IT資格道場

CISA 学習用テキスト

予備知識ゼロから合格ラインへ —— 読んで理解する1冊目

無料サンプル(第1章まで)

CISA 試験範囲(ISACA 公式 CISA Examination Content Outline・2024年8月発効)準拠
2026年10月版

SAMPLE

ご利用にあたって

- このテキストは「IT資格道場」(www.shikaku-doujou.com)の購入者限定テキストのうち、学習用テキストの第1章までを収録した**無料サンプル**です。どなたでもご覧いただけます。
- 無料サンプルも著作物です。転載・改変しての再配布・二次販売はできません。
- AI モデルの学習データとしてのご利用(学習目的の入力・データセット化を含む)はできません。
- 製品版(学習用テキスト・頻出度別ノート・暗記用ノートの3点)は、ご購入者を識別できる透かし入りのPDFとして提供されます。
- 本PDFはスマートフォン・タブレットでの閲覧に合わせたA5版面・文字サイズで組版しています。

SAMPLE

目次

試験の骨組みと、このテキストの読み方 [0]

- 試験の基本情報
- 本番の出題形式
- 用語の表記

序章 監査の基本の考え方 [0]

- リスクの高いところから監査する
- 監査の結論は証拠で支える
- 独立性を守る
- 見つけたことは、決まった順で報告する
- 「最初に」「最も重要」「最も適切」を読み分ける

第1章 情報システム監査プロセス 18% [1.1.1/1.1.2/1.1.3/1.1.4/1.2.1/1.2.2/1.2.3/1.2.4/1.2.5/1.2.6]

- 1-1-1 情報システム監査基準、ガイドライン、機能、倫理規範 [1.1.1]
- 1-1-2 監査、評価、レビューの種類 [1.1.2]
- 1-1-3 リスクベースの監査計画 [1.1.3]
- 1-1-4 コントロールの種類と考慮事項 [1.1.4]
- 1-2-1 監査プロジェクト管理 [1.2.1]
- 1-2-2 監査テストおよびサンプリング方法 [1.2.2]
- 1-2-3 監査証拠の収集技法 [1.2.3]
- 1-2-4 監査データ分析（監査アルゴリズムを含む） [1.2.4]
- 1-2-5 報告およびコミュニケーションの手法 [1.2.5]
- 1-2-6 監査プロセスの品質保証と改善 [1.2.6]

サンプルはここまでです

SAMPLE

3 冊の使い方は、ダウンロード欄の案内を参照してください。

このテキストの骨組みは、ISACA 公開の **CISA Examination Content Outline（2024 年 8 月発効）** です[^guide]。日本語版の受験者ガイドの訳は「CISA試験内容の概要」です[^guideja]。以下、ECO と呼びます。ECO は試験の範囲を、5 つのドメインと 60 の細目で決めています。章と節の並びは ECO のままです。節見出しの末尾の `[1.1.1]` は細目の番号。公式番号「1A1」の A を 1、B を 2 に置き換えた形です。

ECO には細目とは別に、ドメインに紐づかない **補助タスク（Supporting Tasks）** が 43 項目あります[^guide]。補助タスクとは、IS 監査人が仕事で行うことの一覧。各節の冒頭に、その節で扱う補助タスクの番号を添えました。

CISA の問題の中心は、用語の暗記ではありません。「IS 監査人はこの場面で最初に何をするか」「最も適切なのはどれか」を問います。受験者ガイドによると、問題が測るのは実務の知識と、概念や基準を当てはめる力です[^guideja]。そのため各節は、次の 5 つの順で書きました。

1. 定義（その言葉が何を指すか）
2. なぜ監査で問われるか
3. 監査人が確かめること（何を見て、何を証拠にするか、どの順で進めるか）
4. よくある誤り（誤答になりやすい行動）
5. 関連する基準

SAMPLE

試験の骨組みと、このテキストの読み方 [0]

試験の基本情報

項目	内容
版	CISA Examination Content Outline（2024 年 8 月発効）[^guide]
問題数	**150 問**。採点されない事前テスト問題を含む。どれが事前テストかは不明[^guide]
試験時間	**240 分**（4 時間）[^guide]
形式	すべて **4 択**。最も適切な答えを 1 つ選ぶ。状況の記述を読んで 2 問以上に答える **シナリオ型** もある[^guideja]
採点	スケールスコア **200〜800 点、450 点以上で合格**。誤答による減点なし[^guide]
ドメインの比率	**1 情報システム監査プロセス 18%／2 IT のガバナンスと管理 18%／3 情報システムの取得、開発、実装 12%／4 情報システムの運用とビジネスの回復力 26%／5 情報資産の保護 26%**[^guide]
日本語	日本語で受験できる[^guide]
受験方法	PSI のテストセンター、またはリモート監督[^cert]
受験料	ISACA の認定ページでは、会員 575 米ドル、非会員 760 米ドル[^cert]
再受験	12 か月の間に最大 4 回。2 回目は初回から 30 日、3 回目と 4 回目は前回から 90 日空ける[^guide]

合格しただけでは CISA を名乗れません。合格から 5 年以内に、認定を申請します。申請には実務経験 5 年が必要。対象は情報システムの監査、コントロール、保証、セキュリティの実務。申請日から遡って 10 年以内のものです。学歴などで最大 3 年まで免除を受けられます[^app]。認定後は、CPE（継続的専門教育）を報告します。毎年 20 時間以上、3 年間で 120 時間以上。毎年の維持費も納めます。毎年、無作為に選ばれた人は CPE の証拠を提出します[^cpe]。

SAMPLE

本番の出題形式

受験者ガイドによる問題の形は、次のとおりです[^guideja]。

- どの問題にも、問題文と 4 つの選択肢がある
- 問題文は、疑問文か、文の穴埋め
- 正しい答え、または最も適切な答えを 1 つ選ぶ
- シナリオ型は、状況の説明を読み、その情報をもとに 2 問以上に答える

同じガイドの勧めは、修飾語への注意です。例は「MOST likely（最も可能性が高い）」「BEST（最も適切）」[^guideja]。選択肢に、正しい行動が 2 つ以上並ぶことは珍しくありません。その中から、修飾語が求める 1 つを選ぶ。これが CISA の問題の核心です。

用語の表記

日本語の用語は、2 つにそろえます。ISACA の CISA 用語集 日本語版（2022）[^term] と、受験者ガイド日本語版の訳[^guideja] です。原語は、初めて出る場所で一度だけ添えます。

このテキストの表記	原語
IS 監査人	IS auditor
監査憲章	audit charter
監査委員会	audit committee
監査証拠	audit evidence
監査リスク	audit risk
固有リスク	inherent risk
統制上のリスク	control risk
発見リスク	detection risk
重要性	materiality
準拠性テスト	compliance test
実証性テスト	substantive test
属性サンプリング	attribute sampling
変数サンプリング	variable sampling

SAMPLE

このテキストの表記	原語
発見抽出法	discovery sampling
コンピュータ支援監査技法（CAAT）	computer-assisted audit technique
予防的コントロール	preventive control
発見的コントロール	detective control
是正的コントロール	corrective control
補完的コントロール	compensating control
職務の分離	segregation of duties
合理的な保証	reasonable assurance
ビジネス・インパクト分析（BIA）	business impact analysis
目標復旧時間（RTO）	recovery time objective
目標復旧ポイント（RPO）	recovery point objective
データ所有者	data owner
データ管理者	data custodian
導入事後評価	post-implementation review
分析過程の保全管理（証拠保全の連鎖）	chain of custody

資格名の CISA は、米国の官庁名と同じ綴り。官庁名は Cybersecurity and Infrastructure Security Agency（サイバーセキュリティ・インフラストラクチャセキュリティ庁）。このテキストでは、略称の CISA を資格名以外に使いません。

SAMPLE

序章 監査の基本の考え方 [0]

