0001 ガバナンス・内部統制 > コーポレートガバナンス・ITガバナンス ｜ 難易度：基礎

ITガバナンスの実践で、取締役会等が最も重視すべき役割はどれか。

ア．経営戦略とIT戦略の整合を確認し、重要なIT投資・リスクについて方向付けと監督を行う
イ．個々のプログラムコードを取締役会が直接レビューする
ウ．全てのIT運用作業を監査部門へ委任する
エ．IT投資の効果を確認せず導入件数だけを増やす

答え・解説 正答：ア

ア：ITガバナンスでは、経営戦略とIT戦略の整合、重要な意思決定、実行責任・説明責任の明確化が重要である。
イ：取締役会等の主な役割は経営レベルの方向付け・監督であり、実装作業の直接実施ではない。
ウ：監査部門は独立評価を行う立場であり、業務執行の主体ではない。
エ：ITガバナンスではITパフォーマンスや価値の確認が必要である。
総合解説：システム管理基準は、経営戦略・ビジネスモデルの確認、IT戦略、ITパフォーマンス、実行責任・説明責任、取締役会等のリーダーシップをITガバナンスの要素として示している。

対象：2026年度 / 基準日 2026-09-02

0002 ガバナンス・内部統制 > コーポレートガバナンス・ITガバナンス ｜ 難易度：基礎

IT戦略を策定する際に最も適切な考え方はどれか。

ア．最新技術を採用すること自体を目的にする
イ．経営戦略・ビジネスモデルを踏まえ、ITが事業価値の創出やリスク管理にどう寄与するかを明確にする
ウ．IT部門の予算消化を最優先する
エ．既存システムを一切変更しない方針を固定する

答え・解説 正答：イ

ア：技術導入は経営目的や価値との対応が必要である。
イ：IT戦略はIT部門だけの技術計画ではなく、経営戦略と一体で策定する必要がある。
ウ：予算消化はIT戦略の目的ではない。
エ：経営環境やリスクの変化に応じた見直しが必要である。
総合解説：ITガバナンスでは、経営戦略とビジネスモデルを確認し、それを実現するIT戦略を策定して成果を評価する。

対象：2026年度 / 基準日 2026-09-02

0003 ガバナンス・内部統制 > コーポレートガバナンス・ITガバナンス ｜ 難易度：基礎

ITガバナンスにおける『説明責任』の例として最も適切なものはどれか。

ア．責任者を決めず複数部門で共同管理する
イ．失敗時だけ担当者個人に責任を押し付ける
ウ．重要なIT投資の意思決定者が、目的・判断根拠・結果について関係者へ説明できる状態にする
エ．IT投資の目的を記録しない

答え・解説 正答：ウ

ア：責任の所在が曖昧になる。
イ：組織的な権限・責任設計になっていない。
ウ：説明責任は、誰が何を決定・実行し、その結果について説明する責任を負うかを明確にする考え方である。
エ：後から判断根拠や成果を説明できない。
総合解説：ITガバナンスでは意思決定権限、実行責任、説明責任を明確にし、ステークホルダーへの透明性を確保する。

対象：2026年度 / 基準日 2026-09-02

0004 ガバナンス・内部統制 > コーポレートガバナンス・ITガバナンス ｜ 難易度：標準

IT投資のガバナンス監査で、投資案件の承認後に最も重要な確認はどれか。

ア．承認済みなら効果測定を行わない
イ．予算を使い切ったかだけを確認する
ウ．システム稼働開始後は経営層が関与しない
エ．期待効果・コスト・リスクについて実績をモニタリングし、必要に応じ是正しているか

答え・解説 正答：エ

ア：投資価値や問題を把握できない。
イ：成果やリスクを評価できない。
ウ：重要投資は継続的な監督が必要である。
エ：ITガバナンスでは承認時だけでなく、実施後のITパフォーマンス確認と是正が重要である。
総合解説：監査では、投資前の期待価値と稼働後の成果を比較し、KPI、コスト、リスク、利用状況等を経営レベルで監視しているかを確認する。

