起こり得る。その主な要因は,リスクをどのようなレベルで管理するのかという点で基本とすべき考え方がないことである。

● リスクやコントロールの網羅性をどのようにチェックすればよいかがわからない。リスクを識別する手順,コントロールを定義する手順が確立されていないため,チェックの視点が曖昧になる。

これらの課題を解決するため,リスクのモデルを設定し,リスクの識別の方法を確立する必要がある。

リスクは企業のミッション実現のための戦略を阻害するようなマイナス要因のことである。経営者から「企業のミッション」が提示され,業務にブレークダウンしていく段階で「戦略・戦術」が検討されるが,その「戦略・戦術」の遂行を阻害するようなマイナス要因がリスクである。そのため,業務の目標の裏返しがリスクになる。

提案2:リスクパターンに基づくリスク識別

● リスクパターンの各リスク分類に対応したリスクを検討する。

- 各成果物に対して,リスク分類のそれぞれに対応するリスクが存在するか(あり得るか)否かを検討し,存在するものについてリスクとして挙げる。

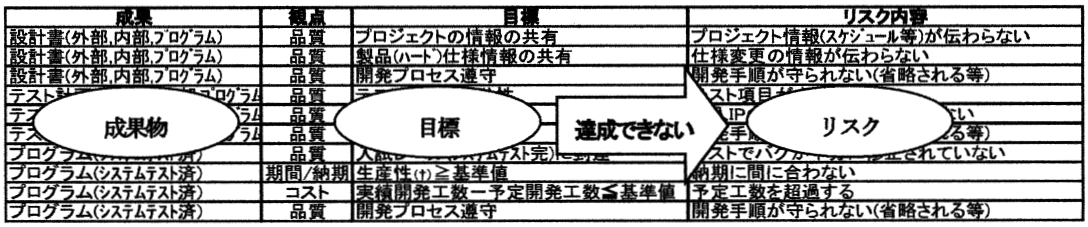

図2 リスク識別の例

2.4 リスクパターンを活用したコントロール検討

内部統制文書化における問題点の 3 点目はコントロールの記述方法が不明なことである。コントロールとしてどのようなことを挙げればよいかが不明なことである。内部統制の運用では各コントロールをモニタリングするが,どのようにコントロールを導き出すかによって,モニタリングの有効性に差が出る。

提案3:リスクパターンを活用したコントロール検討

- リスクパターン(リスク発生原因,対応策)を活用してコントロールを検討する。
  - ① ステップ 1: リスクに関連するリスク発生原因をパターンの中から特定する。
  - ② ステップ 2:リスク発生原因の対応策をパターンの中から特定する。
  - ③ ステップ 3:対応策(パターン)を業務に即した具体的な表現にし,コントロールを定義する。

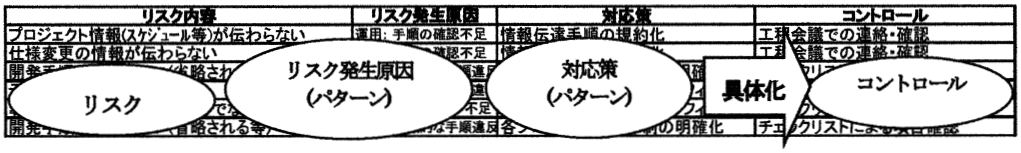

図3 コントロール検討の例

2.5 業務フローを利用したコントロール記述

リスクに対するコントロールは1段下のレベルの業務(例えば,部のリスクに対するコントロールは課の業務)である。さらに一段下のレベルのリスクがリスク発生原因になる。コントロールの記述に際して,業務フローの記述の詳細度に記述レベルを合わせる。

提案4:業務フローを利用したコントロール記述

- 業務フローを利用してコントロールの記述レベルを合わせる
- 1段下のレベルの業務をコントロールとする。
- コントロールに対するリスクを識別しないこと。無限ループ(コントロールのリスク,コントロールのリスクのコントロールのリスク,・・・)に陥る。

3. ソフトウェア開発プロセスでの検証

ソフトウェア開発フローをサンプルとして提案の方法を適用して我々の方法を検証した。採用したソフトウェア開発プロセスは,実際に適用されているプロセスをベースに,ソフトウェア開発技術関係の教科書[2],[3],[4]等で解説されている一般的なソフトウェア開発プロセスを参考にしたものである。

