システム監査

○システム監査

情報システムを対象にした, 第三者による評価である. システムの複雑化・高度化に伴って, 当事者以外の利害関係者[1]が, システムの信頼性・安全性・効率性・有効性を把握しにくくなっている. そのため, 依頼を受けたシステムの専門家や担当部署が, システムの企画・開発・運用・保守・利用までの状況を客観的に評価し, お墨付き(保証)を与えたり, 助言したりする.

◆監査の種類

監査には, 大きく分けて 2 種類ある.

- 法定監査
  法律により実施が義務付けられている監査. 例えば, 会計監査・内部統制監査

- 任意監査
  法律により実施が義務付けられていない監査. 例えば, 取引先や契約先からの信頼を得るために行う監査.

システム監査は, 任意監査の一種であるが, 法定監査である会計監査・内部統制監査において, その一部として行われることが多い. その場合, システム監査人は, その監査チームの一員として監査を行う.

また, 他にも次のように監査を分類することができる.

- 保証型監査
  コントロールが適切であることを「保証」するために行う監査

- 助言型監査
  問題点を指摘し, 改善を助言するために行う監査

◆システム監査人

システム監査を行う人のことである. 監査を受ける組織から, 身分上の独立性を確保し, 客観的な立場にいるという外観に配慮しなければならない. 監査人は, 監査計画を立案し, 監査を実施し, 関西圏を監査依頼者に報告し, 被監査部門による改善をフォローアップする[2].
システム監査基準では, システム監査人に次の資質および責務を要求している.

- 外観上の独立性[3]
  監査対象から独立し, 被監査主体と身分上, 密接な利害関係を有しない

- 精神上の独立性
  偏向を排し, 常に公正かつ客観的に監査判断を行う

- 職業倫理, 及び誠実性
  職業倫理に従い, 誠実に業務を実施する

- 守秘義務
  正当な理由なく, 監査業務上で知り得た情報をほかに開示したり不当に利用したりしない

---

1 顧客・取引先・株主・金融機関等
2 システム監査人は関西圏に責任を持つが, 自らは問題の改善は行わない(フォローアップのみ). 改善は被監査部門が主導する.
3 独立性の観点からは, 被監査部門に所属する者が監査人になってはならない. 過去に被監査部門に所属していた場合には, 1 年以上のクーリングオフ期間が必要

○システム監査基準

システム監査のために, 経済産業省が策定したガイドラインは, 次のとおりである.

- システム監査基準
  監査人の行為規範[4]で, 監査人が行うべき内容をまとめたもの. 例えば, 独立性の確保・守秘義務

- システム管理基準
  システム監査を受ける組織の実践規範[5]で, システム監査において組織が行うべき推奨事例をまとめたもの. また, システム管理基準にどれほど沿っているかが, 監査における判断の尺度(基準)となる.

○情報システムの可監査性

情報システムの可監査性とは「監査を実施しやすい」ことを意味する性質である. 具体的には「コントロールが存在し, 有効に機能していることを証拠で示すことができる」ことで, 次の要件を含める.

表　可監査性の要件

コントロールの存在	情報システムに信頼性, 安全性, 効率性を確保するようなコントロールが含まれていること
監査証跡の存在	情報システムの信頼性, 安全性, 効率性が確保されていることを, 事後的かつ継続的に検証するための手段が用意されていること

4　守るべきとされるルール
5　行うべきとされるルール

○システム監査の流れ

システム監査の流れは, ① 監査計画➡②予備調査➡③本調査➡④評価➡⑤監査報告➡⑥改善指導である.

◆①監査計画

「なぜ今回, システム監査を行うことになったか？」など, システム監査に至る経緯・現状・抱える課題をもとに, システム監査の目的・対象範囲・時期についてまとめる段階である.

●監査計画書

監査計画の段階でまとめられる資料のこと

◆②予備調査

本調査に至るまでの, 事前準備の段階である. 本調査で確認すべき, 監査要点・監査証拠・監査手続を, 監査を受ける組織の関係者へのインタビューなどを元に検討する段階である. どの問題点について(監査要点), 何を(監査証拠), どこから・どのようにして(監査手続), 入手すべきかをまとめる. たとえば「事前入手した資料の閲覧」や「リスク認識に関するアンケート調査」などが予備調査で実施される.

予備調査の手順は①監査対象の現状分析➡②問題点の認識➡③個別計画書の見直しである.

- 監査要点
  システム監査における問題点

- 監査証拠
  監査の結論を立証するための裏付け. 証憑ともいう. 監査業務の実施記録である監査調書にまとめられる.

- 監査手続
  監査証拠を入手するための手法・手順・手続

さらに, 監査要点について, そのリスクを統制するための対策であるコントロールをする.

