SAAJ近畿支部　第157回定例研究会

システム監査の多様性について

2016年1月15日

日本システム監査人協会　近畿支部

林　裕正

目次

■自己紹介

■システム監査の多様性

■システム開発プロジェクトの監査

★本資料の内、意見等に関わる部分は全て講演者個人見解です。

システム監査の多様性

■テーマ選定の背景
■システム監査学会主催イベントの統一論題
■システム監査講演会の講演テーマ
■システム監査技術者試験の出題範囲
■公認システム監査人の得意分野
■システム監査に関係した出来事
■多様性をもたらす要因
■多様化するシステム監査へ向けて

参考資料

■システム監査学会　研究大会・公開シンポジウム　講演資料
■情報ｼｽﾃﾑ・ﾕｰｻﾞ会連盟　システム監査講演会　講演資料
■システム監査技術者試験　出題範囲・シラバス（IPA資料）
■公認システム監査人　公開名簿（協会HP）
■日経コンピュータ誌　「動かないコンピュータ」
■SAAJ　月例研究会　講演資料
■SAAJ近畿支部　定例研究会　講演資料

テーマ選定の背景（1）

システム監査学会　第25回公開シンポジウム（2012年）

＜開催趣旨＞

最近、銀行システム開発の中止／頓挫を巡る損害賠償の裁判、特許庁システムの開発中断、インフラトラブルによるソリューションシステムの停止、サイバーテロによる個人情報・機密情報の流失およびバグによる業務アプリケーションの中断等、システム監査の必要性が叫ばれています。このように、各方面、各分野において**多様なシステム監査**の必然性が求められています。

テーマ選定の背景（2）

システム監査学会　研究プロジェクト（２０１４年度～）

システム監査の多様性 研究プロジェクト（主査：荒牧裕一氏）

＜プロジェクトの概要＞

ICTを利用した情報システムが高度化し適用範囲が広がるに従って、情報システム関連の評価に対する要求も多様化し、システム監査においても従来と違う視点が求められている。

本研究会では、ビッグデータ、知的財産保護、SNS等の多様化する情報システムについて、システム監査の視点からの検討を行っている。研究会での討議を通じて、知識の整理と相互研鑽の場とする。2015年度も、引き続き、多様性のテーマについて発表と討議を行う（マイナンバー制度、クラウドサービス、知的財産権、IoT等）。

多様性に関する視点

対象組織の多様性

民間企業
→　公共団体
　　非営利団体
→教育機関等

目的の多様性

信頼性・安全性・効率性
＋
適法性・利便性・
　　経営戦略適合性

技術の進歩　→　リスクの拡大・変容

クラウド　ビッグデータ　SNS　オープンソース
スマホ　仮想化　モバイル端末　サイバー攻撃
IoT　人口知能　BYOD　　etc

SAAJ近畿支部第153回定例研究会(2015.7.17)資料より荒牧氏の了解を得て引用

システム監査学会主催イベント 統一論題

開催年度	研究大会	公開シンポジウム
2007年度	経営の統制基盤を支えるシステム監査	新ICTによる変貌する社会とシステム監査
2008年度	今求められる経営の変革の視点とシステム監査	経営インフラを支えるシステム監査 ービジネス改革・内部統制から工事進行基準までー
2009年度	MOT（技術経営）、リスク管理、そしてシステム監査の連携	クラウド時代とシステム監査の役割 来るべきｸﾗｳﾄﾞｺﾝﾋﾟｭｰﾃｨﾝｸﾞと専門的な診断の視点
2010年度	システム監査 ー グローバル化への対応 ～IFRS・XBRLの動向とシステム監査の視点～	クラウドコンピューティングの進展とシステム監査
2011年度	リスクマネジメントとシステム監査 ー東日本大震災からの考察ー	想定外脆弱性時代の経営
2012年度	システム監査の新しいステージ	多様性が求められるシステム監査
2013年度	ビッグデータ時代における統制 ーシステム監査の研究と活用ー	個人情報の共有とシステム監査
2014年度	ITの進化とシステム監査	安心安全な社会生活とシステム監査
2015年度	レピュテーションリスクマネジメントとシステム監査	マイナンバー制度とシステム監査