対象：2026年度 / 基準日 2026-09-02

0005 ガバナンス・内部統制 > コーポレートガバナンス・ITガバナンス ｜ 難易度：標準

データ利活用をITガバナンスの観点から監査する際、最も適切な着眼点はどれか。

ア．データの責任者、品質、利用目的、アクセス、意思決定への利用方法が組織的に管理されているか

イ．データ量が多いほどガバナンスが優れていると判断する

ウ．分析担当者だけが自由に利用ルールを決める

エ．データ品質を確認せずAIに入力すればよい

答え・解説 正答：ア

ア：データを経営判断に使うには、責任・品質・利用ルールをガバナンスの仕組みとして整備する必要がある。

イ：量だけでは品質や適正利用を評価できない。

ウ：組織的な責任・方針が必要である。

エ：不正確なデータは誤った意思決定につながる。

総合解説：システム管理基準ではITガバナンス実践に必要な要件としてデータ利活用と意思決定を位置付けている。

対象：2026年度 / 基準日 2026-09-02

0006 ガバナンス・内部統制 > コーポレートガバナンス・ITガバナンス ｜ 難易度：標準

ITガバナンス監査でステークホルダーへの対応を評価する際、最も適切な確認はどれか。

ア．IT部門の都合だけを意思決定基準にする

イ．主要ステークホルダーの要求や利害を把握し、ITに関する意思決定へ適切に反映しているか

ウ．全ステークホルダーの要求を無条件に全て採用する

エ．ステークホルダーを特定しない

答え・解説 正答：イ

ア：他のステークホルダーの要求を無視している。

イ：ITガバナンスは株主・顧客・従業員・取引先等の利害を考慮して意思決定する必要がある。

ウ：相反する要求を優先順位付けする必要がある。

エ：要求やリスクを把握できない。

総合解説：監査では、重要な利害関係者を特定し、価値・リスク・資源配分の意思決定にその要求が適切に考慮されているかを見る。

対象：2026年度 / 基準日 2026-09-02

0007 ガバナンス・内部統制 > コーポレートガバナンス・ITガバナンス ｜ 難易度：標準

全社で生成AIの利用が急拡大したが、利用方針や責任部門が定まっていない。ITガバナンス上の最も適切な改善はどれか。

ア．各従業員が独自ルールを決める
イ．生成AIを使う部門だけで経営リスクを判断する
ウ．経営レベルで利用方針、リスク許容度、責任・説明体制を定め、利用状況をモニタリングする
エ．利用実態を把握せず全面禁止とするだけ

答え・解説 正答：ウ

ア：組織として一貫した統制ができない。
イ：全社的なリスクや法務・情報管理を考慮しにくい。
ウ：新技術の利用でも、方向付け・責任・リスク管理・成果確認というガバナンスが必要である。
エ：経営目的やリスクを踏まえたガバナンス判断になっていない。
総合解説：新技術導入時は、経営戦略との整合、リスク評価、責任分担、データ管理、成果モニタリングをガバナンスの枠組みに組み込む。

対象：2026年度 / 基準日 2026-09-02

0008 ガバナンス・内部統制 > コーポレートガバナンス・ITガバナンス ｜ 難易度：標準

ITガバナンスとITマネジメントの関係として最も適切なものはどれか。

ア．両者は完全に同一概念で区別しない
イ．ITマネジメントが取締役会を監督する
ウ．ITガバナンスは日々のジョブ運用だけを行う
エ．ITガバナンスが方向付け・監督・評価を行い、ITマネジメントがその方針に基づき計画・実行・運用する

答え・解説 正答：エ

ア：経営レベルの方向付けと業務執行管理は区別される。
イ：通常は逆方向のガバナンス関係である。
ウ：日常運用はマネジメント・運用の領域である。
エ：ガバナンスとマネジメントは役割が異なるが、相互に連携して機能する。
総合解説：監査では、経営がITを方向付け・監督する仕組みと、管理者が具体的に実行・運用する仕組みの双方を評価する。

対象：2026年度 / 基準日 2026-09-02

0009 ガバナンス・内部統制 > コーポレートガバナンス・ITガバナンス ｜ 難易度：応用

ITガバナンス監査で、重要な意思決定の議事録が残されていない場合の主なリスクはどれか。

ア．意思決定根拠と責任所在を後から検証できず、説明責任が弱くなる
イ．必ずシステム障害が発生する
ウ．IT予算が必ず減少する
エ．全ての取引が無効になる

答え・解説 正答：ア

ア：意思決定記録は透明性、説明責任、モニタリングの基礎となる。
イ：議事録欠如が直ちに障害を意味するわけではない。
ウ：直接的な因果関係はない。
エ：一般的にはそのような効果はない。
総合解説：監査では、重要なIT投資・リスク受容・方針変更について、承認者、判断根拠、条件、フォロー事項が追跡可能かを確認する。

対象：2026年度 / 基準日 2026-09-02

0010 ガバナンス・内部統制 > コーポレートガバナンス・ITガバナンス ｜ 難易度：応用

ITガバナンスの有効性を評価する指標として最も適切なものはどれか。

ア．サーバ台数だけ
イ．経営目標に対するIT成果、リスク状況、資源利用、重要施策の達成度を組み合わせて評価する
ウ．IT部門の残業時間だけ
エ．導入製品のブランド数だけ

答え・解説 正答：イ

ア：台数だけでは経営価値やリスクを評価できない。
イ：ITガバナンスの有効性は、技術指標だけでなく価値・リスク・資源・成果の観点から評価する。
ウ：一つの運用指標にすぎない。
エ：ガバナンス成果とは関係しない。
総合解説：監査では、IT戦略の実現度、投資効果、重大リスク、サービス成果、資源配分を経営目標と対応させて確認する。

