Business Literacy

システム監査の基礎知識

東京デザインテクノロジーセンター専門学校　講師　石川敢也

Systems Audit

- 監査
  - 業務や成果物が、守るべき法令や社内規程などの規準を基に則っているかどうかを調査し、証拠を集めることによって、監査対象の有効性を利害関係者に合理的に保証すること。
- 内容
  - システム監査、システム監査人
  - 内部監査、監査報告書
  - コーポレートガバナンス、ITガバナンス
  - 内部統制、IT統制
  - 業務処理統制、全般統制
  - 職務分掌、事業継続計画策定ガイドライン

Systems Auditor

- システム監査
  - 組織体の情報システムに関わるリスク対策が適切に整備、運用されているかを、独立的な立場で検証すること。
  - 情報システムのリスクに対するコントロールが適切に整備、運用されていることを検証するための手段。
- システム監査人
  - 組織体の情報システムを独立した専門的な立場で検証または評価する者。
  - 監査計画の立案、予備調査、本調査、監査報告書の作成と提出、監査報告に基づく改善指導等を行う。
  - 監査対象者と利害関係を有することは許されない独立性と専門性が必要。

Independent Audit

- 独立性
  - 外観上の独立性
  - 精神上の独立性
  - 職業倫理と誠実性
- 専門能力
  - 情報セキュリティ監査人は、適切な教育と実務経験を通じて、専門職としての知識および技能を保持しなければならない。
- 守秘義務
  - 情報セキュリティ監査人は、監査の業務上知り得た秘密を正当な理由なく他に開示し、自らの利益のために利用してはならない。

Internal Audit

- 内部監査
  - 監査対象部門以外の自組織に属する者が、監査対象部門での業務がルールどおり実施されているかを確認する。
- システム監査報告書
  - システム監査人が作成した、監査証拠に裏付けられた合理的な根拠に基づく報告書。
  - 遅滞なく監査の依頼者に提出しなければならない。
- 監査証拠
  - 監査手続を実施して収集または監査人の判断に基づいて評価された検証可能な資料。

Corporate Governance

- コーポレートガバナンス
  - 企業の目的に適合した経営が行われるようにする企業統治。
  - 経営者または取締役会による企業の経営を、株主などの利害関係者が監督・監視する仕組み。
- ITガバナンス（IT Governance）
  - 企業が、ITの企画、導入、運営および活用を行うに当たり、関係者を含む全ての活動を適正に統制し、目指すべき姿に導くための仕組みを、組織に組み込む能力。

Internal Control

- 内部統制
  - 業務の有効性および効率性、財務報告の信頼性、不正を防止しリスクを低減する法令遵守、資産の保全を達成するために、企業内のすべての者によって遂行されるプロセス。
    - (1) 統制環境
    - (2) リスクの評価と対応
    - (3) 統制活動
    - (4) 情報と伝達
    - (5) モニタリング (監視活動)
    - (6) ITへの対応

Control Environment

- 統制環境
  - 組織の気風を決定し、統制に対する組織内のすべての者の意識に影響を与えるとともに、他の基本的要素の基礎をなし、リスクの評価と対応、統制活動、情報と伝達、モニタリング、ITへの対応に影響を及ぼす基盤。
- IT環境
  - 組織が活動する上で必然的に関わる内外のITの利用状況。
  - 社会および市場におけるITの浸透度、組織が行う取引等におけるITの利用状況、および組織が選択的に依拠している一連の情報システムの状況等のことを指す。

Information Technology Control

- IT統制
  - 内部統制システムのうち、ITを利用した部分。
  - 経営目標の達成に向けてITをマネジメントしていく組織内の仕組みのこと。
  - ITに係る全般統制や業務処理統制などに分類される。

Application Control

- 業務処理統制
  - 業務を管理するシステムにおいて承認された業務が全て正確に処理、記録されることを確保するための統制活動。
- 全般統制
  - 全社で共通に用いるシステム開発規程など、それぞれの業務処理統制が有効に機能する環境を保証する統制活動。
- 職務(しょくむ)分掌(ぶんしょう)
  - 内部統制の観点から、担当者間で相互けん制を働かせることで、業務における不正や誤りが発生するリスクを減らすために、担当者の役割を決めること。

Software Management Guidelines

- システム管理基準
  - 組織体が主体的に経営戦略に沿って効果的な情報システム戦略を立案し、その戦略に基づき情報システムの企画・開発・運用・保守というライフサイクルの中で、効果的な情報システム投資のための、またリスクを低減するためのコントロールを適切に整備・運用するための実践規範。
- ソフトウェア管理ガイドライン
  - ソフトウェアの違法複製等を防止するため、法人や団体等を対象として、ソフトウェアを使用するに当たって実行されるべき事項をとりまとめたもの。

Information Security Surveillance

- 情報セキュリティ監査
  - 独立かつ専門的な立場から、組織体の情報セキュリティの状況を検証または評価して、情報セキュリティの適切性を保証し、情報セキュリティの改善に役立つ的確な助言を与える活動。
- 情報セキュリティ監査人
  - 情報セキュリティ監査を実施する者。
  - 情報セキュリティ監査を実施する目的および対象範囲、並びに権限と責任は、文書化された規程または契約書等により明確に定められていなければならない。

Cybersecurity Management Guidelines

- サイバーセキュリティ経営ガイドライン
  - 経済産業省と独立行政法人情報処理推進機構が、サイバー攻撃から企業を守る観点で、認識する必要のあるリーダーシップ、パートナー、コミュニケーションの「三原則」と、責任者となる担当幹部（CISOなど）に指示すべき「重要10項目」をまとめたもの。
- 情報セキュリティ監査基準
  - 情報セキュリティ監査業務の品質を確保し、有効かつ効率的に監査を実施することを目的とした監査人の行為規範。

Security Guidelines on Computer Systems

- 情報システム安全対策基準
  - 情報システムの機密性、保全性および可用性を確保することを目的として、リスクを未然に防止し、発生したときの影響の最小化、回復の迅速化を図るため、情報システムの利用者が実施する対策項目を列挙したもの。
- コンピュータ不正アクセス対策基準
  - 被害の予防、発見および復旧並びに拡大および再発防止について、実行すべき対策をとりまとめたもの。
- コンピュータウイルス対策基準
  - コンピュータウイルスに対する予防、発見、駆除、復旧等について実効性の高い対策をとりまとめたもの。

Business Continuity Plan

- 事業継続計画策定ガイドライン
  - 事業継続計画の構築を検討する企業にとって、考え方の理解を促すガイドライン。
- BCP
  - 潜在的損失によるインパクトの認識を行い、実行可能な継続戦略の策定と実施、事業を継続させるための計画。
- BCM（Business Continuity Management）
  - 組織を脅かす潜在的なインパクトを認識し、利害関係者の利益、名声、ブランドおよび価値創造活動を守るため、復旧力および対応力を構築するための有効な対応を行うフレームワーク、包括的なマネジメントプロセス。

お疲れさまでした！