システム監査講演会 講演テーマ

開催年度	基調講演・テーマ
2006年度	ニッポンの内部統制報告制度の課題と展望 サイバー犯罪の最新動向とシステム監査における留意点
2007年度	2つの内部統制　～会社法と金融商品取引法～ 働く人のメンタルヘルス
2008年度	我が国の情報セキュリティ政策の概要 ライフサイクル思考に基づいた環境経営戦略とグリーンIT
2009年度	ISACA/ITGIの提唱するITガバナンスと国際的動向 クラウドが企業情報システムとIT業界に与えるインパクト
2010年度	なぜクラウドが内部統制を楽にするのか？ IFRS(国際会計基準)が及ぼす情報システムへの影響と対応について
2011年度	危機管理に対応するシステム監査～サイバーから震災まで～
2012年度	グローバル・クラウド時代に向けたシステム監査のありかた
2013年度	企業内ICTのクラウド活用とシステム監査－クラウド監査事例を切り口に－
2014年度	情報セキュリティとシステム監査
2015年度	施行待ったなし!!マイナンバー直前対策とセキュリティ監査

システム監査技術者試験 出題範囲

■IPA公開HP（2015年10月改訂版）より引用

1. 情報システム・組込みシステム・通信ネットワークに関すること

経営一般，情報戦略，情報システム（アプリケーションシステム，ソフトウェアパッケージ，クラウドコンピューティング，モバイルコンピューティングなどを含む），組込みシステム，通信ネットワーク（インターネット，有線及び無線LANなど），ソフトウェアライフサイクルモデル，プロジェクトマネジメント，IT サービスマネジメント，インシデント管理，ITリスク管理，品質管理，情報セキュリティマネジメント及び情報セキュリティ関連技術（不正アクセス対策，サイバー犯罪対策，マルウェア対策などを含む），業務継続管理 など

2. システム監査全般に関すること

IT ガバナンス，IT 統制，情報システムや組込みシステムの企画・開発・運用・保守業務の監査，業務継続管理の監査，システム開発プロジェクトの監査，情報セキュリティ監査，個人情報保護監査，他の監査（会計監査，業務監査）との連携・調整 など

3. システム監査の計画・実施・報告に関すること

監査計画，リスクアプローチ，監査の実施，監査報告，フォローアップの実施，CAAT（データ分析ツール，電子調書システムなど），ディジタルフォレンジックス，CSA，システム監査業務の管理（監査業務の品質管理を含む） など

4. システム監査関連法規に関すること

情報セキュリティ関連法規（刑法，不正アクセス禁止法，プロバイダ責任制限法など），個人情報保護関連法規，知的財産権関連法規，労働関連法規，法定監査関連法規（会社法，金融商品取引法など），システム監査及び情報セキュリティ監査に関する基準・ガイドライン・施策，内部監査及び内部統制に関する基準・ガイドライン・施策 など

