システム監査学会第２８回研究大会

＜法とシステム監査研究プロジェクト**成果報告**＞

外部委託先管理のガバナンスとマネジメント
― システム監査の視点から

"Governance & Management Process of Outsourcing Technology Services
- Review Points for IT Auditor"

Friday.6.6.2014

成田　和弘
システム監査技術者，ＣＩＡ，ＣＩＳＡ

Kazuhiro Narita

はじめに

- 研究プロジェクトの概要
  - 主査　稲垣 隆一、副主査　黒澤 兵夫
  - 概要

    システム監査は、情報システムの企画、開発、運用、保守に関する現実的な課題の予防、解決に、いかに役立つのか？クラウドコンピューティング、ソーシャルネットワーク、ビッグデータの取扱い、マイナンバー制度など現下の課題、判決例に表れた紛争事例、現下のシステム上の課題を素材に検討し、その成果を生み出すシステム監査の技法の開発、管理基準の改訂の提案などに結びつける。

「法とシステム監査研究プロジェクト」メンバー

（原則五十音順）

氏名	所属等	備考
荒木 哲郎	弁護士・システム監査技術者	
稲垣 隆一	稲垣隆一法律事務所・弁護士	主査
植野 俊雄	ISU	
黒澤 兵夫	TAKE国際技術士研究所	副主査
芳仲 宏	東京地方裁判所	
成田 和弘	システム監査技術者，CIA，CISA	発表

発表テーマ

■ 外部委託先管理のガバナンスとマネジメント ー システム監査の視点から

"*Governance & Management Process of Outsourcing Technology Services - Review Points for IT Auditor*"

- 開発プロジェクトでは、専門的な作業を外部委託することが一般的であり、開発作業を一括してアウトソーシングすることも少なくない。開発プロジェクトの成功率は3割程度ともいわれ、ベンダとユーザーはこのリスクをコントロールして協働する必要がある。
- ベンダのプロジェクトマネジメント義務違反とユーザーの協力義務違反が争われた裁判、システム更改時に埋め込まれたバグによる賠償責任が問われた裁判等を教訓に、このようなリスクの発現を防ぐために、システム監査でどのような観点で検証すべきかを、COBITフレームワーク等の最新の国際標準を参考に、システム管理基準の記述内容との比較・検証を交えて考察する。

Agenda

1. ガバナンスとリスクマネジメント
   ～ベンダのプロジェクトマネジメント義務違反と
   ユーザーの協力義務違反が争われている事案

2. コンプライアンスと品質管理
   ～バグ顕在化が深刻な業務影響を及ぼした事案

3. システム管理基準・システム監査基準の方向性

4. まとめ

Kazuhiro Narita

1. ガバナンスとリスクマネジメント

～ ベンダのプロジェクトマネジメント義務違反と
ユーザーの協力義務違反が争われている事案

- スルガ銀行・日本IBM裁判の概要
- 国保事件東京地裁判決
- スルガ銀行・日本IBM裁判東京高裁判決
- システム投資とリスク
- システム監査の視点～COBIT5を参考に
- システム監査の視点～ユーザー企業のプロセス
- システム監査の視点～ベンダのプロセス

Kazuhiro Narita

スルガ銀行・日本IBM裁判の概要

- プロジェクトがシステムの開発に至らずに頓挫し、スルガ銀行が日本IBMに約116億円の賠償を請求
- システム開発契約におけるITベンダの「プロジェクトマネジメント義務違反」、ユーザー企業の「協力義務違反」が主な争点

➢ 東京地裁平成24年3月29日判決（金融法務事情1952 P111）

✓ 日本IBMの賠償の範囲を、システムの企画・提案の段階から開発中止に至るまでの費用全額とし、74億円余の支払い命令

➢ 東京高裁平成25年9月26日判決（金融・商事判例1428 P16）

✓ 賠償の範囲を、システムの要件定義を経て最終合意書を交わした以降の費用に限定し、41億円余の支払い命令

国保事件東京地裁判決

- 東京地裁平成16年3月10日判決 （判例タイムズ 1211 P129）
  - ➢ITベンダには、システム開発の専門業者として、自らが有する高度の専門的知識と経験に基づき、合意のとおりのシステムを完成させるべき債務があり、ユーザーにはこれに協力する義務がある
  - ✓ITベンダのプロジェクトマネジメント義務
    - ユーザーとの間で合意された開発手順や開発手法、作業工程等に従って開発作業を進める
    - 常に進捗状況を管理し、開発作業を阻害する要因の発見に努め、これに適切に対処する
    - 専門知識を有しないユーザーによって開発作業を阻害する行為がされることがないようにユーザーに働きかけ、導く
  - ✓ユーザーの協力義務
    - 要件定義や基本設計の工程では、ユーザー企業の協力義務が強く求められる
      ～ ユーザー企業の準備不足や体制不備は、協力義務違反