CISA の問題の多くを解く鍵は、次の 5 つの考え方です。60 の細目に入る前に押さえます。

リスクの高いところから監査する

監査に使える人と時間は限られています。IS 監査人は、すべてを同じ深さでは調べません。リスクの高い領域を、先に深く調べます。ISACA の用語集の定義：リスク評価とは「リスクとその影響を特定し評価するプロセス」。用途は、IS の年間監査計画に入れる領域の選定です[^glossary]。

「監査計画を立てるとき最初に行うこと」の正解は、リスク評価か、対象の業務とシステムの理解である場面が多くあります。ただし、既にリスク評価が済んでいる場面では、次の段階が正解です。リスク評価には 2 つの段階があります。年間の監査計画のリスク評価は、どの領域を監査するかを選ぶためのもの。個々の監査を計画するときのリスク評価は、その業務のリスクを見つけて優先順位を付けるもの。目的と範囲を決めるために行います。IIA のグローバル内部監査基準も同じです。個々の業務のリスク評価をもとに、目的と範囲を決めます[^iia]。1-1-3 は、この考え方に沿った並びです。リスク評価、目的と範囲の決定、監査手続の設計の順になっています。場面の中で何が済んでいるかを、必ず数えます。

監査の結論は証拠で支える

監査の結論を決めるのは、IS 監査人の意見ではなく証拠です。証拠は **十分**（量が足りる）で、**適切**（質が高い）ことが条件です[^glossary]。信頼できる証拠は、次のとおりです。組織の外の独立した情報源から得た証拠。IS 監査人が直接得た証拠。担当者への質問（インタビュー）だけでは、コントロールが有効という結論を支えられません[^as1105]。

独立性を守る

IS 監査人は、監査の対象から独立している必要があります。用語集の定義は「利害の衝突や不当な影響から自由であること」[^glossary]。IS 監査人がコントロールを自分で設計し、導入し、運用したとします。後でそのコントロールを客観的には評価できません。助言はしますが、決めて実行するのは経営者です。

SAMPLE

見つけたことは、決まった順で報告する

発見事項は、まず監査対象の責任者と事実を確かめます。そのうえで報告書に載せます。報告書の内容は、発見事項、その影響、推奨事項、経営者の回答（対応計画）。報告の後は、対応が実際に行われたかをフォローアップで確かめます[^glossary]。経営者の代わりに直すことは、IS 監査人の仕事ではありません。

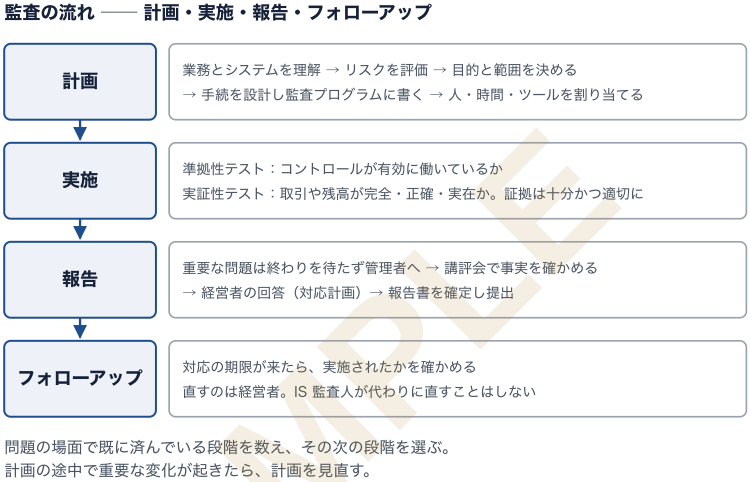


図 0-1　監査の流れ：計画・実施・報告・フォローアップ

「最初に」「最も重要」「最も適切」を読み分ける

CISA の問題文の末尾は、たいてい次の 4 つのどれかです。

問い方	選ぶもの
最初に行うべきことは	順番が一番早いもの。正しくても、後の段階の行動は誤り
最も重要なのは	影響が一番大きいもの。順番は問わない
最も適切なのは	場面の条件をすべて満たし、副作用が少ないもの
最も懸念すべきなのは	放置したときの損害が一番大きいもの

例：「バックアップの方針の監査で最初に行うこと」の正解は、方針の文書を読むこと。同じ場面の「最も重要なこと」なら、正解は復元テストの成功の確認。問い方が変わると、同じ選択肢

SAMPLE

の中で正解が入れ替わります。

各節の「監査人が確かめること」の番号は、項目の見分け用です。どの節でも確かめる順を表すわけではありません。順に意味がある節では、一覧の後に順序と理由を書きました。例は「1から順に確かめます」「最初に CPS を入手します」。順序を問われたら、その節の順序に従います。多くの場面で最初に来るのは、後の確認の土台になるものです。方針、計画、一覧、権限、手順や通知先の取り決めなどです。土台が無いと、設定や記録を調べても、良し悪しを決める物差しがありません。問題の場面で既に済んでいることがあれば、その次の段階に進みます。取り決めが既にある場面で、働いているかを問われたら、記録を抽出して取り決めと照らします。担当者への質問や手順書の閲覧は、働いていることの証拠になりません。

監査を始めるときの「最初に」は、次の一続きの順で考えます。1-1-1、1-1-2、1-1-3、1-2-1 の順を、一つにつなげました。

1. 監査の依頼を受け、自分の権限と独立性を確かめる（1-1-1）
2. 監査の目的と範囲を、依頼者と文書で合意する（1-1-2）
3. 対象の業務とシステムを理解する（1-1-3）
4. リスクを評価する（1-1-3）
5. 目的と範囲の案を確定し、監査手続を設計する（1-1-3）
6. 開始の会議で、監査対象の責任者と目的と範囲を合意する（1-2-1）
7. 作業を分け、担当と期限を決めて進める（1-2-1）

2 の合意は、依頼者との大枠の合意です。理解とリスク評価を経て、5 で細かく確定します。6 は、その案を監査対象の責任者と合意する段階。問題の場面がどこまで済んでいるかを数え、その次の段階を選びます。

SAMPLE

第1章 情報システム監査プロセス 18% [1.1.1/1.1.2/1.1.3/1.1.4/1.2.1/1.2.2/1.2.3/1.2.4/1.2.5/1.2.6]

この章の主題は、IS 監査そのものの進め方です。ECO の比率は 18%。A 計画（4 細目）と B 実施（6 細目）に分かれます。ほかの 4 章の問題も、この章の手順が土台です。

1-1-1 情報システム監査基準、ガイドライン、機能、倫理規範 [1.1.1]

関係する補助タスク：2（基準に従った監査の実施）、42（品質とコントロールを改善するための助言）

定義

IS 監査の「基準」とは、IS 監査人が必ず守る要求事項。ISACA は、IS 監査と保証の基準を **ITAF（IT Audit Framework）** にまとめました。ITAF は 2026 年 2 月に第 5 版が出ました。試験で問われるのは番号ではなく、区分と中身です。ITAF の内容は 3 つ。1 つ目は、基準。IS 監査人の役割と責任、倫理、職業上の行動、必要な知識と技能を定めます。2 つ目は、用語の定義。3 つ目は、計画、実施、報告の手引きです[^itaf]。ガイドラインとは、基準をどう満たすかの手引き。手順（procedure）ほど細かく縛りません[^glossary]。

IS 監査の「機能」とは、組織の中で監査を担う部門とその権限。内部監査部門の目的、権限、責任は **監査憲章（audit charter）** に書きます。用語集によると、監査憲章は、ガバナンスの責任者が承認する文書。責任者は取締役会や監査委員会です。監査部門の位置づけを決めます。監査に必要な記録、人、物理的な場所へのアクセスも認めます[^glossary]。

ISACA の職業倫理規定は、会員と認定保持者に 7 つの義務を課しています[^ethics]。主なものは次の 4 つです。

- 職業基準に従い、客観性、相当な注意、職業上の注意をもって職務を行う
- 業務で得た情報の機密を守る。法的な権限による開示の求めがある場合は除く
- 必要な技能と知識で完了できると合理的に見込める仕事だけを引き受ける
- 仕事の結果を関係者に伝える。伏せると結果をゆがめる重要な事実は、すべて開示する

