Chapter３

システム監査

# 1.　システム監査

学習のポイント

✅ まずは監査の大まかな流れを掴み、出題頻度を参考に、用語や考え方を覚えよう！

✅ システム監査人の立場として、独立性が重要であることを覚えよう！

## 1. 監査業務

監査とは、独立した立場の監査人が、対象となる事象が遵守すべき法令や規則に違反していないどうか、収集した証拠に基づいて評価し、その結果を利害関係者に報告することです。

代表的な監査業務には、会計監査、業務監査、情報セキュリティ監査、システム監査などがあります。

#### ①システム監査

システム監査は、組織の情報システム環境を対象とした監査で、監査対象から独立かつ客観的立場のシステム監査人が実施します。経済産業省が平成30年に改訂したシステム監査基準では、システム監査を「専門性と客観性を備えたシステム監査人が、一定の基準に基づいて情報システムを総合的に点検・評価・検証をして、監査報告の利用者に情報システムのガバナンス、マネジメント、コントロールの適切性等に対する保証を与える、又は改善のための助言を行う監査の一類型である。」と定義しています。

#### ②情報セキュリティ監査

情報セキュリティ監査は、企業の情報セキュリティマネジメントの現状を対象とした監査で、監査対象から独立かつ客観的立場の情報セキュリティ監査人が実施します。

🏋プラスアルファ

**●会計監査**

会計監査は、企業の公表する財務諸表の記載内容を対象とした監査で、外部の監査人（公認会計士や監査法人）が実施する会計監査人監査（**外部監査**）と、会社内部の監査人である監査役が実施する監査役監査（**内部監査**）があります。

**●業務監査**

業務監査は、取締役の業務執行の内容を対象とした監査で、会社内部の監査人である監査役が実施します（内部監査）。

なお、会計監査や業務監査は、法律で実施を義務付けられた法定監査ですが、情報セキュリティ監査とシステム監査は法定監査ではなく、実施するか否かは経営者の判断による任意監査です。

|  |
| --- |
| 例題　プラスアルファ  システム監査と情報セキュリティ監査における監査対象を説明したものはどれか。  ア　システム監査では情報システムにかかわらない文書情報を対象に含めないが，情報セキュリティ監査では含める。  イ　システム監査と情報セキュリティ監査は，ともにすべての情報資産を対象とする。  ウ　情報セキュリティ監査では情報システムにかかわる人を対象に含めないが，システム監査では含める。  エ　情報セキュリティ監査は情報システムを対象としないが，システム監査は対象とする。  システム監査では、監査対象は情報システムにかかわるものに限定されます。これに対して情報セキュリティ監査では、情報システムにかかわらないものも監査対象に含まれます。  システム監査　平成18年度春　問52　[出題頻度：★☆☆]  解答－ア |

別冊演習ドリル 》 2-72

## 2. システム監査基準・システム管理基準

### １）監査人の行為規範、システム監査上の判断尺度

システム監査基準は、システム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**です。

システム監査基準（平成30年）は、システム監査の体制整備に係る基準、システム監査人の独立性・客観性及び慎重な姿勢に係る基準、システム監査計画策定に係る基準、システム監査実施に係る基準、システム監査報告とフォローアップに係る基準の５つの基準から構成されています。

なおシステム監査を具体的に実施するに当たっては、システム監査基準の姉妹編であるシステム管理基準が、**システム監査上の判断尺度**として用いられています。

システム監査人は、システム監査基準に記載された監査方法にしたがって、監査対象がシステム管理基準に沿っているかを判断することになります。

|  |
| --- |
| 例題  “システム監査基準”が果たす役割はどれか。  ア　監査上の判断尺度 イ　監査手続書作成のチェックリスト  ウ　監査人の行為規範 エ　システムの品質管理ガイドライン  システム監査基準（平成30年）の前文に、「「システム監査基準」とは、情報システムのガバナンス、マネジメント又はコントロールを点検・評価・検証する業務の品質を確保し、有効かつ効率的な監査を実現するためのシステム監査人の行為規範である。」と記述されています。  システム監査　平成19年度春　問42　[出題頻度：★☆☆]  解答－ウ |