スルガ銀行・日本IBM裁判東京高裁判決

- 東京高裁平成25年9月26日判決（金融・商事判例1428 P16）
  - ➢ベンダはユーザーの業務内容等に必ずしも精通していないので情報と能力の非対称性は双方に存する。ユーザーも開発対象業務の分析とベンダの説明を踏まえて自らシステム開発のリスク分析をするべき。
  - ✓ITベンダのプロジェクトマネジメント義務
    - 企画・提案の段階では、開発不可能とまでは認識できなかった － 義務違反はない
    - 計画・要件定義の段階では、当初予定していた開発費用、開発スコープおよび開発期間に収めて開発するのが不可能なことが次第に明らかになり、最終合意の段階では認識していた
    - ➢最終合意締結の段階では、開発遂行上の危機を回避するための適時適切な説明と提言を、回避し得ない場合には中止をも提言する義務があった

システム投資とリスク

- 開発プロジェクトのリスクは高く、成功率は3割ともいわれる （出典：日経コンピュータ2008年12月1日号）
  - ✓ 品質、コスト、期間を守るためには専門的なノウハウと体制が必要
- 組織にとって大きなリスクを取り扱うので、十分なガバナンスと内部統制が求められる
- 専門性とリスク管理が要求される金融商品は・・・
  - ✓投資家はプロとアマに区分され、業者には種々の行為規制が課される
  - ✓アマの投資家へは「適合性の原則」で顧客の状況や契約締結目的に照らし不適当な投資勧誘は不可
  - ✓資本金5億以上の企業や上場企業は原則プロ

参考：「金融商品取引法入門」（金融財政事情研究会）

Kazuhiro Narita

システム監査の視点～COBIT5を参考に

- ガバナンスとリスクマネジメントの関係
  - ✓ガバナンスプロセス「リスク最適化の保証（EDM03）」
    - 取締役会が担う「リスク最適化の保証」のプロセスは、CIOが担う「リスク管理」からの「第三者によるリスクアセスメント結果」や「リスク分析の報告」を元にリスクの最適化に対処する
  - ✓マネジメントプロセス「リスク管理（APO12)」
    - 経営層がリスクとリターンのバランスをとれるよう、「第三者によるリスクアセスメント結果」や「リスク分析」を報告

参考：COBIT5 Enabling Process（ISACA） より

- ➢ リスク最適化のガバナンスプロセスが機能するには、リスクマネジメントのプロセスからの十分な報告が必要

Kazuhiro Narita

システム監査の視点～ユーザー企業のプロセス

- 投資額(リスク)に応じたガバナンスと管理
  - ○両社役員が参画するステアリングコミッティーを設置
  - ×開発リスクはベンダに負担(請負)してもらっているつもりだった・・・
    - 自らの利害関係者に「相手を信じた」だけでは説明できない
    - M&Aなら、監査法人などによるデューデリジェンスを行う
  - ×ベンダの提案のフィジビリティー等、リスクの洗い出しと管理は不十分
    - 必要に応じ外部の(ベンダと対等な)知見を活用するなどにより、プロジェクトのリスクを評価する体制
    - パッケージに関する必要な権利の担保 … etc
- ➢ 外部委託先のプロセスを含めたリスク管理とガバナンス体制の確認

Kazuhiro Narita

システム監査の視点～ベンダのプロセス

- 提案が顧客に適合しているかのチェック体制
  - ×開発リスクの十分なアセスメントおよび対策と説明
    - ソリューションとアプローチ手法の整合性
    - 提案実現に必要な権利の事前の取得
    - フィジビリティのある実現可能な提案
  - ➲不確実なプロジェクトに対して、結果的に虚偽の告知や断定的な判断となる恐れのある勧誘はNG
- ➢ プロジェクトや要件定義のモニタリング報告等、リスク管理と委託先への報告を適切に実施できるガバナンス体制の確認