対象：2026年度 / 基準日 2026-09-02

0011 ガバナンス・内部統制 > IT全般統制 ｜ 難易度：基礎

監査人がIT全般統制として評価対象に分類すべき統制の組合せはどれか。

ア．一つの請求書の金額計算だけ

イ．特定画面の入力必須チェックだけ

ウ．システムの開発・保守、運用・管理、アクセス管理、外部委託管理などIT環境全体に共通する統制

エ．一件の仕訳承認だけ

答え・解説 正答：ウ

ア：個別取引の自動計算はIT業務処理統制の例である。

イ：個別業務処理に組み込まれた統制である。

ウ：IT全般統制は個々の取引処理よりも、ITを利用した統制が安定して機能する基盤を支える。

エ：取引レベルの統制であり、IT全般統制そのものではない。

総合解説：金融庁実施基準はIT全般統制の例として、システム開発・保守、運用管理、アクセス管理、安全性、外部委託管理等を挙げている。

対象：2026年度 / 基準日 2026-09-02

0012 ガバナンス・内部統制 > IT全般統制 ｜ 難易度：基礎

本番プログラム変更のIT全般統制として最も適切なものはどれか。

ア．開発者が自分の判断だけで本番を直接変更する

イ．本番変更履歴を残さない

ウ．緊急変更を全て統制対象外にする

エ．変更申請、影響評価、承認、テスト、本番反映を役割分担して記録する

答え・解説 正答：エ

ア：承認・牽制・テストが不足する。

イ：変更の追跡と事後検証ができない。

ウ：緊急時でも事後承認・記録等の統制が必要である。

エ：変更管理では未承認・未テストの変更が本番へ入らない仕組みが重要である。

総合解説：IT全般統制の監査では、変更要求から本番反映までの承認、職務分掌、テスト、履歴、緊急変更手続を確認する。

対象：2026年度 / 基準日 2026-09-02

0013 ガバナンス・内部統制 > IT全般統制 ｜ 難易度：基礎

システム開発に関するIT全般統制で最も重要な確認はどれか。

ア．要件・設計・テスト・移行について承認と品質確認が行われ、本番利用の可否が適切に判断されているか

イ．開発期間が短いほど統制が有効と判断する

ウ．開発者の人数だけを確認する

エ．本番移行後は開発記録を全て削除する

答え・解説 正答：ア

ア：開発統制は不適切なシステムが本番へ導入されるリスクを低減する。

イ：期間の短さは品質を保証しない。

ウ：人数だけでは開発統制の有効性を評価できない。

エ：変更履歴・追跡性を失う。

総合解説：承認された要件、テスト証拠、移行承認、開発・本番環境の分離などを確認し、開発ライフサイクルの統制を評価する。

対象：2026年度 / 基準日 2026-09-02

0014 ガバナンス・内部統制 > IT全般統制 ｜ 難易度：標準

IT運用管理の統制として最も適切なものはどれか。

ア．異常終了しても記録せず再実行する

イ．定例ジョブの実行結果・異常終了・再実行を監視し、例外処理を記録する

ウ．ジョブ監視を行わず利用者からの苦情だけで障害を知る

エ．運用手順を担当者の記憶だけに依存する

答え・解説 正答：イ

ア：原因・影響・再実行の妥当性を追跡できない。

イ：運用統制では日常処理が完全・正確・継続的に実行されているかを管理する。

ウ：早期検知と統制が不十分である。

エ：属人化と処理誤りのリスクが高い。

総合解説：IT全般統制ではジョブ管理、バックアップ、障害管理、構成管理等の日常運用が定めた手順で実施・記録されているかを確認する。

対象：2026年度 / 基準日 2026-09-02

0015 ガバナンス・内部統制 > IT全般統制 ｜ 難易度：標準

特権ID管理をIT全般統制として監査する際、最も適切な確認はどれか。

ア．特権IDを全担当者で共有する
イ．特権IDの利用ログを保存しない
ウ．特権IDの付与・利用・レビュー・削除が承認され、利用ログを追跡できるか
エ．退職者の特権IDを予備として残す

答え・解説 正答：ウ

ア：個人単位の追跡性が失われる。
イ：不正・誤操作を事後確認できない。
ウ：特権権限は広範な変更が可能なため、厳格な管理が必要である。
エ：不要権限が残存する。
総合解説：IT全般統制では、管理者権限の最小化、申請承認、個人識別、利用記録、定期レビュー、退職・異動時削除を確認する。