ITAF の基準は 3 つの区分に分かれます。ISACA Journal の 2020 年の記事の説明は、次のとおりです[^isaca-std]。

SAMPLE

区分	扱うこと
一般基準	すべての業務に当てはまる指針。倫理、独立性、客観性、相当な注意、知識、能力、技能
実施基準	業務の進め方。計画と監督、範囲、リスクと重要性、資源の手配、証拠、職業上の判断と相当な注意
報告基準	報告書の種類、伝え方、伝える情報

同じ記事の内訳は、次のとおりです。一般基準の項目：監査憲章、組織上の独立性、監査人の客観性、合理的な期待、正当な職業上の注意、熟達、アサーション、規準。実施基準の項目：計画でのリスク評価、監査の日程、業務の計画、実施と監督、証拠、他の専門家の作業の利用、不正と違法行為。報告基準は、報告とフォローアップ活動です[^isaca-std]。

ガイドラインも、基準と同じ 3 つの区分で基準を支えます。その外側に「ツールと技法」があります。例はホワイトペーパー、監査プログラム、参考書、COBIT。基準は IT 監査の最低限の要求事項です。CISA の保持者が基準を守らないと、懲戒の対象になりえます。ISACA の理事会などが調査します[^isaca-std]。

なぜ監査で問われるか

監査の結論が信頼される条件は、基準に従い、独立した立場で出すことです。基準から外れた監査は、どれほど調べても結論の価値が下がります。そのため CISA では、独立性、職業上の注意、機密保持が場面の中で試されます。

監査人が確かめること

監査を始める前に、IS 監査人は自分の立場を確かめます。

1. 監査憲章に、今回の監査の権限とアクセスが書かれているか
2. 自分に利害の衝突がないか。IIA の基準は、以前に責任を持っていた業務の評価を控えるよう求める。過去 12 か月以内に責任を持った業務への保証業務は、客観性が損なわれたと推定する[^iia]
3. 必要な技能が自分やチームにあるか。無ければ専門家の力を借りるか

確かめる順は、この 3 つの順です。権限が無ければ、監査を始められません。権限があっても利害の衝突があれば、担当を決め直します。技能の手当ては、その後です。

SAMPLE

独立性が損なわれていると分かったら、黙って進めません。監査部門の責任者に伝えます。必要に応じて監査委員会にも伝えます。そのうえで、担当を替えるか、報告書にその事実を書きます。IIA のグローバル内部監査基準も、内部監査部門の長の機能上の報告先を取締役会とします。目的は、経営者から独立して動けるようにすることです[^iia]。

監査の途中で、以前に自分が責任を持った業務が範囲にあると気づく場合があります。このときも、まず監査部門の責任者に事実を伝えます。IIA の基準は、以前に責任を持っていた業務の評価を控えることを原則とします。そのうえで、責任を持ったのが直近 12 か月以内なら、客観性が損なわれたと推定します[^iia]。12 か月より前でも、評価してよいと自分で決めることはできません。担当を替えるかどうかは責任者が判断し、監査人はその判断に従います。次の行動は、いずれも取りません。自分の判断で手続を続ける。範囲から外す。監査対象の側に範囲を決め直してもらう。伝えずに手続を省く。

利害の衝突は、監査人の個人だけでなく、所属する事務所や監査部門の単位でも見ます。例：同じ事務所が設計と導入を請け負った対策がある。その事務所が監査すると、自分の仕事を自分で評価する形になります。導入の担当者と監査の担当者を分けても、この形は変わりません。引き渡しから間が空いていても、衝突が無い理由にはなりません。衝突を避けられないときは、引き受けを見直します。それでも引き受けるなら、ガバナンスの責任者に伝え、報告書にもその事実を書きます[^itaf]。

よくある誤り

IS 監査人がコントロールを自分で設計し、導入するのは誤りです。助言（補助タスク 42）はしてよい。ただし、決定と実行は経営者の責任です。監査人が担うと、独立性を失います。監査で知った顧客情報を、許可なく別の目的に使うのも誤り。業務で得た情報の機密を守ることは、倫理規定の義務だからです。経験の無い技術領域の監査を、専門家の支援なしに引き受けることもできません。倫理規定は、必要な技能と知識で完了できると見込める仕事だけを求めるからです。経営者から「この発見事項は報告書から外してほしい」と頼まれて外すのも誤り。重要な事実を伏せることは、倫理規定に反します。

関連する基準

- ISACA 職業倫理規定[^ethics]
- ITAF 第 5 版[^itaf]
- IIA グローバル内部監査基準[^iia]

SAMPLE

- ISACA Journal「Standards, Guidelines, Tools and Techniques」(2020 年 第 6 巻・第 4 版時点の記事) [^isaca-std]

1-1-2 監査、評価、レビューの種類 [1.1.2]

関係する補助タスク：1（監査の計画）

定義

IS 監査人が関わる仕事には、いくつかの種類があります。

種類	中身
財務監査	財務諸表の正しさを確かめる。IT はその裏づけのデータを作る仕組みとして調べる
業務監査	業務の手順とコントロールが有効か、効率的かを確かめる
統合監査	財務、業務、IT のコントロールをまとめて評価する
コンプライアンス監査	法令、規制、契約、社内規程を守っているかを確かめる
IS 監査	情報システムとそのコントロールを評価する
特別調査（フォレンジック）	不正や事故の疑いを調べ、法的に使える証拠を集める

保証（assurance）の業務には、2 つの形があります[^glossary]。**証明業務（attest engagement）**とは、経営者の主張を検証する業務。検証するのは IS 監査人です。主張の例は「当社のアクセス管理は有効である」です。**直接報告業務（direct reporting engagement）**とは、主張を使わない業務。IS 監査人が基準に照らして対象を直接評価し、結論を出します。

米国公認会計士協会（AICPA）の証明業務の基準にも、同じ区別があります。AT-C 205 の検証業務は、対象に責任を持つ当事者の主張が前提です。当事者は、業務を行う会計士とは別の人。SSAE 21 で新設の AT-C 206 では、直接の検証業務で会計士が責任者の主張を得ません。適切な規準に照らして、対象を自ら測定、評価します[^cpaj]。2 つを見分ける手がかりは、責任者の主張の有無です。

監査のほかに、**評価**（リスク評価、成熟度の評価など）と **レビュー** があります。レビューは、監査より範囲や手続が限られ、与える保証の水準も低い業務です。**コントロールの自己評価（CSA）**

SAMPLE

とは、経営者と職員が自分の領域のリスクとコントロールを評価する方法。監査人やリスク管理者が進行役になることがあります[^glossary]。

なぜ監査で問われるか

種類によって、目的、範囲、報告の相手、求める証拠が変わります。種類を取り違えると、集める証拠も報告の形も外れます。

監査人が確かめること

監査の依頼を受けたら、最初に目的と範囲を文書で合意します。外部の監査人なら、責任、権限、説明責任を **エンゲージメント・レター** に書きます[^glossary]。そのうえで、次を確かめます。

- 報告書を誰が読むか（経営者、監査委員会、規制当局、顧客）
- 求められる保証の水準（監査か、レビューか、助言か）
- 対象期間（ある時点か、一定の期間か）

この 3 つを確かめる理由は、それぞれで監査の中身が変わるからです。報告書の読み手で、報告の形が変わります。形とは、詳しさ、使う言葉、載せる内容です。保証の水準によって変わるのは、集める証拠の量と報告の書き方。対象期間でも、業務の中身が変わります。ある時点の状態を見るなら、設計と設定を確かめます。一定の期間の運用を見るなら、期間を通して働いたかをテストします。