別冊演習ドリル 》 2-73,74

### ２）監査人の独立性・客観性及び慎重な姿勢

#### ①独立性と客観性

システム監査基準（平成30年）の「基準４　システム監査人としての独立性と客観性の保持」に、「システム監査人は、監査対象の領域又は活動から、独立かつ客観的な立場で監査が実施されているという外観に十分に配慮しなければならない。また、システム監査人は、監査の実施に当たり、客観的な視点から公正な判断を行わなければならない。」と記述されており、前半部分を外観的独立性、後半部分を精神的独立性と呼び、合わせて**監査人の独立性**と呼びます。

**精神的独立性**とは、システム監査実施に当たり、常に公正で客観的な監査判断を行うことであり、**外観的独立性**とは、精神的独立性を担保するものとして、被監査部門と身分上、密接な関係がないことをいいます。システム監査を客観的に実施するために、**監査人の独立性**は欠かせません。

|  |
| --- |
| 例題  経営者が社内のシステム監査人の外観上の独立性を担保するために講じる措置として，最も適切なものはどれか。  ア　システム監査人にITに関する継続的学習を義務付ける。  イ　システム監査人に必要な知識や経験を定めて公表する。  ウ　システム監査人の監査技法研修制度を設ける。  エ　システム監査人の所属部署を内部監査部門とする。  システム監査人は、システム監査を客観的に実施するために、監査対象となる組織体から独立した立場の者でなくてはなりません。これを監査人の独立性といいます。  監査人の独立性は、さらに精神的独立性と外観的独立性に分けられます。  精神的独立性とは、システム監査実施に当たり、常に公正で客観的な監査判断を行うことであり、外観的独立性とは、精神的独立性を担保するものとして、身分のうえで被監査部門と密接な関係がないことをいいます。  基本情報　令和4年度サンプル　問47　[出題頻度：★★★]  解答－エ |

別冊演習ドリル 》 2-75～77

## 3. システム監査の目的と手順

### １）システム監査の目的

システム監査基準（平成30年）には、「システム監査は、情報システムにまつわるリスクに適切に対処しているかどうかを、独立かつ専門的な立場のシステム監査人が点検・評価・検証することを通じて、組織体の経営活動と業務活動の効果的かつ効率的な遂行、さらにはそれらの変革を支援し、組織体の目標達成に寄与すること、又は利害関係者に対する説明責任を果たすことを目的とする。」と記述されています。具体的には、企業の情報システム環境を、本来あるべき姿に向けて指導・改善することがシステム監査の目的です。

### ２）システム監査の流れ

システム監査は、リスクの評価に基づく監査計画の策定、監査証拠の入手と評価、監査調書の作成と保管、監査の結論の形成、監査報告書の作成と提出、改善提案のフォローアップの流れで行われます。

|  |
| --- |
| 例題  システム監査基準（平成30年）における，組織体がシステム監査を実施する目的はどれか。  ア　自社の強み・弱み，自社を取り巻く機会・脅威を整理し，新たな経営戦略・事業分野を設定する。  イ　システム運用部門によるテストによって，社内ネットワーク環境の脆弱性を知り，ネットワーク環境を整備する。  ウ　情報システムにまつわるリスクに適切に対処しているかどうか点検・評価・検証することで，組織体の活動の効果的かつ効率的な遂行，その変革を支援し，目標達成に寄与する。  エ　ソフトウェア開発の生産性のレベルを客観的に知り，開発組織の能力を向上させるために，より高い生産性レベルを目指して取り組む。  ア　SWOT分析に関する記述です。  イ　ネットワークの脆弱性検査に関する記述です。  エ　CMMIに関する記述です。  基本情報　平成28年度春　問60(改)　[出題頻度：★★☆]  解答－ウ |

