

# Protiviti Japan Report

---

## システム監査

## 1 情報システムの意義が問われる時代に

近年、インターネットの普及と共に企業が直面する経営環境は大きく変貌を遂げています。1970年代から80年代にかけて、事務処理の合理化をメインテーマとして導入・活用されてきた情報システム( IT )は、90年代以降には、経営判断を掌る意思決定情報を取り扱う企業活動の生命線、つまり企業の競争優位の根幹としてのインフラの役割を担ってきています。特に95年にインターネットが世に利用されるようになって以降は、それまで競争優位であったノウハウや経験といったものが、ネットに参加するものに広く平等にかつ容易に、さらには瞬時に共有できる環境が構築されたため、情報システムというインフラさえあれば競争優位を保てた時代から、情報システムを如何に有意義に活用するか、さらには情報システムそのものが競争優位の源泉となりうる時代になっています。

そのような中、現在多くの企業でERPの導入や、情報システムの抜本的な見直しなど様々な情報システム開発プロジェクトを推進中ですが、上述のように情報システムの目的が単純かつ一様ではなくなり、導入に期待する効果が高まれば高まるほど、成功を遂げる事は自ずと難しくなります。

情報システムへの投資を成功に収めるための管理( Plan Do Seeのマネージメントプロセス)をこれまで以上に積極的にかつ機動的に実施しなければ、21世紀を生き残る競争優位源泉としての“ 情報システムの活用 ”が、有効に機能しないことは言うまでもありません。

## 2 情報システムの多様化と複雑化

従来からの情報システム( 汎用機と言われた )の時代には、目的が明確であり、システムの構成もシンプルなものでした。例えば、SDLC(ソフトウェア開発ライフサイクル)といった標準的な開発手法が存在し、システムのエンドユーザ( 利用者 )のシステムへの期待を要件として定義し、その要求に対してシステムの仕様を確定し、基本設計、詳細設計、開発、テスト、導入、運用保守という一連の流れの中で開発や運用を進めることが可能でした。

また、構成自体も1つのコンピュータメーカーに委託をすれば、全てが出来上がってしまうように、非常にシンプルなものでした。ところが、90年以降の情報システムの利用目的の多様化と、インターネット時代を支える情報技術の高度化が、情報システムをより複雑化し、情報システムを管理することについて、これと言った標準的かつ安易な手法が通用しなくなってきています。最近になって情報システムに関わるトラブルが多発しています。情報システムに携わる関係者が増え、情報システムの目的も多極化する中、情報システム全体を適切に管理することの難しさが露呈しているのです。情報システムが複雑化し、利害関係者が増えたのなら、情報システムの管理もそれに応じた体制で臨まなければ、情報システムの目標を達成することは難しくなります。

## システム監査

### 3 情報システム監査が重要な成功要因に

情報システムの意義が高度化し、システムが複雑化する中で、それ相応の体制で臨むことが大事であることを述べてきましたが、そのような体制の中で“情報システム監査”の役割がもっとも重要な意味を持ち始めています。

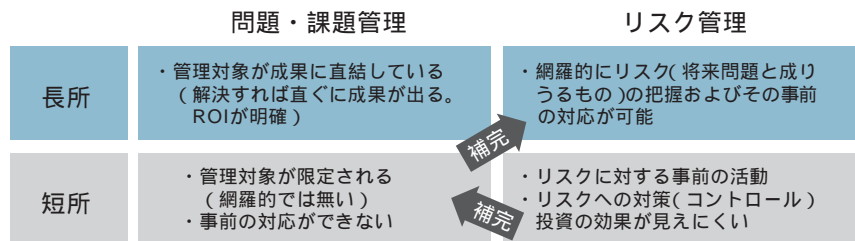
情報システムの開発は往々にして、エンドユーザ(利用者)、システム企画部門、システム開発部門、システム開発業者、メーカー、といった利害関係者のみで進められます。当然ながら利害関係者間においては、懸案事項の調整や各種意思決定を行う上で、お互いの利益が相反することから、客観性・論理性のある判断を下すことが難しくなります。昔のように利害関係者が少ないシステム開発であれば、それほど苦労しなかったものが、最近の複雑化したシステムの開発においては、多数の関係者が参加する中、客観性を持った判断を行うことがより困難となっています。

情報システム監査は、まさにそうした情報システム開発関係者の中であって、独立し、客観性を持った立場で論理的にモニタリングを実行する役割を求められています。

### 4 情報システム監査の役割

情報システム監査と言えば、旧通産省のシステム監査基準を基にした、システムの安全性・効率性・信頼性を監査することと一般的には考えられていますが、上述した観点からすれば、もう少し踏み込んで、情報システムの開発や運用の成功に対して積極的な関与が求められる時代となっています。