CSA を導入している組織では、CSA の結果を監査の入力に使えます。ただし CSA は経営者の評価。IS 監査人は、結果をそのまま結論にしません。自分でテストして確かめます。CSA の評価と違う実際の状態が分かったら、その状態を発見事項として報告書に載せます。CSA の評価との差も示します。次の行動は、いずれも取りません。CSA の評価に合わせて結論を変える。運用されていなかった期間を黙って対象から外す。CSA の担当者に評価を直させ、それを証拠にする。

よくある誤り

CSA が監査を置き換えると考えるのは誤りです。CSA は監査を補うもので、独立した監査の代わりにはなりません。目的と範囲を合意しないまま、テストを始めるのも誤り。目的と範囲で、集める証拠も報告の形も変わるからです。助言の業務で、監査と同じ水準の保証を与える報告

SAMPLE

を書くのも誤りです。求められる保証の水準で、集める証拠の量と報告の書き方が変わるからです。

関連する基準

- ISACA 用語集[^glossary]
- The CPA Journal「Expanding Options for Providing Attestation Services」(AT-C 205・206 の説明) [^cpaj]

1-1-3 リスクベースの監査計画 [1.1.3]

関係する補助タスク：1（監査の計画）、2（リスクベースの監査戦略）

定義

リスクベースの監査計画とは、リスクの高い領域に監査の資源を多く割く計画の立て方。計画には 2 つの層があります。**年間（中長期）の監査計画** は、どの領域をいつ監査するかを決めます。選ぶ元は監査対象の一覧（**監査ユニバース**）です。用語集によると、監査ユニバースは監査の候補となる領域の一覧。年間の監査日程の元になり、全体のリスクの変化に合わせて見直します[^glossary]。**個別の監査の計画** は、1 件の監査の目的、範囲、手続の性質、時期、範囲（量）を決めます。用語集の定義：監査計画とは「十分で適切な監査証拠を得るために行う手続の性質、時期、範囲を含む計画」[^glossary]。

計画の土台は **監査リスク** です。監査リスクとは「監査の発見事項から誤った結論に達するリスク」。固有リスク、統制上のリスク、発見リスクの 3 つからなります[^glossary]。

リスク	意味	誰が左右するか
固有リスク	コントロールが無いとしたときのリスク	対象の性質で決まる
統制上のリスク	誤りや不正を組織のコントロールが防げない、見つけられないリスク	組織のコントロールの設計と運用で決まる
発見リスク	監査人の手続が、存在する誤りを見つけられないリスク	監査人が手続の性質、時期、範囲で下げる

PCAOB の監査基準 AS 1101 の定めは、次のとおりです。固有リスクと統制上のリスクが高いほど、許せる発見リスクを低くします。発見リスクを下げるには、実証的な手続を増やします

SAMPLE

[^as1101]。逆に、この 2 つのリスクが低いと評価できれば、許せる発見リスクは比較的高くできます。そのぶん実証的な手続を少なくできます。

AS 1101 では、監査リスクは「重要な虚偽表示のリスク」と「発見リスク」の関数です[^as1101]。重要な虚偽表示のリスクは、2 つの水準で評価します。財務諸表全体の水準と、個々のアサーションの水準です。アサーションの水準の重要な虚偽表示のリスクは、固有リスクと統制上のリスクの組です。統制上のリスクを決めるのは、内部統制の設計と運用の有効さ。固有リスクと統制上のリスクは、組織とその環境の側にあります。監査人は、集めた証拠でそれを評価します。コントロールのテストの証拠が無いと、統制上のリスクは最大より低く評価できません。発見リスクを左右するのは、実証手続の有効性と、相当な注意をもって行われたかです。

計画の手順に置き直すと、次の 3 段になります[^as1101]。

1. 固有リスクと統制上のリスクを評価し、重要な虚偽表示のリスクを見積もる
2. 重要な虚偽表示のリスクが高いほど、許せる発見リスクを低く決める
3. 許せる発見リスクが低いほど、実証手続の性質、時期、範囲を変え、得る証拠を増やす

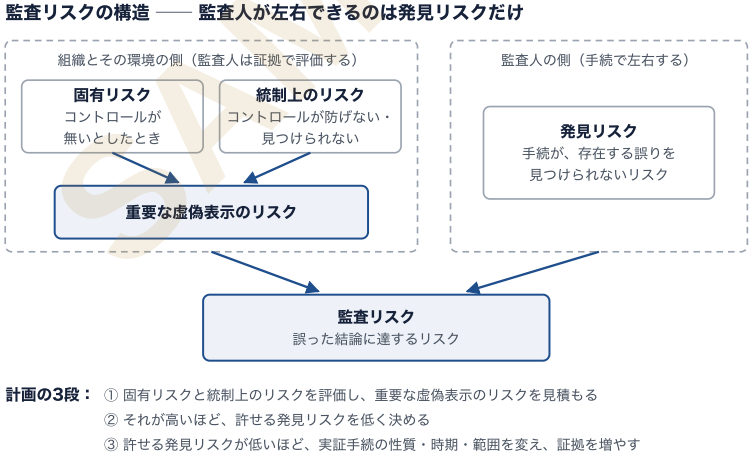


図 1-1　監査リスクの構造：監査人が左右できるのは発見リスクだけ

SAMPLE

なぜ監査で問われるか

監査人が左右できるのは、発見リスクだけです。固有リスクと統制上のリスクの評価が高ければ、発見リスクを下げます。方法は、サンプルを増やす、より信頼できる手続を選ぶ、など。この関係が、計画の多くの判断を決めます。

監査人が確かめること

個別の監査を計画する順番は、おおむね次のとおりです。

1. 対象の業務、システム、組織の目標を理解する（読むもの：過去の監査報告書、組織図、方針、システム構成図）
2. リスクを評価する（固有リスクと統制上のリスクを見積もる）
3. 監査の目的と範囲を決める
4. 監査手続を設計し、監査プログラムに書く。監査プログラムとは、監査を終えるための手続と指示を段階ごとに書いたもの[^glossary]
5. 人、時間、ツールを割り当てる

計画の途中で重要な変化が起きたら、見直します。例はシステムの入れ替えや事故の発生です。計画は、一度決めたら動かさないものではありません。

よくある誤り

業務とシステムを理解する前に、テスト項目を決めるのは誤りです。計画の順は、対象の理解、リスク評価、目的と範囲の決定、手続の設計だからです。前年と同じ計画をそのまま使い、リスクの変化を反映しないのも誤り。計画は、一度決めたら動かさないものではありません。固有リスクが高い領域で、サンプルを減らして時間を節約するのも誤りです。この 2 つが高いほど、許せる発見リスクを低くし、実証的な手続を増やすからです。発見リスクを組織のコントロールで下げるものだと考えるのも誤り。発見リスクは監査人の手続で下げるものです。監査人が左右できるのは、このリスクだけです。

関連する基準

- PCAOB AS 1101 監査リスク[^as1101]
- ISACA 用語集[^glossary]

SAMPLE

1-1-4 コントロールの種類と考慮事項 [1.1.4]

関係する補助タスク：2（基準に従った監査の実施）、40（論理的、物理的、環境的コントロールの評価）

定義

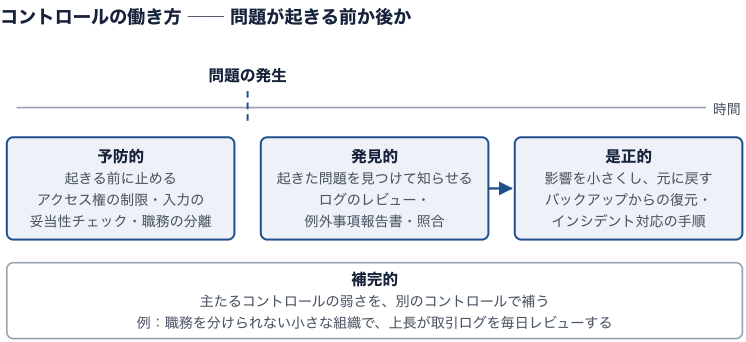
コントロールとは、目標の達成を妨げるリスクを抑える仕組み。働き方で次のように分けます[^glossary]。