🏋プラスアルファ

**4. システム監査の対象業務**

システム監査基準（平成30年）の前文に、「システム監査とは、専門性と客観性を備えたシステム監査人が、一定の基準に基づいて情報システムを総合的に点検・評価・検証をして、監査報告の利用者に情報システムのガバナンス、マネジメント、コントロールの適切性等に対する保証を与える、又は改善のための助言を行う監査の一類型である。」と記述されています。情報システムなどの情報技術のガバナンスは、**ITガバナンス**と呼ばれ、システム管理基準（平成30年）では、「経営陣がステークホルダのニーズに基づき、組織の価値を高めるために実践する行動であり、情報システムのあるべき姿を示す情報システム戦略の策定及び実現に必要となる組織能力」と定義されています。したがって、システム監査の対象業務は、情報システムが正しく管理、運用されていることに加え、経営などにおける組織の価値を高めることに貢献できる情報システムとなるように改善していくための助言も含まれることになります。

|  |
| --- |
| 例題　プラスアルファ  システム監査報告書に記載された改善勧告に対して，被監査部門から提出された改善計画を経営者がITガバナンスの観点から評価する際の方針のうち，適切なものはどれか。  ア　１年以内に実現できる改善を実施する。  イ　情報システムの機能面の改善に絞って実施する。  ウ　経営資源の状況を踏まえて改善を実施する。  エ　被監査部門の情報化予算の範囲内で改善を実施する。  ア　１年以内に実現できるというように期限を区切るのではなく、必要な改善であれば実施しなければなりません。  イ　情報システムの機能面の改善に絞るのではなく、必要な改善であれば実施しなければなりません。  エ　被監査部門の情報化予算の範囲内と予算を区切るのではなく、企業全体の予算の中で、必要な改善であれば実施しなければなりません。  応用情報　平成23年度春　問60　[出題頻度：★☆☆]  解答－ウ |

🏋プラスアルファ

**5. システム監査計画の策定**

システム監査人は、実施するシステム監査の目的を有効かつ効率的に達成するために、監査手続の内容、時期および範囲について、適格なシステム監査計画を立案しなければなりません。具体的には、まず企業の中長期のシステム化計画に基づいた中長期システム監査計画を作成します。次に、これに基づいて年度ごとの基本計画書を作成します。**基本計画書**には、その年度に実施する監査対象、重点監査テーマ、実施体制および年間計画などが記述されます。さらに、この基本計画書に基づいて個別計画書を作成します。**個別計画書**には、個々の監査対象ごとに監査目的、監査範囲と手続き、期日および日程、責任者および業務分担、報告時期などの具体的な監査活動が記述されます。なお監査計画は、事情に応じて適時に修正できるように弾力的に運用しなければなりません。

|  |
| --- |
| 例題　プラスアルファ  システム監査の個別計画書の説明として，適切なものはどれか。  ア　監査対象，監査目的，監査範囲，監査手続，監査実施日，責任者，分担及び報告時期を記載したものである。  イ　基本計画書に基づいて，個別のシステム監査業務のスケジュールを定めたものである。  ウ　基本計画書に基づいて，当該年度に実施するシステム監査の計画を示すものである。  エ　予備調査の結果に基づいて，監査の方針を記載したものである。  イ　基本計画書に関する記述です。  ウ　基本計画書に関する記述です。  エ　中長期計画書に関する記述です。  情報セキュリティアドミニストレータ　平成13年度秋　問48　[出題頻度：★☆☆]  解答－ア |

別冊演習ドリル 》 2-78

## 6. システム監査の実施（予備調査、本調査、評価、結論）

システム監査人は、監査計画に基づいて十分な調査を行い、システムを点検、評価、検証します。

#### ①監査手続の適用

システム監査は、監査計画に基づき、「予備調査」、「本調査」および「評価・結論」の手順によって実施しなければなりません。実施に当たっては、具体的な手順や方法を記載した**監査手続書**を作成します。

**予備調査**は、監査対象の実態を明確に把握するために行うアンケート調査、資料収集などで、「監査対象の現状分析」、「問題点の洗い出し」、「本調査の見直し」の順に行います。

予備調査の結果を受けて行われる**本調査**は、監査目的にしたがって対象業務の実態を調査・分析・検討することで、「現状の確認」、「監査証拠の入手」、「証拠能力の評価」の順に行います。

なお予備調査および本調査では、必要があれば専門家の支援を受けます。

|  |
| --- |
| 例題  システム監査の手順に関する記述のうち，適切なものはどれか。  ア　監査作業は，予備調査，本調査，評価・結論，指導事項に対する改善の順に行う。  イ　評価・結論の作業は，監査担当者による評価，被監査部門による評価，監査責任者による評価を順に経て，最終結論を下す。  ウ　本調査の作業は，予備調査結果の確認，監査証拠の入手，証拠能力の評価の順に行う。  エ　予備調査の作業は，同業他社の状況調査，被監査部門の過去の監査結果の評価，サンプリングによる実地調査の順に行う。  ア　予備調査は計画ではなく、事前準備のための情報収集です。  イ　最終結論はシステム監査人が自らの判断で行います。  エ　予備調査は、監査対象の現状分析、問題点の洗い出し、本調査の見直しの順に行います。  システム監査　平成27年度春Ⅱ　問7　[出題頻度：★☆☆]  解答－ウ |