図1 問題・課題管理とリスク管理の相互補完関係



旧通産省のシステム監査基準は、これまで情報システム業界が経験してきた問題や課題などを基に、特に注意を払うべき箇所が、集大成として基準にまとめられているものであり、これ自体は非常に参考とすべき観点が挙げられています。この基準を基にしたシステム監査は、いわゆるベンチマーク(基準)と現状とのGAP評価を行い、改善の方向性を提示する監査となります。

また、ベンチマーク監査に留まらず、情報システムの複雑性や目的の多様化に応じた、将来問題が発生する可能性のある事項まで含めて、積極的に評価を行うことも情報システム監査の役割として重要になってきています。別の観点でご説明しますと、従来からある問題・課題管理がベンチマークとのGAP監査と例えれば、将来の不確実性を監査することはリスク管理の一環での監査と例えられます。つまりリスクアプローチの監査を実施することが求められているのです。

情報システム監査を実施する意義は、情報システムが有効に機能し、十分に活用されていることを保障するために、情報システム管理プロセスの重要な役割として、モニタリング機能を担うことにあるでしょう。

## 5 情報システム監査の種類

先に、システム監査基準を基にしたシステム監査とリスク管理の一環としてのシステム監査に触れましたが、システム監査を大別すると以下の3種類にカテゴライズできます。

### 1:旧通産省「システム監査基準」に則したシステム監査

情報システムの開発・運用における信頼性・安全性・効率性の監査

### 2:リスクアプローチによる重要なビジネスプロセスに関する情報システムの内部統制評価

情報システムの内部統制の有効性を評価するシステム監査

システムからの視点ではなく、業務からの視点による情報システムの内部統制の有効性監査

### 3:情報システムに関わるテーマ別監査

情報セキュリティ監査、システム統合監査、システム外部委託先監査、変更管理監査、等のテーマ別システム監査

情報システムに関して、あるテーマを設定し、情報システムの細部(設定・プログラムロジック等)にまで踏み込んだ監査

上記3種類のシステム監査は択一するものではなく、全てが必要な監査であり、3つの監査を上手く組み合わせることで実施することが重要となります。

各システム監査の内容を比較したものが次表です。

表1 システム監査比較表

	目 的	対象範囲	実施方法	実施頻度
① ベンチマーク監査	情報システムの安全性、信頼性、効率性の監査を行うこと(準拠性の意味合いが強い。)	情報システム全般を対象とする。	監査基準を作成し、監査基準と比較しながら監査を実施。文章査閲とインタビューが中心で、場合によっては、現場を実査定する。	通常3年間を1サイクルとし全体の監査を実施。
② リスクアプローチ監査	情報システムプロセスに関連のあるリスクに対する内部統制の有効性を評価すること。(実証性の意味合いが強い)	重要なプロセスを対象とする。	対象となる内部統制の有効性を評価するチェックリストを作成し、評価を実施。インタビューおよび現場の実査により有効性を確認。	通常プロセスの優先順位に応じて年度毎に内部統制の評価を順次実施。
③ テーマ別監査	情報セキュリティシステム統合プロジェクト外部委託先変更管理等の各種テーマについて実証性と準拠性を監査すること。	テーマに応じた対象を都度選定する。	テーマに応じて詳細な監査の視点を作成し、監査を実施。情報システム設定の検証や場合によってはテストを実施。	通常年度毎にテーマを選定し、定期的に監査を実施。

## 6 情報システム監査の内容

ここでは、先に紹介した3種類のシステム監査の内容を詳しく見ていきます。

### 1:システム監査基準に則ったベンチマーク監査

システム監査基準に則った「システム監査」は、情報システムの企画・開発・運用について、信頼性・安全性・効率性の観点で、監査を実施するもので、監査対象は主として情報システム部門となります。つまり、情報システム部門のシステムの企画・開発・運用に関わる業務を主として監査することになり、エンドユーザによるシステムの利用に関わる部分は軽微な監査に留まるのが特徴です。