種類	働き	例
予防的	問題が起きる前に止める	アクセス権の制限、入力の妥当性チェック、職務の分離
発見的	起きた問題を見つけて知らせる	ログのレビュー、例外事項報告書、照合
是正的	見つけた問題の影響を小さくし、元に戻す	バックアップからの復元、インシデント対応の手順
補完的	主たるコントロールの弱さを別のコントロールで補う	小さな組織で職務を分けられないとき、上長が取引ログを毎日レビューする

用語集の定義：補完的コントロールとは「既存の、または潜在的なコントロールの弱さが誤りや漏れにつながるリスクを小さくする内部コントロール」[^glossary]。

実装の形でも分けます。**管理的**（方針、手順、教育）。**技術的**（論理的：認証、暗号化、ファイアウォール）。**物理的**（錠、入退室管理、監視カメラ）。範囲でも分けます。**IT 全般統制（ITGC）** は、多くのシステムに共通する土台のコントロール。例はアクセス管理、変更管理、運用管理。**アプリケーション・コントロール** は、個々のアプリの入力、処理、出力を守るコントロールです。

SAMPLE



実装の形では、管理的（方針・手順・教育）、技術的（認証・暗号化）、物理的（錠・入退室管理）に分ける。

図 1-2　コントロールの働き方：問題が起きる前か後か

職務の分離 とは、取引の起票、記録、資産の保管を別の人に割り当てる仕組み。誤りや不正を防ぐ、または見つける基本のコントロールです[^glossary]。

内部統制の枠組みで広く使われるのは、COSO の「内部統制の統合的枠組み」。構成要素は 5 つ。統制環境、リスク評価、統制活動、情報と伝達、モニタリング活動です[^coso]。

COSO の枠組みの要約（2013 年 5 月）は、5 つの構成要素を次のように説明します[^coso-es]。

構成要素	中身
統制環境	組織全体で内部統制を行う土台となる基準、プロセス、構造。取締役会と上級経営者が、内部統制の大切さと期待する行動の基準を示す（トップの姿勢）。含むもの：誠実性と倫理観、取締役会の監督、組織構造と権限と責任、有能な人材の確保と育成、業績の評価と報酬。内部統制の全体に広く影響する
リスク評価	目標の達成を妨げるリスクを特定し評価する、動的で繰り返しのプロセス。リスクの許容度に照らして考え、リスクをどう管理するかを決める土台になる。前提として、目標がはっきり決まっている必要がある

SAMPLE

構成要素	中身
統制活動	方針と手順で定め、リスクを抑える経営者の指示が実行されるようにする行動。組織のすべての階層、業務プロセスの各段階、技術の環境で行う。予防的なものも発見的なものもあり、承認、検証、照合、業績のレビューなどを含む。職務の分離ができないときは、経営者が代わりの統制活動を選ぶ
情報と伝達	内部統制に必要な、関連のある質の高い情報を社内外から得て使う。組織の上下と横に伝え、外部の関係者とも必要な情報をやり取りする
モニタリング活動	日常的評価、独立的評価、またはその組み合わせで、5つの構成要素の存在と機能を確かめる。不備は経営者と取締役会に適宜伝える

目標は 3 つに分かれます。業務（有効性と効率性、資産の保全）。報告（財務と非財務、社内と社外）。コンプライアンス（法令の遵守）。5 つの構成要素の下には 17 の原則があります。例：統制活動の原則には、技術に関する全般的な統制活動を選んで整えることがあります[^coso-es]。

内部統制が有効といえる条件は、2 つです。5 つの構成要素とそれに関わる原則がすべて「存在し」「機能し」ていること。5 つが一体となって働いていること。どれかに重大な不備があれば、有効とは結論できません。有効な内部統制でも、与えるのは合理的な保証です。限界は 4 つ。判断の誤り、単純な人の誤り、経営者による内部統制の無視、共謀による回避です[^coso-es]。

SAMPLE

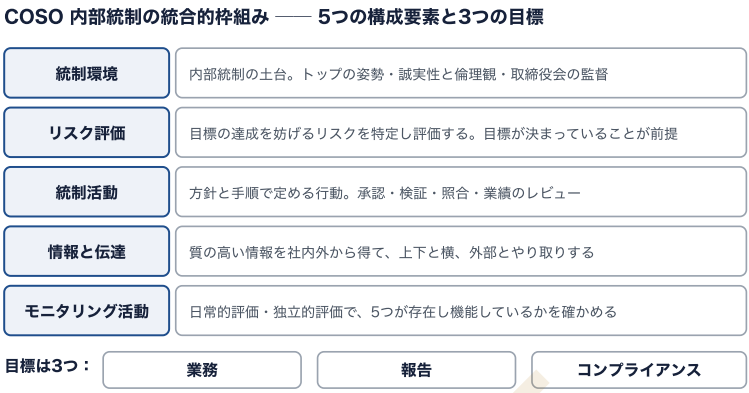


図 1-3　COSO 内部統制の統合的枠組み：5つの構成要素と3つの目標

なぜ監査で問われるか

コントロールは、100% の保証を与えません。与えるのは **合理的な保証** です。用語集の定義は「保証には届かないが、コントロールの費用と見込まれる効果に照らして十分とみなせる安心の水準」[^glossary]。そのため監査人が評価するのは、「完璧か」ではなく「リスクに見合っているか」です。

監査人が確かめること

1. リスクに対して、どのコントロールが置かれているかを特定する
2. **設計** が有効か（正しく働けばリスクを抑えられるか）を評価する
3. 設計が有効なら、**運用** が有効か（対象期間中、決めたとおりに働いたか）をテストする
4. 弱さが見つかったら、補完的コントロールがリスクを十分に抑えているかを評価する

設計が有効でないコントロールの運用をテストしても、意味がありません。設計の評価が先です。

よくある誤り

予防的コントロールがあれば発見的コントロールは要らない、と考えるのは誤りです。予防は破られうるので、発見と組み合わせるからです。補完的コントロールを確かめずに、職務の分離

SAMPLE

の欠如を重大な欠陥と結論づけるのも誤り。主たるコントロールの弱さは、別のコントロールで補われていることがあります。それを確かめる前に、結論は出せません。方針の文書があることを、コントロールが運用されている証拠とみなすのも誤りです。対象期間中に決めたとおりに働いたかは、運用のテストでしか分かりません。

関連する基準

- COSO 内部統制の統合的枠組み[^coso]
- ISACA 用語集[^glossary]
- NIST SP 800-53 第 5 版[^sp800-53]
- COSO 内部統制の統合的枠組み 要約（2013 年 5 月）[^coso-es]

1-2-1 監査プロジェクト管理 [1.2.1]

関係する補助タスク：3（監査にプロジェクト管理の手法を使う）

定義

個々の監査は、目的・期限・予算・要員を持つ一つのプロジェクトです。

監査のプロジェクト管理とは、計画・実施・報告を終える管理。範囲と品質は決めたまま、期限と予算の中で終える。

用語集が挙げる監査計画の中身は、次の 7 つです[^glossary]。

- 監査する領域
- 作業の種類
- 目的と範囲
- 予算
- 要員の割り当て
- 日程
- 報告書の種類と読み手

なぜ監査で問われるか

監査では、次の問題がよく起きます。

- 範囲が途中で広がる

SAMPLE

- 要員が足りない
- 監査対象の協力が得られない

対処の仕方で、監査の品質と独立性が変わります。

監査人が確かめること

監査の管理者（監査の責任者）の仕事は、次の 5 つです。

1. 目的と範囲の合意：開始の会議（キックオフ）で、監査対象の責任者と行う
2. 作業の分担：担当者に割り当て、期限を決める
3. 進み具合の確認：計画と比べ、遅れの原因をつかむ
4. 上位者によるレビュー（監督）：担当者の作業と調書が対象
5. 早めの報告：問題は、監査部門の責任者へ