公認システム監査人の得意分野

BCP運用支援	エンタープライズアーキテクチャ	プロジェクト監査	技術情報システム、PDM	生産管理カリキュラム作成支援	医療情報システム
CRM(SFA,コールセンタ)	オフショア開発	プロセス改善、人材育成	業務・システムの最適化計画策定	税務会計コンサルティング	卸売業
ERP(SAP)	コンプライアンス	マネジメントシステム	業務の見える化、業務改善・改革	設計開発、製造業(情報戦略)	会計システム
EUC	サプライチェーンマネジメント	メインフレーム運用管理	業務プロセス構築	設計技術情報・生産情報システム	学校法人
ISMS	シンギュラリティ	ライブ・プロジェクト監査	業務改革	戦略策定、業務改善、業務監査	官公庁
ISO20000	セキュリティ	リスクマネジメント	業務監査	組織・PJTの品質保証、監査	原価計算
ISO27001	ソフトウエアライセンス監査	ロジスティクス	経営／情報化戦略・システム診断	大規模システム見直し支援	購買システム
ITSMS構築運用支援	ソフトウエア開発プロセス	運用のアウトソーシング	研修企画、講師、運営	通信ネットワーク	財務会計
IT統制	ソフトウェア資産管理	海外法人インフラ監査	個人情報保護	投資運用ポートフォリオ管理	自治体
IT利活用高度化	データセンター監査	開発・保守プロセス評価(監査)	財務コンサルティング	統合マネジメントシステム	商社
J-SOx IT統制監査	デジタル・フォレンジックス	開発段階での信頼性監査:品質	資金決済システム構築	特許創出、アイデア摘出	食品製造業
MS-OFFICEエキスパート	テレコムオペレーションシステム	外部調達	事業継続BCMS	特許入金支援方法	生活協同組合
PMS構築	ネットワークセキュリティ監査	株式公開コンサルティング	事務手続きの現状分析・改善	内部監査	製造業
QMS審査	ネットワーク技術	環境コンプライアンス管理	自己情報コントロール	内部統制	地方公共団体
QRトータルソリューション	パケージ導入、水道業務、銀行系	環境会計	情報システム開発・運用	認証局監査	通信業
RFIDトータルソリューション	パッケージSW導入、データ変換	監査導入、Web脆弱性検診	情報子会社マネジメント	汎用機のOS設計～構築	病院
SAP会計システム	ビジネスモデル改革	危機管理・災害対策	情報通信分野全般	品質管理、ISO9001	物流システム
Webアプリのセキュリティ監査	ビジネスリスクマネジメント	基幹業務プロセス構築	人材育成	物理セキュリティ	貿易、国際物流
インターネット募金	ヒューマンリソースバランシング	基幹系:財務会計、給与、販売等	制御システムのセキュリティ	法人税･所得税･相続税	流通業
エネルギーソリューション	プライバシーマーク	機器組込システムの監査	整合性・有効性	有効性監査:目的適合、投資効果	労働・社会保険

システム監査に関係した出来事

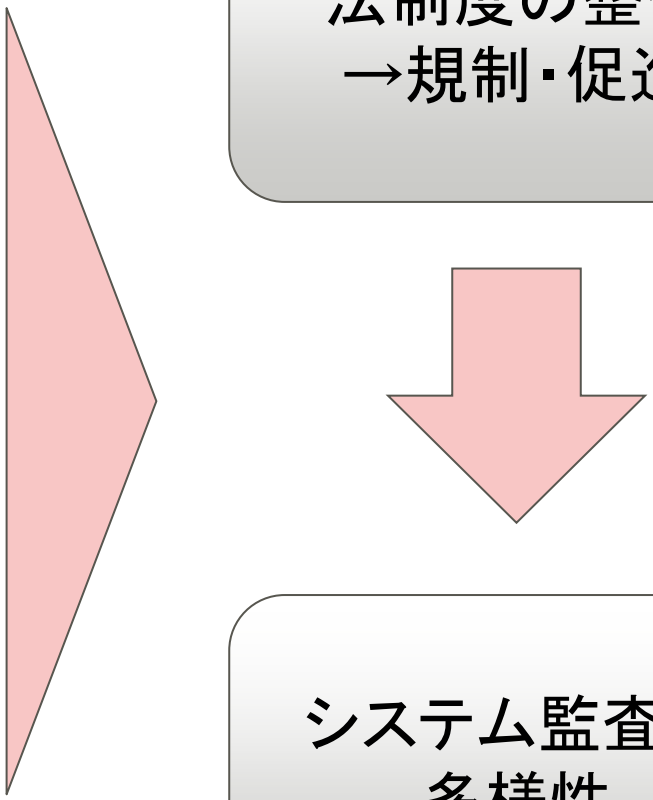
年度	制度など	新技術・事件・事故など
2005年	個人情報保護法の全面施行	みずほ証券大量誤発注事件
2006年	金融商品取引法の成立	Facebook開始　アマゾンAWS開始
2007年	共通フレーム2007	iPhone発表
2008年		スルガ銀行事件　リーマンショック
2009年		ビットコイン開始
2010年	IFRS（国際会計基準）	
2011年		東日本大震災　ソニーPE不正アクセス事件
2012年	マイナンバー法案	スルガ銀行勝訴
2013年	共通フレーム2013	JR東日本 SUICA情報提供事件
2014年		Mt. Gox事件　ベネッセ事件
2015年	マイナンバー法施行	日本年金機構事件　東芝不正会計