対象：2026年度 / 基準日 2026-09-02

0016 ガバナンス・内部統制 > IT全般統制 ｜ 難易度：標準

バックアップ統制を監査する際、最も適切な証拠はどれか。

ア．バックアップ方針書だけ
イ．ストレージ容量だけ
ウ．担当者の『取れている』という説明だけ
エ．バックアップ実行ログに加え、定期的な復元テストの記録

答え・解説 正答：エ

ア：運用と復元可能性を確認できない。
イ：バックアップの完全性・復元性を証明しない。
ウ：客観的な運用証拠が必要である。
エ：バックアップが取得されていても復元できなければ統制目的を達成できない。
総合解説：監査では対象・頻度・保管・暗号化・世代管理に加え、実際に復元できることを証拠で確認する。

対象：2026年度 / 基準日 2026-09-02

0017 ガバナンス・内部統制 > IT全般統制 ｜ 難易度：標準

外部委託先が運用するシステムのIT全般統制を評価する際、最も適切な考え方はどれか。

ア．委託しても委託元の管理責任は残るため、契約・SLA・報告・監査情報等で統制状況を把握する

イ．委託した時点で統制評価は不要になる

ウ．委託先の営業資料だけで有効と判断する

エ．契約に統制要件を記載しない

答え・解説 正答：ア

ア：外部委託は統制責任の消滅を意味しない。

イ：委託先リスクを含めて管理する必要がある。

ウ：客観的な保証や運用証拠が必要である。

エ：要求事項や責任分界が曖昧になる。

総合解説：金融庁実施基準は外部委託に関する契約管理をIT全般統制の例に含めている。監査では委託先統制の把握方法も確認する。

対象：2026年度 / 基準日 2026-09-02

0018 ガバナンス・内部統制 > IT全般統制 ｜ 難易度：標準

IT全般統制が弱い場合、IT業務処理統制の評価へ与える影響として最も適切なものはどれか。

ア．IT業務処理統制は必ず有効になる

イ．プログラム変更やアクセスが適切に管理されていないと、自動統制を継続的に信頼しにくくなる

ウ．IT全般統制と業務処理統制は常に無関係である

エ．統制評価は不要になる

答え・解説 正答：イ

ア：逆であり、基盤統制の弱さは信頼性を低下させる。

イ：IT業務処理統制は基盤となるIT全般統制に依存する場合がある。

ウ：自動統制は変更管理・アクセス管理等に依存する。

エ：むしろ追加手続や代替統制の評価が必要になる。

総合解説：監査では、自動化された業務処理統制のロジックが承認なく変更されないことや、関連マスタへのアクセスが管理されていることをIT全般統制で確認する。

対象：2026年度 / 基準日 2026-09-02

0019 ガバナンス・内部統制 > IT全般統制 ｜ 難易度：応用

緊急変更の管理として最も適切なものはどれか。

ア．緊急変更は一切記録しない
イ．誰でも本番を自由に変更できる
ウ．緊急時の簡略手続を事前定義し、実施後に記録・テスト・事後承認を行う
エ．緊急変更を通常変更と全く同じ時間をかけて処理し、障害復旧を妨げる

答え・解説 正答：ウ

ア：未承認変更や原因不明の障害につながる。
イ：権限統制を損なう。
ウ：緊急性に対応しつつ統制証跡を残す必要がある。
エ：緊急時に適した統制設計が必要である。
総合解説：監査では、緊急変更の定義、権限者、最小限の事前確認、事後レビュー、恒久対応への移行が定められているかを見る。

対象：2026年度 / 基準日 2026-09-02

0020 ガバナンス・内部統制 > IT全般統制 ｜ 難易度：応用

IT全般統制の運用有効性を評価する監査手続として最も適切なものはどれか。

ア．規程の表紙だけ確認する
イ．一件の成功例だけで年間有効と断定する
ウ．担当者への口頭質問だけで評価する
エ．一定期間の変更・アクセス・運用記録からサンプルを選び、定めた統制が実際に実施されたか検証する

答え・解説 正答：エ

ア：整備状況すら十分に確認できない。
イ：対象期間全体を代表する証拠が不足する。
ウ：運用証拠との突合が必要である。
エ：方針の存在だけでなく、対象期間にわたり統制が継続運用されているかを確認する。
総合解説：統制頻度・母集団・リスクに応じたサンプルを用い、承認記録、ログ、チケット等から統制の実施を確認する。

対象：2026年度 / 基準日 2026-09-02

0021 ガバナンス・内部統制 > IT業務処理統制・職務分掌 ｜ 難易度：基礎

IT業務処理統制の例として最も適切なものはどれか。

ア．入力された売上金額が許容範囲を超える場合にエラーとして登録を拒否する入力チェック
イ．データセンターへの入退室管理
ウ．プログラム変更の承認
エ．OS管理者IDの定期レビュー

答え・解説 正答：ア

ア：IT業務処理統制は個々の取引処理の完全性・正確性・正当性を確保するため業務アプリケーションに組み込まれる。
イ：IT全般統制・物理統制の例である。
ウ：IT全般統制の変更管理である。
エ：IT全般統制のアクセス管理である。
総合解説：入力チェック、マスタ参照、自動計算、重複防止、処理結果照合等はIT業務処理統制の代表例である。