別冊演習ドリル 》 2-79～81

#### ②監査証拠の入手と評価

システム監査人は適切かつ慎重に監査手続を実施し、保証または助言について監査結果を裏付けるのに十分かつ適切な監査証拠を入手し、評価しなければなりません。

監査証拠とは、システム監査報告書に記載する監査意見を立証するために必要な事実を意味し、物理的証拠、文書的証拠、文書化された口頭的証拠などに大別されます。

そしてこれらの一連の監査証拠が結びつき、監査対象システムの入力から出力に至る過程を追跡できる一連の仕組みと記録を**監査証跡**と呼びます。

なお監査証跡は、多ければ多いほど監査人は被監査対象を評価しやすいですが、処理過程を全て記録しておくことは経済性を損なうおそれがあるので、必要十分な監査証跡を決定し、被監査対象にその確保を依頼すべきです。

|  |
| --- |
| 例題  システム監査において，監査証拠となるものはどれか。  ア　システム監査チームが監査意見を取りまとめるためのミーティングの議事録  イ　システム監査チームが監査報告書に記載した指摘事項  ウ　システム監査チームが作成した個別監査計画書  エ　システム監査チームが被監査部門から入手したシステム運用記録  監査証拠は、システム監査報告書に記載する監査意見を立証するために必要な事実を意味し、物理的証拠、文書的証拠、文書化された口頭的証拠などに大別されます。  なお被監査部門以外の第三者から入手した文書は、被監査部門から入手した同種の文書よりも、監査証拠として強い証明力があります。  情報セキュリティマネジメント　平成30年度春　問39　[出題頻度：★☆☆]  解答－エ |

別冊演習ドリル 》 2-82～85

#### ③監査調書の作成と保管

システム監査人は、実施した監査手続の結果とその関連資料を、監査調書として作成しなければなりません。監査調書は、監査結果の裏付けとなるため、監査の結論に至った過程がわかるように秩序整然と記録し、適切な方法によって保存しなければなりません。

|  |
| --- |
| 例題  監査調書の説明はどれか。  ア　監査人が行った監査手続の実施記録であり，監査意見の根拠となる。  イ　監査人が監査実施に当たり被監査部門に対して提出する，監査人自身のセキュリティ誓約書をまとめたものである。  ウ　監査人が監査の実施に利用した基準書，ガイドラインをまとめたものである。  エ　監査人が正当な注意義務を払ったことを証明するために，監査報告書とともに公表するよう義務付けられたものである。  監査調書は、システム監査人が実施した監査手続の結果とその関連資料を監査結果の裏付けとなるように、監査の結論に至った過程がわかるように秩序整然と記録し、適切な方法によって保存したものです。  基本情報　平成29年度秋　問60　[出題頻度：★☆☆]  解答－ア |

別冊演習ドリル 》 2-86

#### ④代表的なシステム監査技法

**インタビュー法**は、直接、関係者に口頭で回答を求める（ヒアリングする）方法です。

チェックリスト法は、過去の経験をもとに作成された標準的な仕様のチェックリスト形式の質問書を監査目的や被監査部門の状況に合わせてシステム監査人が修正したものに対して、関係者から回答を求める方法です。