（参考） Fiduciary Duty；広範な裁量権を有し財産の処分・管理を行う信託受託者が受益者の利益を専一に考え、裁量権の濫用を防止する法理
（出典：企業年金連合会用語集 http://www.pfa.or.jp/yogoshu/fu/fu02.html ）

2. コンプライアンスと品質管理

～バグの顕在化が深刻な業務影響を及ぼした事案

- みずほ証券-東証誤発注裁判の概要
- みずほ証券-東証誤発注裁判東京高裁判決
- システム監査の視点～COBIT5を参考に
- システム監査の視点～提供システムの品質保証

みずほ証券-東証誤発注裁判の概要

- みずほ証券が東京証券取引所の旧・株式売買システムに発注を取り消せないバグがあったことで生じた損失など約415億円の賠償を求めた裁判

➢ 東京地裁平成21年9月25日（判決判例タイムス1322 P149）

- ✓ バグについて「回帰テストの確認を怠ったことだけでは重大な過失とはいえない（軽過失は契約で免責）」として、東証の責任を否定した
- ✓ 誤発注の判明後も売買停止権限を行使しなかった点について「人的な対応を含めた全体としての市場システムの提供義務」について、東証に故意に近い過失（重過失）を認め、東証とみずほ証券の過失割合を7対3として、東証に107億円余の支払いを命じた。

➢ 東京高裁平成25年7月24日（金融・商事判例1422 P20）

- ✓ システム開発業者を履行補助者と認定したが、システムのバグについては「不具合を容易に発見できたとは認められないため重過失はない」として、東証の責任を否定した。
- ✓ 売買停止権限を行使しなかった点についての過失割合、支払金額は第一審を踏襲

みずほ証券-東証誤発注裁判東京高裁判決

- 取引参加者契約
  - ✓故意または重過失のときのみ賠償責任を負う契約
  - ✓約定株式数が発行済み株式総数の3倍を超え、異常を認識したのに売買停止としなかったのは著しい注意義務違反（重過失）
- システム提供義務の履行
  - ✓不十分であったが重過失にはあたらないとされた
    ①稼働後5年類似の不具合無し
    ②複数の条件が重なったときだけ発生
    ③バグの回避、発見、修正が容易といえない
  - ➢ 外部委託先は履行補助者と認定されたので、もし重過失があれば責任が問われる

（金融・商事判例1422 P20）

Kazuhiro Narita

システムの品質とコンプライアンス～COBIT5を参考に

- コンプライアンスと品質管理の関係
  - ✓モニタリングプロセス「外部要件への準拠性のモニタリグ、評価およびアセスメント（MEA03）」
    - 各事業部門が「外部要件への対応の最適化」のため、法規制および契約要件に関し、「コンプライアンス要件の周知」をすべての関係者に対して行う
  - ✓マネジメントプロセス「品質管理（APO11）」
    - CIOが「品質管理システムの確立」の有効性をレビューし、品質保証を継続的に改善する

  参考：COBIT5 Enabling Process（ISACA） より

- ➢ 法規制や契約などを遵守するために求められる品質水準を満たす品質保証となっていることが必要

Kazuhiro Narita

システム監査の視点～提供システムの品質保証

- 取引参加契約上の義務を果たせるシステム
  - ×「現行通り」という要件定義
    - 開発委託先は自らの業務の履行補助者
    - 取引参加契約上の義務もシステム要件
    - 要件は既存機能もすべて文書化してテストする
  - ×システム障害時の業務継続
    - システムが止まったときの対応漏れが重過失となった
    - 障害時にコンプライアンス要件を満たす業務継続対応も重要

➢ 外部委託先作業を含めた品質管理プロセスが、システムの重要度に相応しいものであることが必要

3. システム管理基準・システム監査基準

～現状と改訂の方向性

- ガバナンスとリスク管理への対応状況
- コンプライアンスとシステム品質への対応状況
- システム管理基準の改訂の方向性
- 内部監査の重要性の高まりとシステム監査
- システム監査基準の改訂の方向性