対象：2026年度 / 基準日 2026-09-02

0022 ガバナンス・内部統制 > IT業務処理統制・職務分掌 ｜ 難易度：基礎

売上システムで同じ伝票番号の二重登録を拒否する機能の主な統制目的はどれか。

ア．利用者の本人認証を行う
イ．取引の重複計上を防止し、処理の完全性・正確性を高める
ウ．システムのバックアップを取得する
エ．開発者の職務分掌を確保する

答え・解説 正答：イ

ア：伝票番号チェックは利用者認証とは別である。
イ：一意性チェックは同一取引の重複処理リスクを低減する。
ウ：データ保全統制とは異なる。
エ：組織的統制とは別の機能である。
総合解説：監査では一意性制約や重複検知ロジックが要件どおり機能し、例外処理も管理されているかを確認する。

対象：2026年度 / 基準日 2026-09-02

0023 ガバナンス・内部統制 > IT業務処理統制・職務分掌 ｜ 難易度：基礎

購買業務で不正を牽制する職務分掌を設計する場合、最も適切な考え方はどれか。

ア．業務効率を優先し全権限を一人に集約する
イ．職務分掌はシステム権限へ反映しない
ウ．一人が取引の申請・承認・実行・記録を全て単独で完結できないよう役割を分離する
エ．役割分担を文書化しない

答え・解説 正答：ウ

ア：不正や誤りを発見しにくくなる。
イ：実際の権限で相互牽制を確保できない。
ウ：相互牽制により誤りや不正の発生・隠蔽リスクを低減する。
エ：責任と権限が曖昧になる。
総合解説：監査では組織上の役割だけでなく、アプリケーション権限やワークフローが職務分掌を実現しているかも確認する。

対象：2026年度 / 基準日 2026-09-02

0024 ガバナンス・内部統制 > IT業務処理統制・職務分掌 ｜ 難易度：標準

購買システムで、発注者が自分の発注を自分で承認できる権限を持っている。最も直接的な統制上の問題はどれか。

ア．バックアップ頻度が不足している
イ．ネットワーク帯域が不足している
ウ．データベースが正規化されていない
エ．申請と承認の職務分掌が機能していない

答え・解説 正答：エ

ア：発注承認権限とは別問題である。
イ：業務承認統制とは関係しない。
ウ：職務分掌の問題とは異なる。
エ：自己承認を許すと架空・不適切な発注を牽制する統制が弱くなる。
総合解説：監査では権限ロールの組合せを分析し、申請・承認・支払・記録等の競合権限が同一利用者へ付与されていないか確認する。

対象：2026年度 / 基準日 2026-09-02

0025 ガバナンス・内部統制 > IT業務処理統制・職務分掌 ｜ 難易度：標準

入力統制の有効性をテストする方法として最も適切なものはどれか。

ア．正常値・境界値・不正値を入力し、仕様どおり受理・拒否されるか再実施する
イ．入力画面の色だけを見る
ウ．担当者の説明だけで有効とする
エ．本番データを無断で変更する

答え・解説 正答：ア

ア：自動入力チェックは監査人がテストデータ等を用いて動作を直接確認できる。
イ：統制ロジックを検証できない。
ウ：実際の動作証拠が不足する。
エ：業務影響を避け、適切なテスト環境・手続を用いる必要がある。
総合解説：監査ではテストデータ、設定確認、プログラム仕様、実データの例外分析を組み合わせて自動統制を評価する。

対象：2026年度 / 基準日 2026-09-02

0026 ガバナンス・内部統制 > IT業務処理統制・職務分掌 ｜ 難易度：標準

マスタデータの変更統制として最も適切なものはどれか。

ア．利用者なら誰でも直接変更できる
イ．価格や取引先マスタの変更を申請・承認し、変更前後と変更者を記録する
ウ．変更履歴を保存しない
エ．マスタ変更は業務処理に影響しないとみなす

答え・解説 正答：イ

ア：不正・誤変更のリスクが高い。
イ：マスタは多くの取引処理結果に影響するため、変更権限と承認を管理する必要がある。
ウ：後から変更の正当性を検証できない。
エ：自動計算・判定に広範な影響を与えることがある。
総合解説：監査ではマスタ変更権限、申請承認、変更ログ、定期レビュー、職務分掌を確認する。

対象：2026年度 / 基準日 2026-09-02

0027 ガバナンス・内部統制 > IT業務処理統制・職務分掌 ｜ 難易度：標準

自動計算統制を監査する際、最も重要な確認はどれか。

ア．計算処理が高速かだけを確認する
イ．一件だけ結果が正しければ永続的に有効とする
ウ．計算ロジックが承認された業務ルールと一致し、変更が適切に管理されているか
エ．計算式の所有者を不明確にする

