1-6-3 サービスマネジメント3 システム監査

目次 Contents

1　システム監査

ここでは、企業活動をチェックする監査の意味と、システム監査について学習します。

（1）監査業務

企業の財務や業務が法令や基準に違反していないか、**監査人**が客観的な立場で検証・評価することを**監査**と呼びます。

主な監査業務

種類	説明
会計監査	独立した監査組織によって、企業の経理・会計についての監査を行います。
業務監査	会計以外の企業の諸活動の内容や組織、制度に対する監査を行います
システム監査	システムの総合的な監査です。 （詳細は次ページ）
情報セキュリティ監査	情報セキュリティ監査基準、情報セキュリティ管理基準などを元に、情報セキュリティ体制に対する監査を行います。
個人情報保護監査	個人情報保護の標準でありJIS Q 15001やプライバシーマーク制度なども活用して個人情報を適切に管理できているか監査を行います。
コンプライアンス監査	著作権法、不正競争防止法、労働基準法など企業活動にかかわる法令を順守しているか監査を行います。

補足　内部監査と外部監査

企業などの被監査主体の監査部門が実施する監査を**内部監査**、外部の第三者機関が行う監査を**外部監査**と呼びます。

（2）システム監査

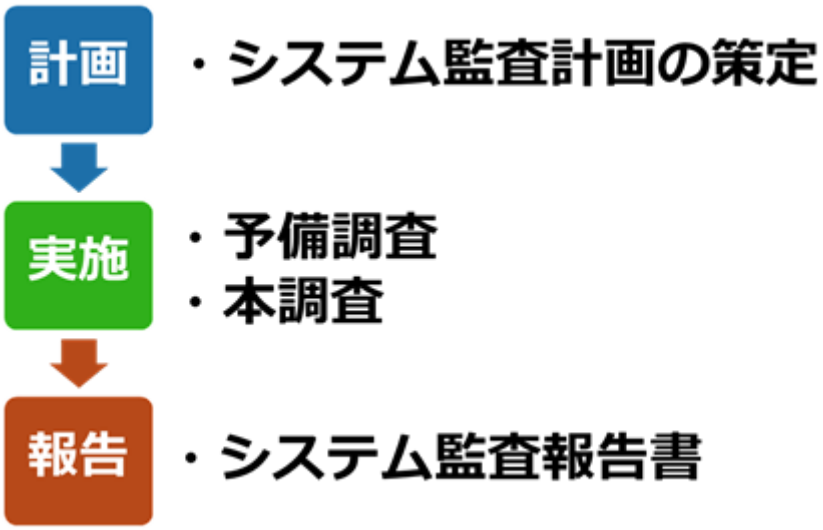
システム監査は、**システム監査人**と呼ばれる企業からは独立した組織（第三者）によって、システムを検証、評価し、その結果から助言や勧告を行うものです。一般的に、監査には経済産業省の**システム監査基準**を用います。

システム監査によって、情報システムの信頼性、安全性、効率性の向上を図ります。

- **信頼性の向上**：システム品質の向上、障害発生時の影響範囲縮小や回復の迅速化。
- **安全性の向上**：リスク（自然災害、不正アクセス、破壊行為）に対する準備。
- **効率性の向上**：費用対効果の向上、経営資源の有効活用。

システム監査の手順

システム監査は次の流れで進められます。



① システム監査計画の作成

システム監査の目的や監査対象を明確にし、監査手続きの内容や時期、範囲などを定める**システム監査計画**の策定を行います。

システム監査計画は、複数年度の**中長期計画書**、中長期計画書に基づいた年度ごとの**基本計画書**、基本計画書に基づいた監査項目ごとの**個別計画書**によって構成されます。