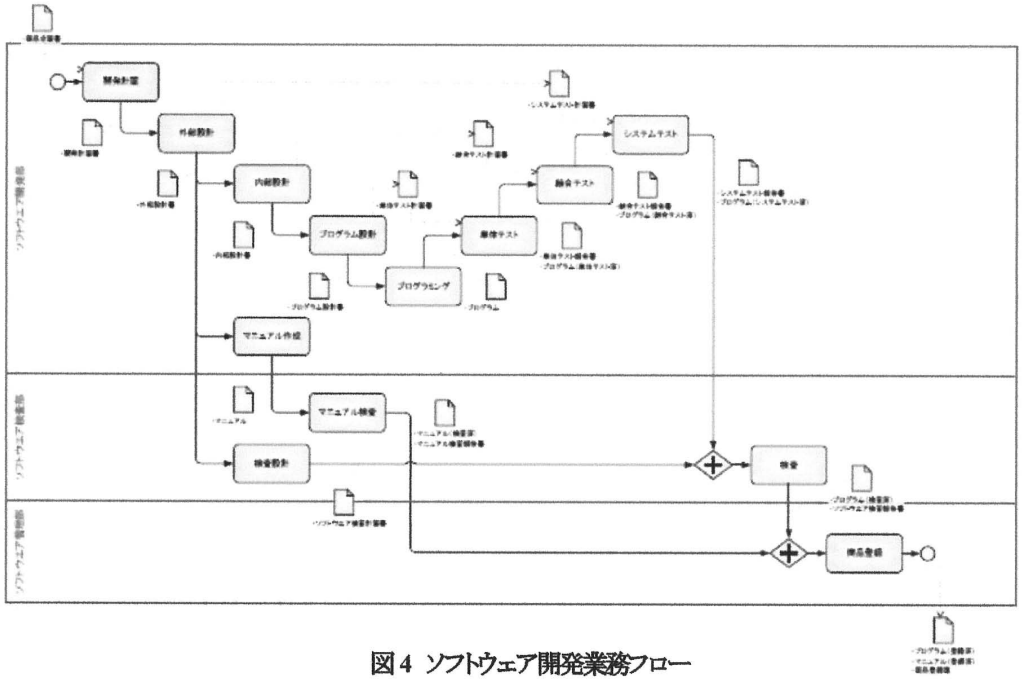

図4 ソフトウェア開発業務フロー

リスクパターンに基づくリスク識別,リスクパターンを活用したコントロール検討,および業務フローを利用したコントロール記述を実施し,抜け,漏れの確認が可能なことを確認した。

表2 ソフトウェア開発業務のRCM(一部)

No.	開発プロセス	担当部署	成果物	観点	目標	リスク内容	リスク発生原因	対応策	コントロール
1	ソフトウェア開発	ソフトウェア開発部	設計書(外部,内部,ﾌﾟﾛｸﾞﾗﾑ)	品質	プロジェクトの情報の共有	プロジェクト情報(スケジュール等)が伝わらない	運用: 手順の確認不足	情報伝達手順の規約化	工程会議での連絡・確認
2	ソフトウェア開発	ソフトウェア開発部	設計書(外部,内部,ﾌﾟﾛｸﾞﾗﾑ)	品質	製品(ハード)仕様情報の共有	仕様変更の情報が伝わらない	運用: 手順の確認不足	情報伝達手順の規約化	工程会議での連絡・確認
3	ソフトウェア開発	ソフトウェア開発部	設計書(外部,内部,ﾌﾟﾛｸﾞﾗﾑ)	品質	開発プロセス遵守	開発手順が守られない(省略される等)	作成: 意識的な手順違反	各プロセスの責任体制の明確化	チェックリストによる手順確認
4	ソフトウェア開発	ソフトウェア開発部	ﾃｽﾄ計画書(外部,内部,ﾌﾟﾛｸﾞﾗﾑ)	品質	テスト項目の十分性	テスト項目が十分でない	作成: 意識的な手順違反	最新技術の作業基準へのフィードバック	チェックリストによる項目確認
5	ソフトウェア開発	ソフトウェア開発部	ﾃｽﾄ計画書(外部,内部,ﾌﾟﾛｸﾞﾗﾑ)	品質	導入IPの品質確保	導入IPの評価やテストが十分でない	作成: 手順がない/不足	最新技術の作業基準へのフィードバック	チェックリストによる項目確認
6	ソフトウェア開発	ソフトウェア開発部	ﾃｽﾄ報告書(外部,内部,ﾌﾟﾛｸﾞﾗﾑ)	品質	開発プロセス遵守	開発手順が守られない(省略される等)	作成: 意識的な手順違反	各プロセスの責任体制の明確化	チェックリストによる項目確認
7	ソフトウェア開発	ソフトウェア開発部	プログラム(システムテスト済)	品質	入試レベル(システムテスト完)に到達	テストでバグが十分に修正されていない	作成: 意識的な手順違反	各プロセスの承認体制の明確化	チェックリストによる成果物確認
8	ソフトウェア開発	ソフトウェア開発部	プログラム(システムテスト済)	期間/納期	生産性(↑)≧基準値	納期に間に合わない	作成: 手順がない/不足	最新技術の作業基準へのフィードバック	チェックポイント設定による中間チェック
9	ソフトウェア開発	ソフトウェア開発部	プログラム(システムテスト済)	コスト	実績開発工数≦予定開発工数≦基準値	予定工数を超過する	作成: 手順がない/不足	最新技術の作業基準へのフィードバック	チェックポイント設定による中間チェック