答え・解説 正答：ウ

ア：速度は正確性を保証しない。
イ：ロジック変更や条件差を考慮する必要がある。
ウ：自動計算は一度誤ると大量の取引へ同じ誤りを与える可能性がある。
エ：責任や変更管理が弱くなる。
総合解説：監査では仕様・設定・テスト・変更管理を確認し、必要に応じ再計算して正確性を検証する。

対象：2026年度 / 基準日 2026-09-02

0028 ガバナンス・内部統制 > IT業務処理統制・職務分掌 ｜ 難易度：標準

例外取引を通常処理から外して手動承認する仕組みを監査する際、最も適切な確認はどれか。

ア．例外処理は少ないので統制不要とする
イ．誰でも例外承認できるようにする
ウ．例外履歴を残さない
エ．例外条件、承認権限、処理理由、事後レビューが明確で記録されているか

答え・解説 正答：エ

ア：少数でも重大な不正・誤りにつながることがある。
イ：権限統制が弱くなる。
ウ：濫用や傾向を分析できない。
エ：例外処理は通常統制を迂回する可能性があるため、特に厳格な管理が必要である。
総合解説：監査では例外件数、理由、承認者、再発傾向を分析し、通常統制を不当に回避していないか確認する。

対象：2026年度 / 基準日 2026-09-02

0029 ガバナンス・内部統制 > IT業務処理統制・職務分掌 ｜ 難易度：応用

職務分掌上の競合権限を完全に分離できない小規模組織で、最も適切な代替統制はどれか。

ア．独立した責任者が取引や権限利用を定期的に事後レビューする
イ．競合権限を放置し一切確認しない
ウ．全員に管理者権限を付与する
エ．職務分掌のルール自体を廃止する

答え・解説 正答：ア

ア：人員制約で分離が困難な場合、補完的なモニタリング等でリスクを低減する。
イ：不正・誤りの検知機会がない。
ウ：リスクをさらに高める。
エ：制約を踏まえた代替統制が必要である。
総合解説：監査では組織規模や業務特性を考慮し、独立レビュー、詳細ログ監視、経営者承認等の代替統制が有効か評価する。

対象：2026年度 / 基準日 2026-09-02

0030 ガバナンス・内部統制 > IT業務処理統制・職務分掌 ｜ 難易度：応用

IT業務処理統制をCAATで監査する例として最も適切なものはどれか。

ア．監査対象者の勤怠だけを集計する
イ．全取引データから承認限度額超過や重複伝票を抽出し、統制例外を分析する
ウ．サーバの型番だけを一覧化する
エ．プログラムの行数だけを数える

答え・解説 正答：イ

ア：業務処理統制と直接関係しない。
イ：大量データの例外抽出は自動統制の運用実態を検証するのに有効である。
ウ：取引処理統制を検証できない。
エ：統制の有効性を評価できない。
総合解説：監査では全件データ分析により、通常統制を通過した不自然な取引、閾値分割、重複、欠番等を識別できる。

対象：2026年度 / 基準日 2026-09-02

0031 リスク管理・コンプライアンス > リスク識別・評価・対応 ｜ 難易度：基礎

ITリスクを識別する際、最も適切な出発点はどれか。

ア．発生済み事故だけを対象にする
イ．システム名の一覧だけでリスクを決める
ウ．経営目標・重要業務・情報資産を把握し、それらに影響する脅威や脆弱性を洗い出す
エ．技術部門の感覚だけで決める

答え・解説 正答：ウ

ア：未発生の潜在リスクも識別する必要がある。
イ：重要性や脅威・脆弱性を評価できない。
ウ：リスクは組織目標への影響として捉え、重要な業務・資産と脅威・脆弱性の関係から識別する。
エ：事業影響や経営目標との関係を考慮する必要がある。
総合解説：システム管理基準はITガバナンスでリスクの評価と対応を求めている。監査では、経営目的と重要資産からリスクが体系的に識別されているかを見る。

対象：2026年度 / 基準日 2026-09-02

0032 リスク管理・コンプライアンス > リスク識別・評価・対応 ｜ 難易度：基礎

リスクを『発生可能性×影響度』で評価する主な目的はどれか。

ア．全てのリスクを同じ対応にするため
イ．リスクを完全にゼロにするため
ウ．影響度を無視するため
エ．リスクの大きさを比較し、対応の優先順位を付けるため

答え・解説 正答：エ

ア：リスクの大きさに応じて対応を変える。
イ：リスク管理は必ずしもゼロ化を目的としない。
ウ：発生可能性と影響度の双方を考慮する。
エ：複数リスクを共通尺度で評価することで、限られた資源を重要リスクへ配分しやすくなる。
総合解説：リスク評価では定性的・定量的な尺度を用いて重要度を比較し、対応方針や監査優先度を決める。

