法とシステム監査研究プロジェクト 成果報告

システム監査学会第２７回研究大会

開催日：２０１３年６月７日（金）

発表：荒木哲郎（弁護士・システム監査技術者）

序　研究プロジェクトの概要

1　概要

■　主査　弁護士　稲垣隆一

■　概要

国、自治体、企業の遵法経営のために情報システムの企画、開発、運用、保守が抱える課題と、課題解決のためのシステム監査の経営における位置づけ、監査の尺度、監査技法を研究して、コンプライアンス経営のためにシステム監査が果たし得る実務的な役割を明らかにする。

2 研究テーマ

ソリューションプロジェクトにおけるユーザの協力義務と課題

3　今回のテーマを選択した趣旨

- **スルガ銀行　VS　日本ＩＢＭ　裁判**
  （東京地裁平成２４年３月２９日判決。
  現在、控訴審審理中）

  「被告には、本件システム開発のベンダとして適切にシステム開発を管理することなどを内容とするプロジェクト・マネジメント義務の違反があるものというべきである。」

- **プロジェクト・マネジメント義務という概念は、この裁判例以前にも使用されており（後述、「国保事件」参照）、この裁判例でいきなり使われたわけではない。**

・今後、プロジェクトマネジメント義務という概念が今まで以上に多用される可能性。

・対応概念としてのユーザの協力義務にも着目し、両者の関係を適切に把握しておく必要あり。

ユーザの協力義務

対応

ベンダの
プロジェクトマネジメント義務

４　目次

第１　総論

１　法（裁判）とシステム監査の関係

・裁判とは、トラブルを事後的に解決する手段

・トラブルとの関係から、時系列を見ると

システム開発　→　運用・保守

監査

トラブル発生　→　話し合い　→　裁判

・トラブルの予防や、最終的に起きるかも知れない裁判のために、監査でやっておくべきことは何か。

2　裁判で要求される事実と監査

・裁判における紛争解決の構造

事実 → 法 → 法的効果 → 紛争解決

〇裁判における事実

・・裁判官が感得した事実。真実発見の要請はあるが、必ずしも客観的真実とは限らない。

→どのような事実を主張・立証するかが重要。

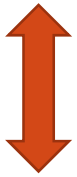
→監査においてもそれを念頭にすれば、トラブルの防止等に役立つのでは？

第２　ユーザの協力義務の概念

１「プロジェクトマネジメント義務」（ICTベンダ）と「協力義務」（ユーザ企業）

（ユーザ側）

**　ベンダから協力を求められた場合に適時に適切な意思決定をする協力義務**



（ＩＣＴベンダ側）

**　開発を成功させるために、問題点を発見し、ユーザに対して問題点について協力を求める義務**

協力義務とPM義務

ユーザ企業の協力義務	ＩＣＴベンダのＰＭ義務
要件定義や基本設計の工程では、ユーザ企業の協力義務が強く求められる。即ち、ユーザ企業の準備不足や体制不備は、協力義務違反	①ユーザ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 ②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。 ③専門知識を有しないユーザ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に働きかけ、導く（例：要件定義の確定、パッケージ選定における性能・最適性・検証）

2　判例での現われ

- **東京地方裁判所平成16年3月10日判決（国保事件判決）**

（1）ＩＣＴベンダのPM義務

「システム開発は注文者と打ち合わせを重ねて、その意向を踏まえながら行うものであるから、被告（ベンダ）は、注文者である原告（ユーザ）のシステム開発へのかかわりについても、適切に管理し、システム開発について専門的知識を有しない原告（ユーザ）によって開発作業を阻害する行為がされることのないよう原告（ユーザ）に働きかける義務（以下、これらの義務を「プロジェクトマネージメント義務」という。）を負っていたというべきである。」

（２）ユーザの協力義務

「したがって、原告国保（ユーザ）は、本件電算システムの開発過程において、資料等の提供その他本件電算システム開発のために必要な協力を求められた場合、これに応じて必要な協力を行うべき契約上の義務（以下「協力義務」という。）を負っていたというべきである。