② 予備調査の実施

予備調査では、円滑な監査を行えるように対象資料の収集、分析し、チェックリストの作成、調査項目の洗い出し、個別計画書の修正を行います。

予備調査後は本調査の手順方法などを記述した**監査手続書**を作成します。

③ 本調査の実施

本調査では、監査手続書に従い、関連する記録や資料の調査、担当者へのインタビューなどを行います。また、情報システムの正当性や健全性を確認できる仕組み（**監査証跡**）などによって、監査対象の評価の裏付けとなる**監査証拠**を採取します。

監査の実施記録は**システム監査調書**としてまとめ、監査終了後も一定期間保管します。

④ システム監査報告書の提出・改善指導

本調査の結果を元に、総合的な評価をまとめ、経営者への結果説明のための**システム監査報告書**を作成し提出します。

システム監査報告書には、監査の実施状況、監査対象についての評価（保証意見や助言意見）、指摘事項などを記述します。緊急性があるものは改善勧告として報告し、改善指導（フォローアップ）も行います。

2　内部統制

次に、適正な企業活動にあたり重要な、企業自身の考え方や取り組みについてまとめます。

（1）内部統制

内部統制とは、企業が業務を適正に進めるための体制を構築し、運用する仕組みを指します。実現には、業務プロセスの明確化、職務分掌、実施ルールの設定及びそのチェック体制の確立が必要です。企業活動の健全化によって市場や顧客からの信頼を得ることを目的とした取り組みである**コーポレートガバナンス**（企業統治）の一環と言えます。

COSOフレームワーク

COSO（Committee of Sponsoring Organizations of the Tread way Commission）は、内部統制の世界標準とされる**フレームワーク**（枠組み）です。

内部統制の3つの目的

・業務　　：業務の有効性および効率性の維持向上
・財務報告　　：財務報告の信頼性の維持向上
・コンプライアンス：会社法や金融商品取引法といった内部統制関連法規の遵守

内部統制の5つの構成要素

構成要素	説明
統制環境	他の構成要素の基礎となる組織の気風を決定し、組織を構成する人々に影響を与えて、組織に規律と構造を提供します。
リスク評価	業務プロセスに潜むリスクと統制（コントロール）の対応関係を整理・検討・評価します。リスクの内容や影響、コントロールなどをまとめた**リスクコントロールマトリクス（RCM）**を作成します。
統制活動	経営者の命令や指示が適切に実行されるための方針や手続きのことです。権限や職責の適切な付与、職務分掌なども含まれます。
情報と伝達	必要な情報が把握でき、組織内外や関係者に正しく伝えられる状態を確保することです。
監査活動	**モニタリング**によって内部統制が機能していることを継続的に評価することを指します。これにより内部統制は監視、評価され、改善することができます。

（2）ITガバナンス

コーポレートガバナンスのうち、企業のIT化を進めるにあたり、企業戦略や情報システム戦略の実現に導く組織能力のことを**IT ガバナンス**と呼びます。

部門ごとの評価ではなく、企業全体として評価され、適切なIT化の推進には、情報システム戦略や目的の設定、**CIO**（Chief Information Officer：最高情報責任者）を中心としたIT化を実現しコントロールしていくための体制づくりが必要です。

経営戦略とIT戦略との整合性、費用対効果やリスク管理、人員、組織体制などの評価を行った上で、運用ポリシーや利用ルールの策定、マネジメントシステムの構築が必要となります。

IT統制

企業の内部統制やその他の活動のためにITを有効かつ効果的に利用することを**IT統制**と呼びます。いくらITを導入しても適正に活用されないと企業活動にとって有効にならないため、監視や統制が必要です。

企業全体の目標達成に対するIT活用能力がITガバナンスであるのに対し、IT統制は内部統制をはじめとする企業内の管理・統制のためにITを活用することを指します。

予防統制

IT統制のうち、日常業務において不正や誤り・ミスが起こらないようにあらかじめ管理することを指します。アクセス権限の適切な管理、マニュアル整備などがこれにあたります。

発見統制

IT統制のうち、不正やミスが発生時に速やかに発見することを指します。アクセス状況のモニタリングや入力チェックなどがこれにあたります。