3. システム管理基準・システム監査基準

ガバナンスとリスク管理への対応状況

- **システム管理基準の記述** （出典:「システム管理基準」経済産業省）
  - ✓ **ガバナンス**
    - Ⅰ.2.1(5) 委員会は、意思決定を支援するための情報を組織体の長に提供すること。
    - Ⅱ.1.(1) 開発計画は、組織体の長が承認すること。
  - ✓ **リスク管理**
    - Ⅱ.2.(5) 情報システムの導入に伴って発生する可能性のあるリスク分析を実施すること。
  - ✓ **パッケージ導入の開発計画**
    - Ⅱ.1.(8) 開発計画の策定に当たっては、システム特性及び開発の規模を考慮して形態および開発方法を決定すること。
    - Ⅱ.2.(8) パッケージソフトウエアの使用に当たっては、ユーザーニーズとの適合性を検討すること。
- ■ **ガバナンスのプロセスは不十分で執行と監督の関係が不明確**
- ■ **リスク管理は部分的でマネジメントシステムとして不十分**
- □ **パッケージ導入等の開発管理プロセスは詳細に網羅されている**
- ➢ **種々のリスクの統合管理やガバナンスはイメージしにくい**

Kazuhiro Narita

コンプライアンスとシステムの品質への対応状況

- **システム管理基準の記述** （出典:「システム管理基準」経済産業省）
  - ✓ **コンプライアンス**
    - Ⅰ.3.(2) 全体最適化計画は、コンプライアンスを考慮すること。
    - Ⅰ.6.(1) 法令及び規範の管理体制を確立するとともに、管理責任者を定めること。
    - Ⅰ.6.(2) 遵守すべき法令および規範を識別し、関係者に教育及び周知徹底すること。
    - Ⅰ.6.(5) 法令、規範および情報倫理規定の遵守状況を評価し、改善のために必要な方策を講ずること。
  - ✓ **品質管理**
    - Ⅵ.3.1(1) 品質目標に基づいて品質管理の計画を定め、ユーザー、企画、開発、運用および保守の責任者が承認すること。

□「全体最適化計画」でもコンプライアンスを考慮

□ コンプライアンス管理は、マネジメントシステムを想定している。

□ 品質管理も詳細に記述されている

➢ **プロセスの担い手や成果物等のプロセス間の関連は捉えにくく、“コンプライアンスを踏まえた品質管理“のような発想はしにくい**

Kazuhiro Narita

システム管理基準の改訂の方向性

- ガバナンスプロセスの見直し
  - ✓ガバナンスとは本来、執行と監督を分離し、短期収益のために会社財産を毀損しないよう牽制をかけるもの
  - ✓「全体最適化計画」や「委員会」審議、「組織の長」の承認では体制として不十分
- プロセスの担い手や成果物等の明確化
  - ✓個別管理プロセスの網羅性は有効
  - ✓原因プロセスを追跡・特定するために、プロセスの担い手や成果物等のプロセス間の関連を明確にすることが必要