・例示

①ユーザ社内の意見調整

②開発すべき機能の決定

③外部仕様の決定

④成果物の検収

→　システム開発の要件定義をユーザ責任の下に明示し、ベンダから納品された成果物が要件定義通りであるかを検収すること

3　ユーザの協力義務の種類

（1）契約上の明示義務

契約上明示されている役割分担に基づいて発生する義務

→違反すると債務不履行責任

- **現在、主流の多段階契約においては、段階ごとに、ベンダとユーザの役割分担として定められるものと思われる。**

（２）一般的協力義務

　契約上、明示されていないが、システム開発契約がベンダとユーザの共同作業であるという性質から、ユーザに認められる義務

・不法行為におけるユーザの協力義務

→　スルガ銀行　VS　日本ＩＢＭ事件では、契約上の債務不履行責任が否定されているので、上記の一般的協力義務が問題にされた事例と考えられる

４　企業のＩＣＴ環境との関係

・近時、クラウド化との関係で、システムは「所有」から「使用」へ

ＩＣＴの「持たない化」が進んでいる。

→ユーザ側で持たない部分は、ベンダの関与具合が大きくなる。

→「人（情報システム部門）」と「インフラ」の有無により、ユーザとベンダとの関係、及び責任分担も異なると考えられる。

・パターン

① 情報システム部門「あり」インフラ「なし」の場合

直接、クラウドサービス等を利用する場合

→ ユーザの情報システム部門等が自らサービスの選定、評価を行う。ユーザが加えた変更は自己責任になることが多い。

② 情報システム部門「なし」インフラ「あり」の場合

自社内にサーバ等を所有するが、運用保守を「丸投げ」しているような場合

→ 情報の非対称性により、ベンダ優位になりやすく、ユーザ側で、要件定義や評価を正しく行うことができないので、仕様が曖昧になったり、責任範囲が不明確になりやすい。

③ 情報システム部門「なし」インフラ「なし」の場合

経営者や利用部門担当者がクラウドサービス等を利用する場合等

→ サービス形態にもよるがベンダの責任は限定的である場合が多い。 導入後のトラブルに対してはユーザの自己責任

第３　システム監査におけるポイント

１　概要

協力義務を果たすには、責任分野を明確にして、その責任を全うすることが基本。

・責任の具体例

（１）要件定義

ａ期間厳守での定義の実施（ユーザ側）

ｂ明確な責任分担の提示（ベンダ側）

（２）専門性

ａ自組織が求めるシステム像の定義、利用者の要求事項の把握（ユーザ側）

ｂプロマネ力、パッケージ仕様の知識、ユーザ要求に対する現実解の提案力（ベンダ側）

（例）要件定義における各々の責任

ユーザの責任	ベンダの責任
①利用者視点でのシステム要件（非機能要件含む）の定義 ②システム要件の修正（期間・予算から実現可能性を見て機能を限定） ③利用者意見の集約（過剰な要求、背反する要求の調整含む） ④仕様変更・追加要求の最終期限の厳守	①システム要件定義作業の責任分担の明確化 ②パッケージ利用時の制約（実現できない機能の明確化と代替策提案 ③機能仕様の明確化と利用者含めたレビュー ④仕様変更・追加要求の手続と期限の明確化

（例）要件定義におけるチェック項目

ユーザ側の協力義務チェック項目	ベンダ側のＰＭ義務チェック項目
①利用者視点でのシステム要件の定義 ・機能要件が定義されること ・操作性要件が定義されること ・非機能要件が定義されること ・「現状と同等」など曖昧な表現を用いないこと ②システム要件の修正 ・期間・予算から実現可能性が把握されること ・実現可能性ある範囲の機能に限定されること ・ ・ ・	①システム要件定義作業の責任分担の明確化 ・システム要件定義の記述レベルが明確化され、ユーザと合意されること ・システム要件定義の日程と責任分担がユーザと合意されること ②パッケージ利用時の制約 ・実現できない機能の明確化と代替策提案がされること ・ ・ ・ ・