また、監査の報告先は、被監査部門である情報システム部門と経営になります。監査目的は、情報システム自体の信頼性・安全性・効率性を監査することであり、信頼性とは情報システムの品質並びに障害の発生、影響範囲及び回復の度合、安全性とは情報システムの自然災害、不正アクセス及び破壊行為からの保護の度合、効率性とは情報システムの資源の活用及び費用対効果の度合となります。監査内容は、システム監査基準をベンチマークに、対象となる情報システムの監査をシステム監査人がドキュメントの査読、担当者からのインタビュー、現場の実査を行うことにより実施します。監査計画としては、初年度に情報システム全般の概要を把握し、主として共通基盤となるシステムインフラおよび基幹系システムの監査を実施し、次年度以降に前年度のフォローアップ監査と個別システムの監査を順次実施していきます。監査体制は、通常ケースで2~3名のシステム監査人により年間20人日~60人日の監査を実施します。

### 2:リスクアプローチによる内部統制の有効性監査

内部統制監査は、リスクアプローチにより重要と識別した業務プロセスについて、情報システムが関連している部分の内部統制の有効性を評価するもので、監査対象は主として業務担当部門および該当する情報システムそのものとなります。つまり、情報システムを利用するエンドユーザ側からの視点(業務からの視点)で、情報システムを監査することになります。

また、監査報告先は業務部門(情報システムのオーナー)と経営になります。監査目的は、情報システム内に埋め込まれている内部統制の有効性を評価することであり、情報の入力、処理及び出力の過程において、情報の正確性と信頼性を直接的に保証する内部統制の有効度合いを評価することとなります。監査内容は情報システムの内部統制をヒアリング及びシステム設計書、実際の設定等から洗い出し、その有効性の評価をシステム監査人が実施します。監査計画は、業務監査が対象とするプロセスと連動し対象となるシステムが決定されます。通常は、毎年度、業務監査に付随する形態で情報システムの内部統制有効性監査を実施します。監査体制は通常ケースで、2~3名のシステム監査人及び場合により必要とする情報システムの各種エンジニアを加えて、年間40人日~100人日の監査を実施します。

## システム監査

### 3: テーマ別監査

テーマ別監査は、情報システムに関連する各種テーマを年度ごとに選択し監査を実施するものです。例えば、システムに大幅な改訂が入った場合には、変更管理監査を実施しますし、昨今のセキュリティ意識の高まりの中ではインターネットセキュリティにフォーカスした、不正侵入検査を実施したり、また個人情報保護法が施行されたことを契機に、個人情報保護状況監査を実施したり、もしくは、システムの開発や運用を外部委託している委託先が心配な場合には、委託先監査などを選定して実施します。

監査対象は、主として情報システム部門であり、監査報告先は被監査部門である情報システム部門と経営になります。監査目的は、情報システムにおける各種テーマについて、当該年度に重要と思われるものを選択し、監査を実施することです。監査内容は、情報システムの各種テーマについて詳細な部分まで掘り下げた監査を実施することが特徴です。つまり、一般的なシステム監査人だけではなく、情報システムの各種技術に精通したエキスパートをアサインして、監査を実施します。例えば、セキュリティ監査であれば、実際のハッカーと同等の不正侵入に関するスキルを有したエンジニアを活用するなどがあります。監査計画は、毎年度トピック的に重要なテーマに対して監査を実施しますので、柔軟な計画( 予算・スケジュール )を立てておく必要があります。監査体制は、通常のケースは2~3名のシステム監査人及び場合により必要とする情報システムの各種エキスパートにより、1テーマ20人日~50人日の監査を実施します。

## 7 プロテクトの情報システム監査支援サービス

プロテクトは、情報システム監査を実施しようと考えられているお客様に様々な支援を提供しています。

## 8 システム内部監査の全体計画の立案を支援するサービス

支援内容は、お客様のシステム内部監査担当者向けに知識教育の実施( システム監査に関わる認識の共通化を図る )、お客様の情報システム環境の分析・評価の実施( 計画策定に必要な前提となる情報を収集 )、お客様のシステム内部監査計画の原案作成( 計画のドラフティングを弊社で実施、後貴社と調整の上完成へ )となります。

ご支援のポイントとしては、業務監査他の内部監査計画と整合性をもった計画を策定させていただき、システム監査の各テーマ間で整合性をもった計画を作成させていただき、お客様の情報システムの現状を把握した上で、優先順位付けによる効果的な計画を策定させていただき、お客様の内部監査のリソースを踏まえたうえで、より効率的な計画の策定させていただき、

成果物は、システム内部監査計画書( 案 )を納品いたします。

## 9 システム内部監査の実施を支援するサービス

支援内容は、お客様のシステム内部監査担当者向けの知識教育の実施(システム監査に関わる認識の共通化を図る)、お客様の情報システム現状の分析・評価の実施(対象となる情報システムの情報を収集)、お客様の「システム内部監査基準および実施手続きの策定(弊社で案を作成、後貴社と調整の上完成へ)、お客様のシステム内部監査実施補助(実際の監査に帯同し支援およびOJTによる監査スキルの移転)、監査結果の分析・評価および改善提案の検討(監査基準とのギャップ分析)、監査報告書(案)の作成および報告支援(貴社と調整の上完成し、経営へ報告)となります。