多様性をもたらす要因

ITの進化
→リスクの多様化

事件・事故
→再発抑止・減災

グローバル化
→外圧（？）



法制度の整備
→規制・促進

システム監査の
多様性

多様性するシステム監査へ向けて

監査（Audit）は「聴く」と言う意味を持つ。
「聴く」ためには、相手と向き合うことが大切。
（2008年7月　SAAJ近畿支部20周年記念シンポジウム　堀江正之先生の資料より引用）

- システム監査スキル
- 「聴く」ための技術スキル
- 「聴く」ための業務・業種・技術に関する知識

→　一人の監査人では限界

→「チーム医療」と同様に「チーム監査」による対応が有効ではないか

システム開発プロジェクトの監査

■失敗プロジェクトの理由

■SIベンダーの取組み

■監査のチェックポイント

■システム開発プロジェクトの成功とは

失敗プロジェクトの理由

【2014年1月16日　日経コンピュータ誌】

「多くのSIerが不採算プロジェクトにより決算で減収となった」

・有識者の分析による失敗の理由は・・・

■営業が無理をして受注した

■技術継承がうまくいかずプロマネ力が衰えた

■リスク管理に対して過信した

・SIerの言い訳は・・

■技術的に高いレベルの案件だった

■もともと赤字を見込んでいたが、想定以上に赤字になった

・日経コンピュータ誌編集者の見解は・・

■SE稼働率維持のためリスクのある案件を受注したため

（景気が好転し、企業がIT投資に積極的になれば解消する）

SIベンダーの取組み

【2015年11月12日　日経コンピュター誌　】

「（特集）大損害時代の突破術」

スルガ／IBM裁判、みずほ証券／東証裁判等の決着を受け
今後のベンダー・ユーザ企業等の動きを取材。

・SIベンダーの取組み

■案件開始前の段階でリスクを管理する

■提案段階やプロジェクト計画段階でリスクを開示する

■早い段階でプロジェクトの大方針を顧客と共有する

■リスク管理を現場任せにしない

■第三者による品質評価を実施する

■利用部門の関与度合いを確認する

■定期的に顧客の満足度を確認する

監査のチェックポイント

情報サービス産業協会「ソフトウェア開発委託取引における受注チェックシート」

大項目	中項目	小分類	項目
ビジネス意識	顧客特性及びビジネス戦略	自社のビジネス戦略	3
		開発規模	2
		得意分野商談	2
		新規顧客	4
		継続顧客	5
		個社戦略	3
		IT投資分析	4
受注条件	要件	要件提示	6
		その他の要件提示	8
		環境	2
		支給品	3
		要件確定	3
		仕様変更管理	3
	見積り	コスト見積	8
		提示価格	4
		受託する工程範囲	2
	スケジュール	開発期間	4
		外部要因	2

大項目	中項目	小分類	項目
受注条件	体制	開発体制	5
		顧客体制	5
	契約	全般	1
		多段階契約	2
		瑕疵担保責任	3
		著作権	1
		特許権等	1
		セキュリティ	2
		損害賠償	1
		再委託	1
プロジェクト準備	工程定義	作業内容	2
		成果物	3
	検収	検収	2
	会議	ステアリングコッミティ	1
		進捗会議	3
	納入	納入	2
合計	10	34	103

監査のチェックポイント

情報サービス産業協会「ソフトウェア開発委託取引における受注チェックシート」

No.	大項目	中項目	小分類	チェック項目	チェック結果	改善要
1	ビジネス	顧客特性及びビジネス戦略	自社のビジネス戦略	技術蓄積が可能であるか。		
2				要員育成の機会となるか。		
3				成果物が次のビジネスで再利用できるか。		
4			開発規模	開発規模が大規模でリスクが大きすぎないか。		
5				開発規模が小規模で非効率すぎないか。		
6			得意分野商談	得意分野に応じた生産性向上が見込めるか。		
7				提示価格は投資回収をも意識した適切な利益率で価格を提示しているか。		
8			新規顧客	政策的に新規取引を狙う相手先か。		
9				政策的な案件である場合、戦略的な価値が打ち出せるか（打ち出せているか）。		
10				顧客の経営方針や営業方針等で提案に盛り込むべきことを反映したか。		
11				要求されている案件以外でも自社の特長や差別化のアピールポイントは考えているか。		
12				過去プロジェクトの経験に基づいてリスク低減ができるか。		