２　開発の時系列との関係

・ＩＰＡ－ＳＥＣ「超上流から攻めるＩＴ化の原理原則１７ヶ条」

・・ベンダ、ユーザ双方が、うまくプロジェクトを進めるポイント及び、基本的な考え方に沿った「行動規範」を示している。

→ユーザの協力義務に関係する項目あり。

・ユーザの協力義務に関するものと考えられる例

【以下、ＩＰＡ－ＳＥＣ「超上流から攻めるＩＴ化の原理原則１７ヶ条」から抜粋】

（１）原理原則

［９］　要件定義は発注者の責任である

［１２］表現されない要件はシステムとして実現されない

［１７］要件定義は、説明責任を伴う

（２）行動規範

・発注者は、受注者との役割分担を明確にし、プロジェクトに積極的に参画する。（原理原則１）

・発注者は、依頼する範囲、内容を漏れなく洗い出し、提示する。（原理原則６）

・発注者は、「我々が要件を決め、責任を持つ」という意識を社内に浸透させる。（原理原則９）

・発注者は、業務部門とＩＴ部門が、二人三脚で要件定義を進める。（原理原則９）

・超上流では、ユーザの実施すべき点が多い。

システム監査人としては、プロジェクトの超上流で監査する必要性が高いと思われる。

（初期の段階で、対策が講じられれば、プロジェクトが円滑に推進される確率が高くなる。）

３　フレームワーク等の利用について

（1）ソフトウェアライフサイクルプロセス

【ＪＩＳ　Ｘ　０１６０：２０１２（ＩＳＯ/ＩＥＣ１２２０７：２００８）】

→　ソフトウェア製品のライフサイクルにおける取得者、供給者及び他の利害関係者の間で円滑にコミュニケーションを行う場合に必要なプロセスのフレームワーク

（2）構造

ア　合意プロセス・・契約の締結や変更管理

イ　組織のプロジェクトイネーブリングプロセス
・・中長期的なシステム化計画やシステム人材管理

ウ　プロジェクトプロセス・・プロジェクト管理

エ　テクニカルプロセス・・要件定義、製造、テスト、導入、廃棄等

オ　ソフトウェア固有プロセス

→これらのプロセスの「目的」が達成され、「成果」を得るために「ユーザ（取得者）の協力が必要な事項」を検討していく。

（３）具体例：６．４　テクニカルプロセス
６．４．１　利害関係者要求事項定義プロセス

①サービスに要求される特性や利用場面を指定する。

②システム化の制約条件を定義する。

③要求事項が取得者のどの利害関係者のものか明らかにする。

④システム要求事項定義の背景を明らかにする。

⑤サービスの適合妥当性を確認する方法を定義する。

⑥サービス・製品供給の交渉合意の体制を整える。

第４　まとめ

１　ユーザの協力義務の概要

ユーザの協力義務は、責任の分担として、ＩＣＴベンダのプロジェクトマネジメント義務に対応する義務

↓

種類・環境との関係等を理解・整理し、ソリューションプロジェクトにおける開発・監査に役立てる。

↓

トラブルの防止、または、発生してしまった後の対応（訴訟含む）へつながる。

２　システム監査におけるポイント

（１）ユーザ及びベンダの責任及び協力義務を明らかにし、チェックしていく。

（フレームワーク等を利用して、チェック漏れをなくす。）

（２）超上流（及び上流）がプロジェクトを成功させるか否かを決める重要なフェーズ

↓

超上流で監査を行い対策を講じることが望ましい。

第５　今後の研究の方向性

- **システム監査基準、及びシステム管理基準の記述内容をユーザの協力義務（及びＩＣＴベンダのプロジェクトマネジメント義務）の観点から確認・検証する。**

検証の結果により

解説、（不足部分等あれば）提言等

以　上