ご支援のポイントとしては、グローバルスタンダード、国内標準、業界標準を参考にし、お客様としての監査基準を確立させていただくこと、システム監査の目的明確化と結果の有効活用を重視した手続きを策定させていただくこと、お客様情報システムの現状を把握した上で、効果的な監査を実施させていただくこと、お客様の内部監査のリソースを踏まえたうえで、より効率的な監査を実施させていただくことです。

成果物は、システム内部監査基準および実施手続き(案)、システム内部監査報告書(案)を納品させていただきます。また、監査ノウハウやスキルをお客様へ移転します。

## 10 情報システムの内部統制の有効性の評価をサービス

支援内容は、お客様のシステム内部監査担当者向けにシステムリスクアプローチの知識教育の実施(前提としてシステムリスクに関わる認識の共通化を図る)、お客様の情報システム環境のリスク分析・評価の実施(対象となるプロセスのリスクアセスメントを実施)、リスクに対する現状の内部統制を調査(内部統制の有効性評価基準を導出)、内部統制の有効性評価を実施(貴社監査人に帯同し評価支援およびOJTによる評価スキルの移転)、結果の取りまとめおよび問題点に関する改善提案を策定(評価結果のとりまとめ)、評価結果報告書(案)の作成および報告支援(貴社と調整の上完成し、経営へ報告)となります。

ご支援のポイントとしては、COSO、COBIT等のグローバルスタンダードを参考とし、お客様としてのリスクアプローチによる情報システムの内部統制評価手法を確立させていただくこと、内部統制の有効性の良し悪しが結論ではなく、対象となるリスクの程度を管理することを目的とすること、お客様の情報システムリスクの現状を把握した上で、実効性のある評価を実施させていただくこと、お客様の内部監査のリソースを踏まえたうえで、より効率的な評価を実施させていただくことです。

成果物は、情報システムリスクモデル(案)、情報システム内部統制モデル(案)、リスクアセスメント結果、内部統制評価基準および評価結果、内部統制の有効性評価結果報告書(案)を納品させていただきます。また、評価ノウハウやスキルをお客様へ移転します。

## 11 情報システムのテーマ別監査を支援するサービス

支援内容は、テーマ選定の支援(対象とするトピックを現状の環境から選定)、お客様システム内部監査担当者向けに監査知識教育(前提として監査に関わる認識の共通化を図る)、テーマに応じて、対象となる情報システムの環境調査を実施(現状の分析・評価)、監査基準、手続きの策定(監査の視点を導出)、監査環境の準備(テスト環境、監査環境の構築)、監査の実施(実際の監査に帯同し支援およびOJTによる監査スキルの移転)、監査結果の分析と改善提案の作成(問題点の抽出と課題の設定および解決策の導出)、評価結果報告書(案)の作成および報告支援(貴社と調整の上完成し、経営へ報告)となります。

ご支援のポイントとしては、貴社現状の優先順位を考慮したテーマを選定させていただくこと、テーマに応じて必要なスキルを保有したスペシャリスト(外部リソース含む)を提供させていただくこと、具体的な発見事項と実効性のある改善提案を導出させていただくこと、です。

成果物は、監査基準・手続き、監査結果報告書(案)を納品させていただきます。また、監査ノウハウやスキルをお客様へ移転します。

## 12 システム監査支援サービスを必要としているお客様の例

以下に列挙する事項に心当たりのあるお客様は、早急に弊社のシステム監査支援サービスの導入をご検討されることをお勧めいたします。

システム監査を行ったことがない

会計監査の一環として会計士にシステムを見てもらったことしかない

内部監査部門にシステム監査機能がなく、システム部門がシステム監査を実施している

システム内部監査体制が、法制度対応のレベルに留まっている

貧相な情報システムの内部統制、素人の技術者、複雑なシステム、分散されたシステムに、非常に高い信頼を寄せなければならない状況にある

方針や手順書がきちんとドキュメント化されておらず、情報システムの全体を把握する際や、個別の管理を実施する際に、支障が生じている

お客様の会社は、外部の第三者から何らかの保障(サービスアグリーメント、品質保証、など)を求められている

情報システム監査人を内部要員として確保し、高度化する技術やリスクを継続的に教育し、維持し続けることを難しいと感じられている