1 から 4 は、監査が進む順に並んでいます。理由は次のとおりです。

- 目的と範囲が決まらないと、作業を分けられない。
- 作業と期限が決まらないと、進み具合を計画と比べられない。
- 調書は、作業の後にできる。

目的と範囲を開始の会議で合意し、記録に残す理由は、後の食い違いへの備えです。範囲や資料の求めをめぐって食い違ったとき、合意した内容を拠り所にします。

- 重要な変化があれば、範囲を見直すことはあります（1-1-3）。
- 合意は、監査人が監査対象の業務を代わりに行う根拠になりません。
- 合意は、監査対象が発見事項の中身を決める根拠にもなりません。

監査の途中で範囲外の重要なリスクに気づいたときの対応：

- 黙って範囲を広げない。
- 監査部門の責任者と相談する。
- 範囲を変えるか、別の監査として計画する。

監査対象が資料の提出を拒み、範囲が制限されたときの対応：

- 制限を記録する。

SAMPLE

- 監査部門の責任者と監査委員会に伝える。
- 範囲の制限は報告書にも記載する。

監査の管理者は、途中で次の 3 つの数字を見ます。

- 計画した時間と実際の時間の差
- 終わった手続の割合
- 未解決の質問の数

3 つの数字は、組み合わせて見ます。終わった手続の割合が計画どおりでも、未解決の質問が急に増えたら要注意。後の手続が止まる兆し。割合だけでは、順調と判断できません。質問が増えた原因をつかみます。

差が大きい作業は、原因を分けて考えます。

- 監査対象の資料の遅れ：監査対象の責任者に期限を伝える。
- 監査人の技能の不足：担当を替えるか、専門家を加える。

監査の予算（時間）を超えそうなときも、手続の質を落として帳尻を合わせません。範囲や期限の見直しを、監査部門の責任者に承認してもらいます。

よくある誤り

誤りは次の 4 つです。

- 期限を守るために、計画した手続を黙って省く。予算を超えそうなときも、手続の質は落としません。
- 範囲外の問題を、合意なしに調べ始める。範囲外の重要なリスクに気づいたら、監査部門の責任者と相談します。範囲を変えるか、別の監査として計画します。黙って範囲を広げることはしません。
- 資料の提出を拒まれ、別の担当者の説明だけで済ませる。範囲が制限されたら、制限を記録する。監査部門の責任者と監査委員会に伝え、報告書にも記載します。
- 若手の作業を上位者がレビューしないまま、報告書を書く。監督は、監査の管理者の仕事です。

関連する基準

- ISACA 用語集[^glossary]

SAMPLE

- IIA グローバル内部監査基準（業務の監督）[^iia]

1-2-2 監査テストおよびサンプリング方法 [1.2.2]

関係する補助タスク：2（基準に従った監査の実施）

定義

監査のテストは 2 種類です[^glossary]。

テスト	得る証拠	例
準拠性テスト（compliance test）	コントロールが有効に働いているかの証拠	変更の申請書に承認の署名があるかを、抽出して調べる
実証性テスト（substantive test）	取引や残高の完全性・正確性・実在性の証拠	本番のプログラムと承認された版を比べる。取引を再計算する

- 準拠性テストでコントロールが有効と分かれば、実証性テストを減らせます。
- コントロールが弱ければ、実証性テストを増やします。

監査サンプリングとは、母集団の 100% 未満の項目に手続を当てること[^glossary]。目的は、母集団の特徴についての証拠を得ること。主な方法は次のとおりです。

方法	中身
統計的サンプリング	数学と確率で抽出し、母集団について数学的に根拠のある推論をする[^glossary]
非統計的サンプリング	経験と判断で抽出する。母集団全体について数学的な結論は出せない[^glossary]
属性サンプリング	ある特徴が「あるか無いか」で見る。準拠性テストで逸脱の率を見るのに使う[^glossary]
変数サンプリング	金額などの量を推定する。実証性テストで使う[^glossary]
発見抽出法	属性サンプリングの一種。母集団に 1 件でも事象があれば、決めた確率で見つける[^glossary]
層化	母集団を性質の近いグループに分けて抽出する。必要なサンプル数を減らせる[^as2315]

SAMPLE

なぜ監査で問われるか

サンプルには、2 つのリスクがあります。

- **サンプリングリスク**とは、選んだ項目が母集団を代表しないリスク[^glossary]。同じ設計ならサンプルが小さいほど、大きくなります。出典は PCAOB の AS 2315[^as2315]。
- **ノンサンプリングリスク**とは、サンプリングと関係なく誤るリスク。例は、目的に合わない手続を選ぶ、調べた書類の誤りを見落とす、など[^as2315]。

監査人が確かめること

サンプルの大きさを決める要素は 4 つ。許容誤謬、予想される誤りの率、信頼度、ほかの証拠の有無です[^as2315][^glossary]。

要素	意味	サンプルとの関係
許容誤謬（許容逸脱率）	母集団の中で許せる最大の誤り。準拠性テストでは、許せる逸脱の最大の率	大きいほど、サンプルは小さくて済む
予想される誤りの率	母集団にありそうな誤りの率	大きいほど、サンプルは大きくなる
信頼度	許せるサンプリングリスクの裏返し	高い信頼度を求めるほど、サンプルは大きくなる
ほかの証拠	同じ目的の別の手続による証拠	別の手続が無く、固有リスクと統制上のリスクが最大。ほかの証拠が無いので、サンプルを大きくする

サンプルは、母集団のすべての項目に選ばれる機会があるように選びます[^as2315]。

- サンプルの逸脱率が許容逸脱率を下回っても、差が小さいと注意が要ります。母集団では許容を超えているおそれが残るからです。
- AS 2315 の例：許容逸脱率 5%、サンプル 60 件。逸脱が 0 件なら、サンプリングリスクは許せる程度に低いと結論できます。
- 同じ例で 2 件以上の逸脱があれば、リスクは許せないほど高いとしています[^as2315]。

よくある誤り

誤りは次の 4 つです。

SAMPLE

- 準拠性テストで「金額」を推定しようとする。準拠性テストは属性（あるか無いか）を見るもの。金額などの量は、変数サンプリングを使う実証性テストで推定します。
- 母集団の一部（たとえば最初の 1 か月分だけ）から抽出し、全期間の結論を出す。一部だけから選んだサンプルには、すべての項目に選ばれる機会がありません。
- 逸脱が見つかったのに、サンプルを増やさず、原因も調べずに「有効」と結論づける。逸脱の原因と広がりを調べないと、母集団でどれだけ起きているか分かりません。
- 全件を機械で調べられるのに、手作業のサンプリングにこだわる。全件を調べれば、サンプリングリスクはなくなります（1-2-4）。

関連する基準

- PCAOB AS 2315 監査サンプリング[^as2315]
- ISACA 用語集[^glossary]

1-2-3 監査証拠の収集技法 [1.2.3]

関係する補助タスク：2（基準に従った監査の実施）

定義

監査証拠とは、監査の意見を支える情報[^glossary]。証拠には量と質の条件があります。

- **十分性**：証拠の量の尺度。監査の目的と範囲にかかわる重要な問いをすべて支えられること[^glossary]
- **適切性**：証拠の質の尺度[^glossary]。質は、関連性と信頼性で決まる
- **関連性**：監査の目的と論理的につながり、発見事項と結論を支えること[^glossary]
- **信頼性**：正しく、事実に基づき、客観的で、裏づけられること[^glossary]

証拠を集める技法は次のとおりです[^as1105]。

技法	中身
閲覧（inspection）	文書や記録を調べる。資産を実際に見て調べる
観察（observation）	担当者が手順を行う様子を見る
質問（inquiry）	知っている人に聞く。書面でも口頭でもよい
確認（confirmation）	第三者から、監査人に直接、書面で回答を得る