さらに,一般的な意味でのソフト検査業務では,検査設計書に対するコントロールがないことを発見した。検査設計書のコントロールは,一般的な品質の良否ではなく,そのソフトウェアに対する要求事項等々,ユーザが使用する場合の事項が検査されているか否かに関するものになるはずである。これにより,我々の方法が業務フローの改善に関する分析にもつながるものであることが確認できた。

4. まとめと今後

白紙の状態から取り組んできた内部統制対応作業から,内部統制対応の効率化・高度化,さらには内部統制の本質ともいえる業務フロー改善にもつながるノウハウをまとめることができた。我々の方法は, リスク分類(パターン)を活用したリスク識別,リスク分類に対応策(パターン)を対応させ,それをコントロールとして具体化させるという,個別事象とパターンとを組み合わせることで,リスクやコントロールの粒をそろえようというアプローチである,

リスクのモデルとした失敗知識データベースは,機械,建築,化学等,我々が扱っている ICT の世界とは素材が異なるが,「ものづくり」の観点から,その他の分野にも適用可能と考えている。ICT の分野の失敗事例も分析例に加え,適用可能であることを検証していく必要がある。

分析結果を著者らの身近なソフトウェア開発プロセスに適用した。適用の結果として得られた改善点を実際のソフトウェア開発フローの改善につなげていきたい。今後,ソフトウェア開発以外への適用・検証が必要である。

リスクパターン(リスク分類,リスク発生原因,対応策)はデータベース化し,今後のブラッシュアップに備える。まず,リスク,リスクパターン,対応策パターン,コントロールの構造を整理し,XML で表現することに取り掛かっている。

最後に,この研究は XML コンソーシアム「内部統制勉強会」の成果である。通常では協働できない方々との協働の場を提供していただいたことに感謝する。また,失敗知識データベースの存在と所在を教えていただいた牧野友紀さん,失敗知識データベースの分析に貢献していただいた安藤一幸さんに感謝する。

【参考文献】

[1] 内部統制の統合的枠組み(理論篇) トレッドウェイ委員会組織委員会(鳥羽至英,他訳) 白桃書房 1996 年

[2] ソフトウェア工学理論と実践 シャリ・ローレンス・ブリーガー(堀内泰輔訳) ピアソン・エデュケーション 2001 年 11 月 ISBN4-89471-368-3

[3] よくわかるソフトウェア開発の基本と仕組み 谷口功 秀和システム 2002 年 7 月 ISBN4-7980-0344-1

[4] 図解でわかるソフトウェア開発の実践 Mint(経営情報研究会) 日本実業出版社 2002 年 12 月 ISBN4-534-03510-1

[5] 失敗知識データベース(http://shippai.jst.go.jp/)

[6] 内部統制の入門と実践 佐々野未知 中央経済社 2006 年 1 月 ISBN978-4-502-27550-0