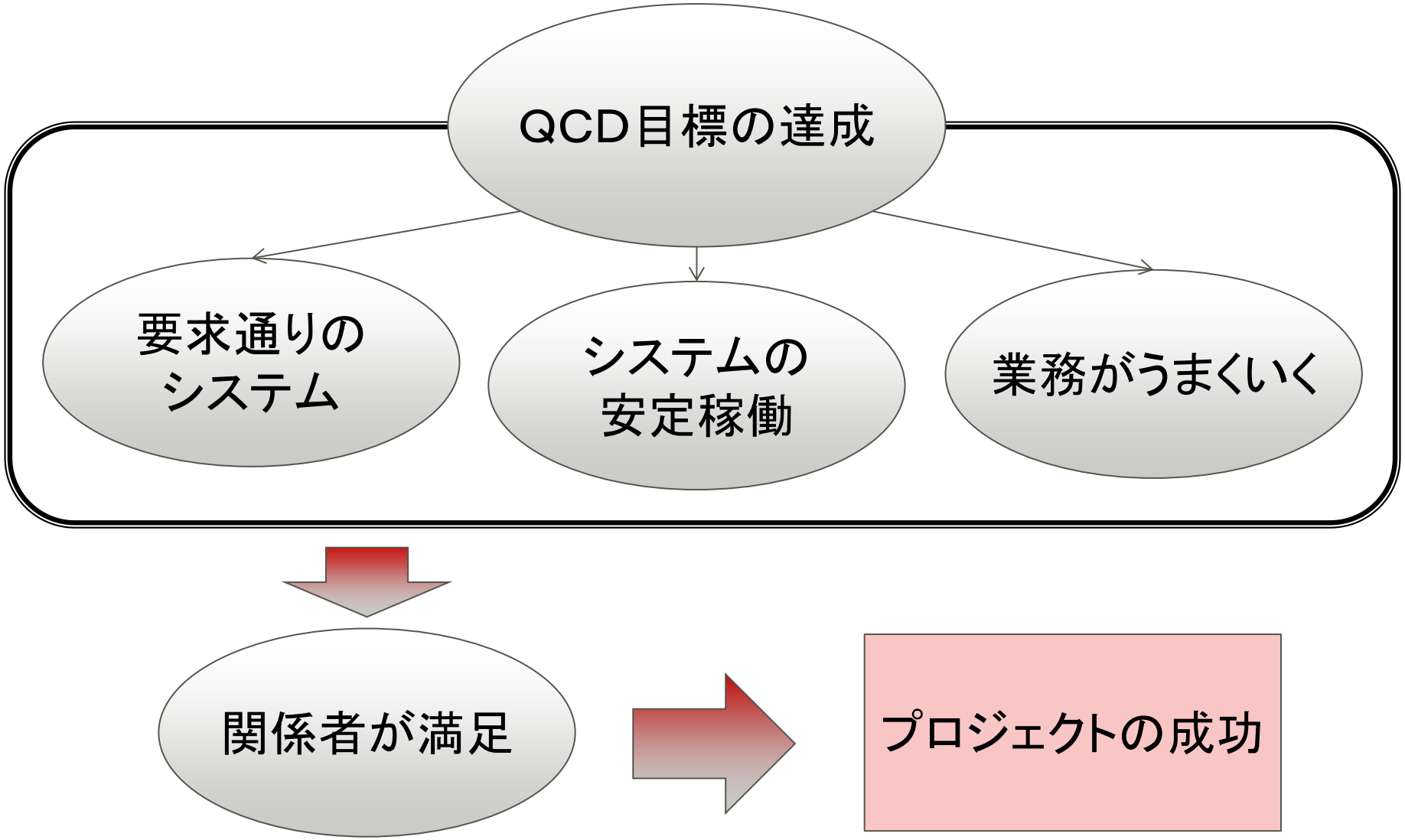
プロジェクト監査での指摘事例

■「現行システム機能を踏襲」が前提条件であったが、肝心の現行システム機能が分かる人や物が十分ではない。

■2つの商談が発生しており、双方とも提案しないといけないが2つとも受注するとSE体制が十分に取れない。

■別ベンダーが途中まで実施した作業を引き継いで作業をする条件であるが、前工程の作業品質が不明である。

システム開発プロジェクトの成功とは



ご清聴ありがとうございました