SAMPLE

技法	中身
再計算（recalculation）	数字の正しさを計算し直して確かめる
再実施（reperformance）	組織が行った手続やコントロールを、監査人が自分で行う
分析的手続	データの間のもっともらしい関係を調べ、予想との大きな差を追う

ウォークスルーとは、システムの流れを確かめる手続。取引を発生から記録まで、組織が使うのと同じ書類とシステムでたどります[^as2201]。

なぜ監査で問われるか

証拠の強さの順を知っていると、「最も信頼できる証拠はどれか」が解けます。AS 1105 による強さの順は次のとおりです。

- 組織の外の独立した情報源の証拠は、組織の中だけの証拠より信頼できる。
- 組織が作った情報は、作る仕組み（IT 全般統制など）が有効なとき、より信頼できる。
- 監査人が直接得た証拠は、間接に得た証拠より信頼できる。
- 原本は、コピーより信頼できる[^as1105]。

観察と質問には、限界があります。

- 観察の証拠は、観察したその時点に限られる。
- 観察されていると分かると、人の行動が変わる[^as1105]。
- 質問だけでは、コントロールが有効だという結論を支えられない[^as1105]。

監査人が確かめること

1. 証拠の目的の決定：監査の目的に照らして、何を証明する証拠が要るかを決める
2. より信頼できる技法の選択：質問だけで済ませず、閲覧や再実施で裏づけます
3. 集めた証拠を **監査調書** に記録する。第三者の IS 監査人が同じ結論に達せるように書く。何を・いつ・誰から・どう得たかを記す。用語集の定義：十分な証拠とは「別の IS 監査人が同じ結論を出せる」もの[^glossary]
4. 電子的な証拠の保存：改ざんされていないことを確かめられる形で行う

SAMPLE

よくある誤り

誤りは次の 3 つです。

- システム管理者の説明（質問）だけで、アクセス制御が有効と結論づける。質問だけでは、コントロールが有効だという結論を支えられません。
- 監査対象が作って渡した一覧を、完全性を確かめずに母集団として使う。組織が作った情報は、それを作る仕組みが有効なときにだけ、より信頼できます。
- 1 回の観察で、1 年間の運用が有効だったと結論づける。観察の証拠は、観察したその時点に限られます。

関連する基準

- PCAOB AS 1105 監査証拠[^as1105]
- AS 2201（ウォークスルー）[^as2201]
- ISACA 用語集[^glossary]

1-2-4 監査データ分析（監査アルゴリズムを含む） [1.2.4]

関係する補助タスク：6（データ分析ツールで監査を強化する）、7（自動化と意思決定システムの役割と影響の評価）

定義

監査データ分析とは、組織のデータをツールで抽出・分析し、監査証拠を得る方法。ISACA の用語集が挙げる技法は、次のとおりです[^glossary]。

技法	中身
コンピュータ支援監査技法（CAAT）	自動化された監査技法の総称。汎用監査ソフト、テストデータの作成ツール、監査用のプログラムなど
汎用監査ソフト（GAS）	レコードの抽出・突き合わせ・再計算・報告に使える多目的のソフト
テストデータ	模擬の取引を流し、プログラムの処理・計算・コントロールを確かめる
統合テスト法（ITF）	本番システムの中に、架空の部門や顧客を作る。テストデータを本番と同時に処理させ、結果を確かめる

SAMPLE

技法	中身
並行シミュレーション	監査人が重要な処理を再現するプログラムを書く。本番のデータを処理し直し、結果を比べる
組み込み監査モジュール（EAM）	アプリケーションに組み込み、決めた条件に合う取引をリアルタイムで拾って報告する
継続的監査	コンピュータを通じて、システムの信頼性を継続的に監視し、証拠を集める

監査アルゴリズムとは、母集団の全件に同じ判定の規則を当てるプログラム。規則の例は次のとおりです。

- 同じ請求書番号と金額の支払を、二重払いの候補として拾う
- 職務の分離に反する権限の組み合わせを持つ利用者を拾う

なぜ監査で問われるか

データ分析を使うと、サンプルでなく全件を調べられます。サンプリングリスクはなくなります。ただし、分析の結果が正しいのは、入力のデータが完全で正確なときだけです。

組織の業務でも、自動化や AI による意思決定が増えています（補助タスク 7）。NIST に AI リスクマネジメント・フレームワークがあります。AI のリスク管理を 4 つの機能で整理しています[^airmf]。

- 統治（Govern）
- 把握（Map）
- 測定（Measure）
- 管理（Manage）

IS 監査人は、自動の判断について次を確かめます。

- 誰が責任を持つか
- どう監視するか
- 誤りをどう直すか

監査人が確かめること

データ分析の手順は次のとおりです。

SAMPLE

1. 目的の決定とデータの特定：監査の目的を決め、どのデータが要るかを洗い出す
2. データの入手：持ち主の了解を得る。本番データを監査人が直接書き換えず、読み取り専用のコピーを使います
3. **データの完全性と正確性の確認**：件数や合計を、元のシステムの管理合計と照合する
4. 分析の規則（アルゴリズム）の検証：作ってテストし、意図どおりに動くことを確かめる
5. 例外の抽出：1 件ずつ原因を調べる。例外がそのまま誤りとは限りません

ITF を使うときは、後で取り消す手順を用意します。架空の取引を、本番の帳簿や報告に残さないためです。継続的監査が特に役立つのは、取引が多く、紙の証跡が残らないシステムです。

分析の途中でデータの誤り（明らかに誤った単価の登録など）を見つけたときの対応：

- 監査人は、本番のデータを直さない。
- 誤りの行を黙って外して、結論を出さない。
- 読み取り専用のコピーで分析を続ける。
- 見つけた誤りを記録し、発見事項の候補にする。

抽出した例外の扱いは、原因の調査結果で分かれます。

調査の結果	扱い
実際の誤り	原因とともに発見事項にする
正当な理由がある	発見事項にしない。ただし、理由と確かめた証拠を調書に記録する

記録の目的は、後から別の人が見ても、なぜ外したかが分かることです。

よくある誤り

誤りは次の 4 つです。

- 監査対象から受け取ったデータを、件数と合計の照合なしで分析する。入力のデータが完全で正確でなければ、分析の結果は正しくなりません。
- 抽出した例外を、すべて不正や誤りと報告する。例外がそのまま誤りとは限りません。1 件ずつ原因を調べてから、発見事項にするかを決めます。

SAMPLE

- 本番システムで、監査人が管理者権限を使って直接問い合わせる。本番のデータは書き換えず、読み取り専用のコピーで分析します。管理者権限で本番に直接触ることはしません。
- 分析のスクリプトを検証しないまま使い、結果を証拠にする。分析の規則は、テストして意図どおりに動くことを確かめてから使います。

関連する基準

- ISACA 用語集[^glossary]
- NIST AI RMF 1.0[^airmf]

1-2-5 報告およびコミュニケーションの手法 [1.2.5]

関係する補助タスク：4（関係者とのコミュニケーションとフィードバックの収集）、5（監査後のフォローアップ）

定義

監査の報告とは、監査の結論と発見事項を、読み手が行動できる形で伝えること。発見事項は、次の要素で書きます[^iia]。

要素	中身
基準（criteria）	あるべき姿。方針、規程、法令、契約など
状況（condition）	監査で分かった実際の状態
根本原因（root cause）	基準と状況の差が生まれた理由
影響（effect）	その差がもたらすリスクや損害

これに **推奨事項** と、**経営者の回答**（対応計画、責任者、期限）を添えます。IIA の基準によると、基準と状況の差が潜在的な発見事項です[^iia]。