対象：2026年度 / 基準日 2026-09-02

0033 リスク管理・コンプライアンス > リスク識別・評価・対応 ｜ 難易度：基礎

重大な法令リスクが見込まれる新規サービスについて、提供そのものを取りやめた。この対応はどれに当たるか。

ア．重大な法令リスクが高いサービスの提供自体を中止する
イ．セキュリティ対策を追加して発生可能性を下げる
ウ．保険へ加入する
エ．追加対策をせず経営者が残存リスクを了承する

答え・解説 正答：ア

ア：リスクの原因となる活動を行わないことでリスクを除去する対応が回避である。
イ：これはリスク低減に当たる。
ウ：損失の一部を第三者へ移転するリスク移転の例である。
エ：リスク受容の例である。
総合解説：代表的な対応には回避、低減、移転・共有、受容などがあり、リスクの性質と許容度に応じて選択する。

対象：2026年度 / 基準日 2026-09-02

0034 リスク管理・コンプライアンス > リスク識別・評価・対応 ｜ 難易度：標準

セキュリティ対策を実施して発生可能性を下げた後も、なお残っているリスクを何というか。

ア．対策実施前のリスク
イ．統制や対策を実施した後にも残るリスク
ウ．まだ識別されていないリスクだけ
エ．必ず受容可能なリスク

答え・解説 正答：イ

ア：一般に固有リスク・初期リスク等として区別される。
イ：対策によってリスクは低減できても、通常は完全には消滅しない。
ウ：残存リスクは既知のリスクにも存在する。
エ：残存リスクが許容水準を超える場合は追加対応が必要である。
総合解説：監査では対策後の残存リスクが組織のリスク許容度内か、誰が受容を承認したかを確認する。

対象：2026年度 / 基準日 2026-09-02

0035 リスク管理・コンプライアンス > リスク識別・評価・対応 ｜ 難易度：標準

クラウド移行のリスク評価で最も適切な観点はどれか。

ア．クラウドは安全なのでリスク評価を省略する
イ．料金だけで採否を決める
ウ．可用性、データ保護、責任分界、委託先依存、法令・契約、退出・移行可能性を総合評価する
エ．サービス提供者が全リスクを負うとみなす

答え・解説 正答：ウ

ア：利用形態に応じた固有リスクがある。
イ：事業影響・安全性等を評価できない。
ウ：クラウドリスクは技術だけでなく契約・事業継続・サプライチェーンを含めて評価する必要がある。
エ：責任共有モデル上、利用者側の責任も残る。
総合解説：監査ではサービス特性と責任分界を踏まえ、情報資産・可用性・データ所在・委託先管理・ロックイン等が評価されているかを見る。

対象：2026年度 / 基準日 2026-09-02

0036 リスク管理・コンプライアンス > リスク識別・評価・対応 ｜ 難易度：標準

サイバーセキュリティリスクの優先順位を決める際、最も不適切な方法はどれか。

ア．重要業務への影響を考慮する
イ．攻撃可能性や既知の悪用状況を考慮する
ウ．代替統制や復旧能力を考慮する
エ．脆弱性の技術的スコアだけで事業影響を考慮せず決定する

答え・解説 正答：エ

ア：重要な判断要素である。
イ：実際の脅威を反映するため有効である。
ウ：実効的な残存リスク評価に役立つ。
エ：技術的深刻度だけでは、資産価値、露出状況、悪用状況、事業影響を十分に反映できない。
総合解説：IPAのサイバーセキュリティ経営の実践では、経営への重要度や脅威の可能性を踏まえたリスク把握と対応を求めている。

対象：2026年度 / 基準日 2026-09-02

0037 リスク管理・コンプライアンス > リスク識別・評価・対応 ｜ 難易度：標準

リスク所有者が対策後のリスクを受け入れる場面で、監査上確認すべき手続はどれか。

ア．残存リスクと根拠を明確にし、定められた権限者が許容度に照らして承認する
イ．担当者が口頭で問題ないと言えば受容完了とする
ウ．高リスクも全て自動的に受容する
エ．受容したリスクは二度と見直さない

答え・解説 正答：ア

ア：リスク受容は『対策しない』ことではなく、情報に基づく意思決定として記録・承認する必要がある。
イ：権限・根拠・証跡が不足する。
ウ：許容度や経営判断が必要である。
エ：環境変化に応じて再評価する必要がある。
総合解説：監査ではリスク所有者、承認権限、受容理由、期限、モニタリング条件が明確かを確認する。

対象：2026年度 / 基準日 2026-09-02

0038 リスク管理・コンプライアンス > リスク識別・評価・対応 ｜ 難易度：標準

リスク登録簿の監査で最も重要な確認はどれか。

ア．リスク名だけが一覧化されているか
イ．主要リスクについて所有者、評価、対応策、期限、残存リスク、状態が更新されているか
ウ．全リスクの評価値が同じか
エ．古いリスクを削除して履歴を残さないか