ドキュメントレビュー法は、監査証拠を入手するために、関連する資料や文書類を評価・検討する方法です。

ウォークスルー法は、データの生成から入力、処理、出力、活用までのプロセスを、書面上または実際に追跡する方法です。

突合・照合法は、原始資料まで遡って、関連する証拠資料を突き合わせる方法です。

現地調査法は、現地（被監査部門）で自ら観察・調査する方法です。

コンピュータ支援監査技法は、監査対象ファイルの検索、抽出、計算等のシステム監査上使用頻度の高い機能に特化したシステム監査を支援する専用のソフトウェアや表計算ソフトを利用する方法です。

|  |
| --- |
| 例題  システム監査人がインタビュー実施時にすべきことのうち，最も適切なものはどれか。  ア　インタビューで監査対象部門から得た情報を裏付けるための文書や記録を入手するよう努める。  イ　インタビューの中で気が付いた不備事項について，その場で監査対象部門に改善を指示する。  ウ　監査対象部門内の監査業務を経験したことのある管理者をインタビューの対象者として選ぶ。  エ　複数の監査人でインタビューを行うと記録内容に相違が出ることがあるので，１人の監査人が行う。  イ　その場で監査対象部門に改善を指示することはありません。  ウ　情報を提供したものをインタビューの対象者として選びます。  エ　客観性の面からも、複数の監査人でインタビューを行います。  基本情報　平成31年度春　問58　[出題頻度：★★★]  解答－ア |

別冊演習ドリル 》 2-87

## 7. システム監査の報告とフォローアップ

システム監査基準（平成30年）のシステム監査報告とフォローアップに係る基準で、監査報告書の作成と提出について、監査報告書の記載事項、改善提案のフォローアップ（改善指導）などについて定めています。

#### ①監査報告書の提出と開示

システム監査人は、監査の目的に応じた適切な形式の監査報告書を作成し、遅滞なく監査の依頼者に提出しなければならなりません。監査報告書の外部への開示が必要とされる場合には、システム監査人は、監査の依頼者と慎重に協議のうえで開示方法を考慮しなければなりません。なお監査の依頼者とは主に組織体の長をいいます。

|  |
| --- |
| 例題  システム監査の実施体制に関する記述のうち，適切なものはどれか。  ア　監査依頼者が監査報告に基づく改善指示を行えるように，システム監査人は監査結果を監査依頼者に報告する。  イ　業務監査の一部として情報システムの監査を行う場合には，利用部門のメンバによる監査チームを編成して行う。  ウ　システム監査人が他の専門家の支援を受ける場合には，支援の範囲・方法，及び監査結果の判断は，他の専門家の責任において行う。  エ　情報システム部門における開発状況の監査を行う場合には，開発内容を熟知した情報システム部門のメンバによる監査チームを編成して行う。  イ　業務監査の一部として情報システムの監査を行う場合には、ユーザ部門は被監査対象になります。したがって、ユーザ部門が監査人になることは独立性に反します。  ウ　他の専門職による支援を仰ぐ場合であっても、利用の範囲、方法、および結果の判断等は、システム監査人の責任において行わなければなりません。  エ　自部門で行っている開発の状況を監査することは、独立性に反します。  基本情報　平成29年度春　問60　[出題頻度：★☆☆]  解答－ア |

別冊演習ドリル 》 2-88

#### ②監査報告書の記載事項

監査報告書には、監査人が負うべき責任の範囲を明確にするために、実施した監査の対象、実施した監査の概要、監査の結論（**保証意見**、**助言意見、指摘事項**、**改善勧告**）、その他特記すべき事項について、証拠との関係を示し、システム監査人が監査の目的に応じて必要と判断した事項を明瞭に記載しなければなりません。

なお、システム監査人には法的な権限はないため、問題点を発見した場合、監査報告書によって指摘事項を示し、改善勧告をすることはできますが、直接監査対象に改善命令を行うことはできません。

|  |
| --- |
| 例題  システム監査人の行為のうち，適切なものはどれか。  ア　調査が不十分な事項について，過去の経験に基づいて監査意見をまとめた。  イ　調査によって発見した問題点について，改善指摘を行った。  ウ　調査の過程で発見した問題点について，その都度，改善を命令した。  エ　調査の途中で当初計画していた期限がきたので，監査報告書の作成に移った。  ア　監査意見には、必ず監査証拠による裏付けが必要です。そのため、十分な調査を行った後、監査意見をまとめます。  ウ　システム監査人は直接改善命令を行うことはできません。調査終了後、改善勧告を行います。  エ　監査意見に必要な監査証拠を十分に得るまでは、監査報告書を作成できません。  基本情報　平成30年度春　問58　[出題頻度：★★★]  解答－イ |