●監査手続書

予備調査の段階でまとめられる資料のこと

◆③本調査
監査手続書にもとづき, 監査手続により, 資料や現場を査閲[6]したり, 関係者にインタビューしたりして, 監査証拠を入手する段階である. 実施した監査手続・入手した監査証拠・発見した事実などをまとめ, 監査のプロセスを記録する.

●監査調書
本調査の段階でまとめられる資料である.

表　基本的な監査技法

チェックリスト法	監査人が作成したチェックリスト(質問書)に対して, 特定者から回答を求める方法. 標準の質問書を利用するときは, 監査対象に適合するように質問の範囲や内容を調整する
ドキュメントレビュー法	特定の情報を収集するために, 関連する資料や文書類を監査人自らレビューする方法. 事前準備として, 被監査部門のドキュメント整備状況を把握しておく
突合法・照合法	関連する記録を突き合わせる方法(例えば, 記録された最終結果とその起因となった事象を示す原始データまでさかのぼり突合せをする
現地調査法	システム監査人が現地に赴き, そこでの作業状況を自ら調査する方法. 原始データの視点から流れに沿って作業を追跡調査する方法や, 一定の作業環境を一定時間ごとに調査する方法などがある
インタビュー法[7]	特定の事項を立証するために, システム監査人が特定の者に直接問い合わせを行い, 回答を得る方法

6　実際に見て, 調べること
7　インタビュー(ヒアリング)で得た回答に関しては, これを裏付ける文書や記録を入手するよう努める

◆④評価・結論
監査調書をもとに, 監査を受けた組織に, お墨付き(保証)を与えたり, 助言したりするための最終的な結論をだす段階である. 監査の実施記録とともに, 監査の結論として, 記載する例は, 次のとおりである.

- 指摘事項
  リスクとなる問題点. その重大性・リスクとなる根拠も併記する

- 改善勧告
  指摘事項に対するコントロール. その重要度・緊急度・改善による効果・改善を担当すべき部署も併記する

●監査報告書
評価・結論の段階でまとめられる資料のこと

◆⑤監査報告
システム監査の依頼者(経営そうに対し, 監査報告書をもとに監査の結果を報告する段階である. なお, 改善勧告が含まれていても, 監査人がみずから改善勧告の内容を行うことはない.

◆⑥改善指導(フォローアップ[8])
改善勧告について, 適切な措置が講じられているかを確認する段階である. 改善するための計画や, その実施状況を確認する.

◆その他の監査用語
監査に関するその他の用語は, 次のとおりである.

- 監査証跡[9]
  監査の過程を追跡し確認できる仕組み. 例えば, 監査証拠を入手する過程を記録したログ[10]. これを用いることで, 事象の発生から最終的な結果までを双方向に追跡することができる. 各種システムのログファイルは有力な監査証跡である.

- リグレッションテスト[11]
  システムに修正・機能の追加を行うことにより, 関連する他のシステムに想定外の影響が及んでいないかを確認するためのテスト. レグレッションテスト・対抗テストともいう.

8 語源は, follow-up(追跡・追求)から
9 アクセスログ→安全性の監査証跡. エラー状況の記録→運用業務の監査証跡
10 履歴を時系列に記録・蓄積したデータ. あとでたどったり, 分析したりする目的で利用する.
11 語源は, regression(後戻り・逆行すること)＋test(検査)から

○コントロール[12]

リスクを統制するための対策である. 監査の目的には, 問題点の発見だけでなく, 「コントロールが適切に実施されているか」を評価することも含まれる. 法律や行政指導面などの外部統制と, 組織内部の基準やチェック体制である内部統制に分けられる.

◆コントロールの種類

- 予防的コントロール[13]
  ミスや不正を防ぐためのコントロール. 例えば, ミスをしにくい画面を設計する・適切なアクセス権限を付与する
- 発見的コントロール[14]
  ミスや不正を発見するためのコントロール. 例えば, 入力した値の合計値や件数を元データと比較する.

◇相互牽制[15]

システム監査を受ける組織では, 誤りや不正行為を防止するために, 職務を分離し, ダブルチェック[16]により相互牽制を行う必要がある. 相互牽制が機能していない現状に対する問題点や改善策を記述させる設問がよく出る.

◆ダブルチェックによる相互牽制が機能しない例
×業務のやりっぱなしで, その後に承認を受けるプロセスがない場合
×データ入力について, 1 人で, 入力権限をもち, かつ承認権限も持つ場合
×利用者 ID の管理について, 1 人で, 操作権限をもち, かつ承認権限も持つ場合

12 組織が正常に活動するための仕組み
13 予防統制ともいう
14 発見統制ともいう
15 相手の自由な行動をおさえ, 妨げること
16 ある事柄の確認を, 1 人ではなく複数人で行うこと

○内部統制[17]
企業が財務会計でミスや不正を行わないように, 組織内部のルールや仕事のやり方を整備・実施・証明することである. 例えば, 担当者任せ・部署任せだと, 不正行為が発生しやすくなるため, 相互にチェックするルールを整備する.