SAMPLE

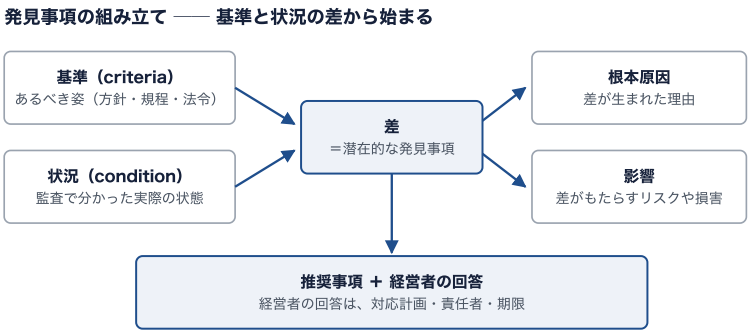


図 1-4　発見事項の組み立て：基準と状況の差から始まる

フォローアップとは、経営者が、欠陥を直す適切な是正措置を取ったかの確認[^glossary]。

なぜ監査で問われるか

報告の順番や相手を間違えると、2 つの問題が起きます。

- 事実の誤りが、報告書に残る。
- 関係者の協力を失う。

CISA では「報告書を出す前に何をするか」「誰に報告するか」がよく問われます。

監査人が確かめること

報告の流れは、おおむね次のとおりです。

1. 早めの伝達：テスト中の重要な問題は、監査の終わりを待たず、適切な管理者に伝える
2. **講評会（exit meeting）**：監査の終わりに、監査対象の責任者と開く。発見事項の事実に誤りがないかを確かめる
3. 経営者の回答（対応計画）の受領
4. 報告書の確定と提出：提出先は経営者。必要に応じて監査委員会にも出す
5. フォローアップ：対応の期限が来たら、実施を確かめる

経営者が発見事項に同意しないときの対応：

- 証拠を見直す。

SAMPLE

- 証拠が十分なら、発見事項を残す。
- 経営者の反対意見も、報告書に併記する。

経営者が推奨事項を実施しないと決めたときの対応：

- リスクの受け入れが、経営者の権限の範囲かを確かめる。
- 受け入れたリスクが組織の許容範囲を超えるなら、上位の経営者や監査委員会に伝える。

フォローアップで、期限を過ぎても推奨事項が実施されていない場合です。経営者が「人手が足りない」などの理由を挙げても、最初に確かめることは同じです。実施しないまま放置するのは、事実上、リスクを受け入れる判断と同じ。

- まず、その判断が経営者の権限の範囲かを確かめる。
- 次に、新しい期限を含む対応計画を求めるか、上位の経営者や監査委員会に伝える。
- 監査人は、期限を勝手に延ばしません。
- 解決済みとして記録することも、代わりに実施することもしません。

不正や違法行為の兆候を見つけたときの対応：

- 自分で調査を進めない。
- 決められた経路（監査部門の責任者、経営者、監査委員会など）に速やかに報告する。
- 関与が疑われる人には伝えない。

よくある誤り

誤りは次の 4 つです。

- 講評会で事実を確かめないまま、報告書を出す。事実の誤りが報告書に残り、関係者の協力を失います。
- 経営者が反対したので、発見事項を報告書から削る。証拠が十分なら発見事項を残し、経営者の反対意見を併記します。反対されたことは、証拠を見直す理由にはなっても、削る理由にはなりません。
- 報告書を出したら監査は終わりと考え、フォローアップをしない。経営者が適切な是正措置を取ったかの確認は、報告の後の監査人の仕事です。
- 推奨事項を、監査人が自分で実施する。監査人が経営者の代わりに直すことはしません。

SAMPLE

関連する基準

- IIA グローバル内部監査基準（Standard 14.2 と報告の基準）[^iia]
- ISACA 用語集[^glossary]
- ISACA 職業倫理規定[^ethics]

1-2-6 監査プロセスの品質保証と改善 [1.2.6]

関係する補助タスク：8（品質保証と改善プログラムの一環として監査プロセスを評価する）

定義

監査の**品質保証**とは、監査が基準に従い、結論が証拠で支えられていると確かめる仕組み。用語集の定義は「対象が決められた要求に合っているという十分な確信を与えるための、計画的で体系的な活動」です[^glossary]。

IIA の基準は、内部監査部門の長に求めます。**品質保証と改善のプログラム** を設けること[^iia]。プログラムは次の 2 つを含みます。

- **内部評価**：日々の監督（調書のレビュー）と、定期的な自己評価
- **外部評価**：組織の外の、資格のある独立した評価者による評価。IIA の基準は、少なくとも 5 年に 1 回の実施を求めている[^iia]

なぜ監査で問われるか

監査部門自身も、改善の対象です。監査の品質が落ちると、経営者や監査委員会が監査の結論を信頼できなくなります。

監査人が確かめること

監査部門の品質の評価で見る点は、次の 5 つです。

1. 監査が計画どおりに行われ、計画の変更が承認されているか
2. 調書が結論を支え、上位者のレビューの記録があるか
3. 監査人の能力を保つ教育が行われているか（CISA の CPE もその一つ[^cpe]）
4. 監査対象からのフィードバック（アンケートなど）を集め、改善に使っているか
5. 監査の指標（計画の達成率、報告までの日数、推奨事項の実施率など）を測っているか

SAMPLE

評価で見つかった改善点は、監査部門の責任者が改善計画にまとめます。監査委員会にも報告します。

監査対象のフィードバックで不満が多く集まったときの対応です。不満の例は「監査の終わりから報告書が届くまでが長すぎる」など。

- 最初に、関係する指標（報告までの日数など）を測り、実態をつかむ。
- 実態が分かる前に、報告書の中身を減らさない。
- 実態が分かる前に、アンケートをやめない。

教育が行われているか（3）の確かめ方：

- 教育の計画と、監査人ごとの受講の記録（CPE の時間など）を閲覧する。
- 予算に研修費の項目があることは、教育が実際に行われた証拠にならない。
- 本人や責任者への質問だけでも足りない。

外部評価の方法は 2 つです。

- 組織の外の評価者が、すべてを評価する形
- 内部で自己評価を行い、外部の評価者がその結果を検証する形

どちらの形でも、評価者の独立性と能力を確かめなければ、前提が成り立ちません。

品質保証のレビューで、基準に合っていない監査が見つかったときの対応：

- その監査の結論が今も正しいかを確かめる。
- 結論に影響があれば、報告書の読み手に伝える。
- 必要なら、追加の手続を行う。

よくある誤り

誤りは次の 3 つです。

- 品質保証のレビューを、その監査を担当した本人に任せる。内部評価の日々の監督は、担当者の調書を上位者がレビューする形で行います。本人のチェックでは、監督になりません。
- 外部評価を、監査部門と利害関係のある人に依頼する。外部評価の前提は、評価者の独立性と能力です。

SAMPLE

- 指標を監査人の人事評価だけに使い、監査の手順の改善に使わない。指標は監査の手順を直す材料です。人の評価だけに使うと、数値の操作を招きます。

関連する基準

- IIA グローバル内部監査基準（Standard 8.3・8.4 の品質）[^iia]
- ISACA 用語集[^glossary]

SAMPLE

サンプルはここまでです

続き(第2章〜巻末)は、CISA 問題集のご購入で、頻出度別ノート・暗記用ノートと合わせて3点すべてダウンロードできます。

SAMPLE

CISA 学習用テキスト(無料サンプル)

版

2026年10月版(CISA 試験範囲(ISACA 公式 CISA Examination Content Outline・2024年8月発効)準拠)

発行

IT資格道場(https://www.shikaku-doujou.com)

お問い合わせ

info@shikaku-doujou.com

ISACA および CISA は、ISACA の登録商標です。記載されているその他の会社名・製品名・サービス名は、各社の商標または登録商標です。

本教材は ISACA が公開している試験内容の概要（受験者ガイド 付録A）などを基に作成したもので、ISACA との提携・承認関係はありません。

本文・図表・設問はすべてオリジナルの著作物です。無断での転載・複製・再配布・二次販売はできません。お気づきの点は info@shikaku-doujou.com までご連絡ください。

SAMPLE