別冊演習ドリル 》 2-89～92

#### ③改善提案のフォローアップ（改善指導）

システム監査人は、監査報告書に改善提案を記載した場合、監査の依頼者の要請に応じて改善指導を行います。また、その改善措置が適切に実施されているか確認するために、改善計画及びその実施状況に関する情報を収集し、改善状況をモニタリングしなければなりません。

|  |
| --- |
| 例題  システム監査報告書に記載された改善勧告への取組みに対する監査人のフォローアップとして，適切なものはどれか。  ア　改善勧告に対する改善の実施を被監査部門の長に指示する。  イ　改善勧告に対する被監査部門の改善実施状況を確認する。  ウ　改善勧告に対する被監査部門の改善実施プロジェクトの管理を行う。  エ　改善勧告の内容を被監査部門に示した上で改善実施計画を策定する。  ア、エ　システム監査の依頼者が行います。  ウ　改善勧告を受けた被監査部門の長が行います。  応用情報　平成28年度秋　問59　[出題頻度：★★☆]  解答－イ |

別冊演習ドリル 》 2-93,94

🏋プラスアルファ

**8. システム監査の体制整備**

システム監査基準（平成30年）の「基準３　システム監査に対するニーズの把握と品質の確保」には、「システム監査の実施に際し、システム監査に対するニーズを十分に把握したうえでシステム監査を行い、システム監査の品質が確保されるための体制を整備しなければならない。」と記述されています。また、＜解釈指針＞には、「システム監査を外部の専門事業者に委託して実施する場合にも、委託先における監査の品質管理体制を確かめておくことが必要である。」と記述されています。

## 9. その他のシステム関連の監査

### １）情報セキュリティ監査

情報セキュリティ監査は、組織体の情報セキュリティに特化した監査です。

情報セキュリティ監査基準では、「情報セキュリティ監査の目的は、情報セキュリティに係わるリスクのマネジメントが効果的に実施されるように、リスクアセスメントに基づく適切なコントロールの整備、運用状況を、情報セキュリティ監査人が独立かつ専門的な立場から検証又は評価して、もって保証を与えあるいは助言を行うことにある。」と定義しています。

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に、**情報セキュリティ監査基準**があります。また、システム監査と同様、監査の判断基準として、**情報セキュリティ管理基準**があります。

情報セキュリティ監査基準は、組織体の内部監査部門等が実施する情報セキュリティ監査だけでなく、組織体の外部者に監査を依頼する情報セキュリティ監査においても利用できます。さらにこの基準は、情報セキュリティに保証を付与することを目的とした監査であっても、情報セキュリティの欠陥に対して助言を行うことを目的とした監査であっても利用できます。

情報セキュリティ監査は、情報セキュリティに係るマネジメントまたはコントロールを対象として行われるものですが、具体的に設定される監査の目的と監査の対象は監査依頼者の要請に応じたものでなければなりません。

|  |
| --- |
| 例題  情報セキュリティに係るリスクマネジメントが効果的に実施されるよう，リスクアセスメントに基づいた適切なコントロールの整備，運用状況を検証又は評価し，保証又は助言を与えるものであり，実施者に独立かつ専門的な立場が求められるものはどれか。  ア　コントロールセルフアセスメント（CSA） イ　情報セキュリティ監査  ウ　情報セキュリティ対策ベンチマーク エ　ディジタルフォレンジックス  ア　コントロール・セルフ・アセスメント（CSA：自己統制評価）は、業務担当者や業務責任者が自らリスクマネジメントや内部統制の有効性の評価を行うことです。  ウ　情報セキュリティ対策ベンチマークは、企業における情報セキュリティに係る対策や適正を考える水準についての目安となる指標です。セルフチェックツールとして、IPAがWeb上に評価項目を公開しています。  エ　ディジタルフォレンジックスは、不正アクセスなどコンピュータに関する犯罪の法的な証拠性を明らかにするために、原因究明に必要な情報を収集保全して分析することです。  情報セキュリティマネジメント　平成28年度春　問3　[出題頻度：★☆☆]  解答－イ |