企業会計審議会が 2007 年 2 月に発表した内部統制の「実施基準」では, IT 業務処理統制として次の 4 項目を挙げている.

1. 入力情報の完全性, 正確性, 正当性等を確保する統制
2. 例外処理(エラー)の修正と再処理
3. マスタデータ[18]の維持管理
4. システムの利用に関する認証, 操作範囲の限定などアクセスの管理

監査において「起票された受注伝票が漏れなく, 重複することなく入力されていることを確かめる」には入力データの完全性および一意性に係るコントロール項目をチェックすることになる.

●プルーフリスト
入力データを加工せずにそのままプリントアウトしたもので, このプルーフリストと受注伝票を照合することで, 入力データの完全性および一意性が確認できる. 監査においてはこの称号が確実に実施されているかを確認するために照合印をチェックすることがポイントとなる.

●職務分離
内部統制のため, 職務を異なる担当者で分担し, 互いを牽制すること.

◆内部統制の基本要素
金融庁による“財務報告に係る内部統制の評価及び監査の基準”では, 内部統制を構成する基本的要素として, 次を挙げている. 最初の五つは, COSO フレームワークと呼ばれるモデルをベースとし, これに金融庁が「IT への対応」を付け加えた.

表　内部統制の基本的要素

統制環境	経営者が内部統制の必要性を理解し, 企業理念や風土を反映する
リスクの評価と対応	各リスクを識別し, 適切な対策の策定と実施を進める
統制活動	各業務プロセスにおいて適切なチェック, 承認, 記録などを行う
情報と伝達	各種情報を適切な範囲に公開し, 入手・利用できるようにする
モニタリング	第三者の視点による監査を行う
IT への対応	情報システムを活用し, 適切な権限制御やログ記録などを行う

「IT への対応」は, 内外の IT 環境に適切に対応していること, 統制に IT を有効に利用していること, IT そのものが適切に管理されていることを含む[19].

◆CSA(統制自己評価)[20]
CSA は, 内部統制の状況を業務をよく知る担当者が評価し, 自律的に改善する手法である. 第三者による内部監査を補足する方法として, 特に現場におけるリスク管理や危機管理に用いられている.

17 法令違反・粉飾決算などがないように, ルールや仕事のやり方を, 整備・実施・証明すること
18 master data . システムを動かす前から入れておく必要のあるデータ. 一方でシステムを動かすことによって蓄積されていくデータのことをトランザクションデータと呼ぶ.
19 IT への対応は「IT 環境への対応」と「IT の利用および統制」からなる.
20 内部統制の「自己評価」「自己改善」

○IT 統制
内部統制のうち, IT に関連した内容を統制することである. システムやシステムを使った業務について, ルールや仕事のやり方を整備・実施・証明する.

統制の対象には, 次の 2 種類がある.

◆IT 業務処理統制
システムを使った業務を統制することである.

- あらかじめ決まった金額を入力する際, 手入力ではなく, 金額を一覧から選択する方式にする.
- 事前に設定した限度額を超える入金・出力処理は行わない.

◆IT 全般統制
IT 業務処理統制を実施できるように, 適切にシステムを開発・運用することである. 仮に, 正しく IT 業務処理統制を行っても, そもそもシステム自体に誤りがあれば, 内部統制が不十分になるため, システムの開発・運用を統制する.

IT 全般統制で問題となる例は, 次のとおりである.
- システムの欠陥により, 財務情報システムのデータを削除した.
- 財務情報システムのアクセス権を不適切に付与したため, 会計の数値が外部に流出した.

◆情報システムのコントロール
情報システムのコントロールとは, システムの信頼性, 安全性, 効率性に影響を与えるリスクを処理する仕組みのことである. 情報システムの監査では, それらのコントロールが適切に整備され, 機能していることを確かめる.

○IT ガバナンス[21]
企業が, 経営目標を達成するために, IT を過不足なく活用することである. 経営戦略をもとに適切な IT 戦略を決めたり, 情報セキュリティや財務会計などの面で問題とならないように, 従業者による IT の利用を統制したり, システム監査は, 最終的に IT ガバナンスの実現に役立てるために実施する.

21 語源は, governance(管理・支配・統治)から. 法的拘束力のあるガバメント(government・政府)とは対象的に, 組織が主体的に行う意思決定・合意形成のこと.