内部監査の重要性の高まりとシステム監査

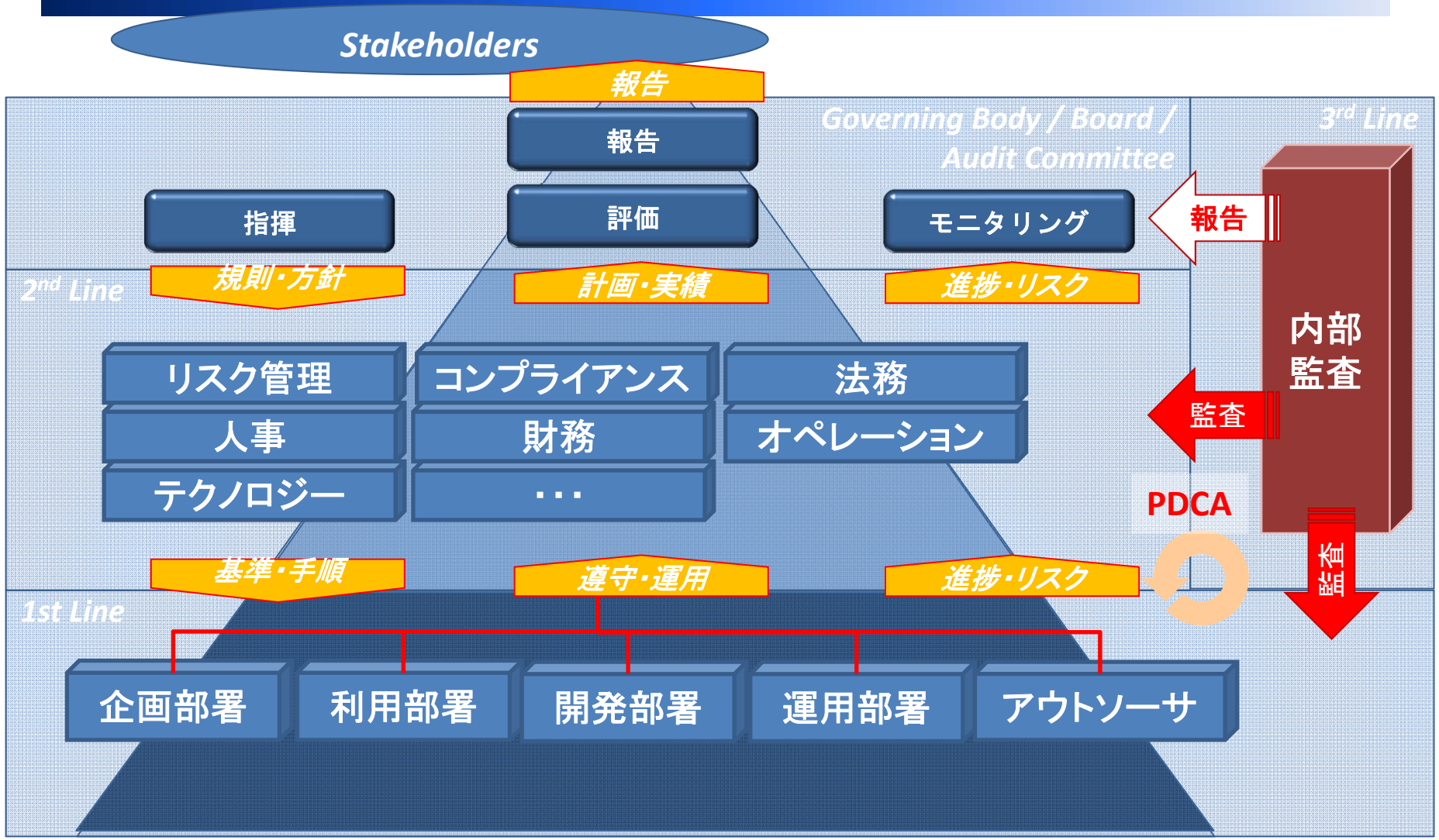
- 巨額な開発プロジェクトや重要な社会インフラの品質の検証など、高いリスクには高い目線が求められる
- 3つのディフェンスライン

  参考:「内部統制の統合的フレームワーク(フレームワーク編)」(トレッドウエイ委員会支援組織委員会),「銀行の内部監査機能」(バーゼル銀行監督委員会)

  - ✓ 第1のディフェンスライン(現業部門の経営者およびその他の構成員は)は取引ベースで日々のリスクを管理
  - ✓ 第2のディフェンスライン(リスク管理、コンプライアンス、法務、人事、財務、オペレーション、テクノロジー)は内部統制の要件を明確化し、その基準の遵守状況を評価
  - ✓ 内部監査は第3のディフェンスラインとして、リスクベースで定期的にこれらの機能が有効であることを評価・報告し、経営者に是正措置または強化策を検討および実行するよう勧告する → 組織横断的な評価
- ➲「システム監査基準」も準拠性だけでなく、内部統制プロセスの有効性を評価できるようレベルアップが望まれる

Kazuhiro Narita

《参考》 3つのディフェンスラインのイメージ



Kazuhiro Narita

4. まとめ

- ☑ 今日の複雑かつ高度なシステムの掌握は、ITベンダにとっても企業ユーザーにとっても容易ではない
- ☑ 一方、企業システムの重要度はますます高まり、高品質の情報サービスが必要
- ☑ ITベンダには、品質・コスト・期間の期待を達成する、より高い専門性の発揮が期待される
- ☑ ユーザー企業には、より高い専門性を有する外部委託先を有効に評価・活用し、IT投資の成功を自ら導けるような、ガバナンスとマネジメントのプロセスが求められる
- ☑ システム監査も第3のディフェンスラインとして、システム関連のリスクのガバナンスとマネジメントのプロセスを内部統制の有効性として評価していく必要がある
- ➲ システム管理基準、システム監査基準は、このような環境変化に対応し、進化していくことが必要

Kazuhiro Narita

ご清聴ありがとうございました

この資料の内容には発表者個人の見解が含まれます。
また、発表者の所属会社とは関係ありません。

Kazuhiro Narita