別冊演習ドリル 》 2-95～97

# 2. 内部統制

学習のポイント

✅ 例題や演習ドリルの問題を参考に、過去の出題論点を確認しよう！

## 1. 内部統制

内部統制は、企業が継続していくためには欠かせない仕組みであり、経営者にはその仕組みを構築し、整備・運用する責任があります。

2007年2月15日に企業会計審議会が公表した「財務報告に係る内部統制の評価及び監査の基準」は、1992年に米国トレッドウェイ委員会組織委員会が公表した内部統制の統合的枠組みである**COSO**（the Committee of Sponsoring Organization of the Treadway Commission：コーソー）を下敷きに、日本の実情を加味して作られています。

ここでは、内部統制は次のように定義されています。

「内部統制とは、基本的に、業務の有効性及び効率性、財務報告の信頼性、事業活動に関わる法令等の遵守並びに資産の保全の４つの目的が達成されているとの合理的な保証を得るために、業務に組み込まれ、組織内の全ての者によって遂行されるプロセスをいい、統制環境、リスクの評価と対応、統制活動、情報と伝達、モニタリング（監視活動）及びIT（情報技術）への対応の６つの基本的要素から構成される。」

### １）内部統制の４つの目的

#### ①業務の有効性及び効率性

事業活動の目的の達成のため、業務の有効性及び効率性を高めること

#### ②財務報告の信頼性

財務諸表及び財務諸表に重要な影響を及ぼす可能性のある情報の信頼性を確保すること

#### ③事業活動に関わる法令等の遵守

事業活動に関わる法令その他の規範の遵守を促進すること

#### ④資産の保全

資産の取得、使用及び処分が正当な手続及び承認の下に行われるよう、資産の保全を図ること

なお、内部統制の目的はそれぞれに独立していますが、相互に関連しています。

### ２）内部統制を構成する６つの基本的要素

#### ①統制環境

統制環境とは、組織の気風を決定し、組織内の全ての者の統制に対する意識に影響を与えるとともに、他の基本的要素の基礎となって、他の５つの基本的要素に影響を及ぼす基盤をいいます。

統制環境としては、例えば、次の事項が挙げられます。

・誠実性及び倫理観

・経営者の意向及び姿勢

・経営方針及び経営戦略

・取締役会及び監査役又は監査委員会の有する機能

・組織構造及び慣行

・権限及び職責

・人的資源に対する方針と管理

#### ②リスクの評価と対応

リスクの評価と対応とは、組織目標の達成を阻害する要因をリスクとして識別、分析及び評価し、適切な対応を行う一連のプロセスをいいます。

#### ③統制活動

統制活動とは、経営者の命令及び指示が適切に実行されることを確保するために定める方針及び手続のことです。その中には、権限及び職責の付与、職務分掌等の広範な方針及び手続が含まれます。なお**職務分掌**とは、仕事の役割分担や仕事の権限を明確にすることで、内部統制を考慮した場合には、業務を遂行する上で違法行為や不正、ミスやエラーなどを防止し、組織が健全かつ有効・効率的に運営されるように基準や業務手続を定め、管理・監視が可能なことが前提となります。

#### ④情報と伝達

情報と伝達とは、必要な情報が識別、把握及び処理され、組織内外及び関係者相互に正しく伝えられることを確保することをいいます。

#### ⑤モニタリング

モニタリングとは、内部統制が有効に機能していることを継続的に評価するプロセスをいいます。

#### ⑥ITへの対応

ITへの対応とは、組織目標を達成するために予め適切な方針及び手続を定め、それを踏まえて、業務の実施において組織の内外のITに対し適切に対応することをいいます。特に組織の業務内容がITに大きく依存している場合や組織の情報システムがITを高度に取り入れている場合等には、内部統制の目的を達成するために不可欠の要素として、内部統制の有効性に係る判断の規準となります。

なおITへの対応は、IT環境への対応とITの利用及びITの統制から構成されています。そしてITの統制は、業務処理統制が有効に機能する環境を保証するための統制活動である**IT全般統制**と、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に業務プロセスに組み込まれた統制活動である**IT業務処理統制**の２つから構成されています。

|  |
| --- |
| 例題  内部統制に関する記述として，適切なものはどれか。  ア　内部監査人は，経営者による内部統制の整備や運用に対して監督責任を持つ。  イ　内部統制に関するリスクは，発生頻度ではなく発生した場合の財務情報への影響度で評価する。  ウ　内部統制の評価法として，業務実施部門がチェックリストで自らの業務ルールどおりに行われているかを評価する独立的モニタリングがある。  エ　内部統制は，経営者が組織目的の達成について合理的な保証を得るためのマネジメントプロセスである。  ア　内部監査人には、経営者を監督することはできません。  イ　内部統制に関するリスクは、組織目標に与える影響度で評価します。  ウ　問題文の記述は「独立的モニタリング」ではなく、「日常的モニタリング」です。「独立的モニタリング」は、業務実施部門から独立した監査人などが評価するモニタリングです。  ITパスポート　平成21年度秋　問49　[出題頻度：★☆☆]  解答－エ |

別冊演習ドリル 》 2-98～102

### ３）内部統制の限界

内部統制は、次のような固有の限界があります。

①判断の誤り、不注意、複数の担当者による共謀によって有効に機能しなくなる場合がある

②当初想定していなかった組織内外の環境の変化や非定型的な取引等には、必ずしも対応しない場合がある

③整備及び運用に際しては、費用と便益との比較衡量が求められる

④経営者が不当な目的の為に内部統制を無視ないし無効ならしめることがある

|  |
| --- |
| 例題  内部統制が有する固有の限界を示すものはどれか。  ア　経営者による不正を発見する機能をもっていない。  イ　担当者の権限逸脱を発見できない。  ウ　特定者への権限集中に起因した不正を防止できない。  エ　リスク認識に基づく合理的な安全対策がなされない。  内部統制のプロセスを整備するのは経営者なので、経営者による不正は発見できません。  イ　職務分掌を明確にすることによって、権限逸脱を発見できます。  ウ　担当者の権限を社内規定等で明確にすることによって、権限の集中を防ぎ、権限集中に起因する不正を防止できます。  エ　内部統制ではリスクの評価と対応を行うので、合理的な安全対策が可能です。  ソフトウェア開発　平成19年度秋　問77　[出題頻度：★☆☆]  解答－ア |

別冊演習ドリル 》 2-103

🏋プラスアルファ

**●ITガバナンス**

ITガバナンスは、システム監査で確認したとおり（P511参照）、経営陣がステークホルダのニーズに基づき、組織の価値を高めるために実践する行動であり、情報システムのあるべき姿を示す情報システム戦略の策定及び実現に必要となる組織能力です。

具体的には、システム管理基準（平成30年）の「システム管理基準の枠組み」の「１．ITガバナンスの定義」には、「ITガバナンスとは経営陣がステークホルダのニーズに基づき、組織の価値を高めるために実践する行動であり、情報システムのあるべき姿を示す情報システム戦略の策定及び実現に必要となる組織能力である。また、経営陣はITガバナンスを実践する上で、情報システムにまつわるリスク（以下「情報システムリスク」という。）だけでなく、予算や人材といった資源の配分や、情報システムから得られる効果の実現にも十分に留意する必要がある。」と記述されています。そして、「３.ITガバナンスにおける６つの原則」に、「ITガバナンスを成功に導くため、経営陣は、次の6つの原則を採用することが望ましい。」として、「①責任　役割に責任を負う人は、その役割を遂行する権限を持つ。」、「②戦略　情報システム戦略は、情報システムの現在及び将来の能力を考慮して策定し、現在及び将来のニーズを満たす必要がある。」、「③取得　情報システムの導入は、短期・長期の両面で効果、リスク、資源のバランスが取れた意思決定に基づく必要がある。」、「④パフォーマンス　情報システムは、現在及び将来のニーズを満たすサービスを提供する必要がある。」、「⑤適合　情報システムは、関連する全ての法律及び規制に適合する必要がある。」、「⑥人間行動　情報システムのパフォーマンスの維持に関わる人間の行動を尊重する必要がある。」と記述しています。

また、ITガバナンスに関する規格としてISO/IEC 38500を完全翻訳した**JIS Q 38500**：2015（情報技術－ITガバナンス）の、「２　用語及び定義」の「2.3 ITガバナンス（corporate governance of IT）」には、「組織のITの現在及び将来の利用を指示し、管理するシステム。ITガバナンスは、組織を支援するためにITの利用を評価すること及び指示すること、並びに計画を遂行するためにこのIT利用をモニタすることに関係する。これには組織におけるITの利用に関する戦略及び方針を含む。」と記述されています。