答え・解説 正答：イ

ア：管理に必要な責任・対応・状態が不足する。
イ：リスク登録簿はリスク管理の継続的な追跡に用いる。
ウ：実態に応じ差があるのが通常である。
エ：変化や判断経緯を追跡できない。
総合解説：監査ではリスクが一度評価されただけで放置されず、対応状況と環境変化に応じて更新されているかを見る。

対象：2026年度 / 基準日 2026-09-02

0039 リスク管理・コンプライアンス > リスク識別・評価・対応 ｜ 難易度：応用

新しい法規制が施行される予定である。リスク管理上最も適切な対応はどれか。

ア．施行後に違反が見つかってから対応する
イ．法務部門だけの問題としてITへの影響を確認しない
ウ．適用範囲と影響を事前評価し、必要な統制・システム変更・教育を施行前に計画する
エ．既存統制が必ず十分と仮定する

答え・解説 正答：ウ

ア：コンプライアンスリスクを高める。
イ：システム・データ・契約等への影響があり得る。
ウ：規制対応は施行後の後追いではなく、変更リスクとして事前管理することが望ましい。
エ：規制要件とのギャップ分析が必要である。
総合解説：監査では法令改正のモニタリング、影響分析、責任者、対応計画、実施状況が管理されているかを確認する。

対象：2026年度 / 基準日 2026-09-02

0040 リスク管理・コンプライアンス > リスク識別・評価・対応 ｜ 難易度：応用

インシデント後にリスク評価を見直す主な理由はどれか。

ア．事故が起きたリスクを必ず削除するため
イ．全リスクを最高レベルへ変更するため
ウ．事故原因を記録しないため
エ．実際の攻撃経路・影響・統制不備から、従来の発生可能性や影響評価の前提を更新するため

答え・解説 正答：エ

ア：再発リスクはむしろ高い場合がある。
イ：個別の影響と対策を評価する。
ウ：教訓をリスク管理へ反映する必要がある。
エ：実際の事象はリスク評価モデルや統制有効性を検証する重要な情報である。
総合解説：監査ではインシデント後の原因分析、残存リスク、再発防止策がリスク登録簿や対応計画へ反映されているかを見る。

対象：2026年度 / 基準日 2026-09-02

0041 リスク管理・コンプライアンス > 法令・契約・標準・ガイドライン ｜ 難易度：基礎

システム監査で法令を評価基準として用いる場合、最も重要なことはどれか。

ア．監査対象・期間に適用される法令と施行時点の要件を特定する
イ．現在の条文だけで過去期間も同じとみなす
ウ．一般的なブログ記事だけを基準にする
エ．法令名だけ把握し具体的要件を確認しない

答え・解説 正答：ア

ア：法令は改正されるため、監査対象期間に適用される内容を確認する必要がある。
イ：改正前後で要件が異なる場合がある。
ウ：一次情報を優先すべきである。
エ：準拠性を評価できない。
総合解説：監査では適用法令、施行日、所管官庁の公式ガイドライン等を確認し、対象業務の義務と実態を比較する。

対象：2026年度 / 基準日 2026-09-02

0042 リスク管理・コンプライアンス > 法令・契約・標準・ガイドライン ｜ 難易度：基礎

契約を監査基準として評価する例として最も適切なものはどれか。

ア．契約にない条件を後から当然の義務として扱う
イ．クラウド事業者とのSLAで定めた可用性・通知・データ返却条件が実際に履行されているか確認する
ウ．契約書を読まずサービス提供者の説明だけで判断する
エ．SLA違反の記録を保存しない

答え・解説 正答：イ

ア：契約・法令・合意の根拠確認が必要である。
イ：契約は当事者間の権利・義務を定めるため、委託・サービス監査の重要な評価基準となる。
ウ：義務内容を確認できない。
エ：履行状況や改善を追跡できない。
総合解説：監査では契約条項、SLA、責任分界、再委託、監査権、事故通知、終了時データ処理等を実態と照合する。

対象：2026年度 / 基準日 2026-09-02

**0043** リスク管理・コンプライアンス > 法令・契約・標準・ガイドライン ｜ 難易度：基礎

法令、契約、社内規程、任意のガイドラインが同じテーマに関係する場合、監査人の最も適切な対応はどれか。

ア．全て同じ法的強制力があるとみなす
イ．最も緩い基準だけを採用する
ウ．それぞれの適用関係と拘束力を整理し、監査対象に実際に求められる基準を特定する
エ．社内規程は監査基準にならないとする

**答え・解説** 正答：ウ

ア：任意ガイドラインと法令は同一ではない。
イ：法令や契約上の義務を満たさない可能性がある。
ウ：資料の種類によって法的拘束力や適用条件が異なるため、位置付けを区別する必要がある。
エ：組織が定めた統制基準として重要である。
総合解説：監査では法令上の義務、契約義務、自社方針、標準・ガイドラインの採用状況を整理し、評価基準を明示する。

対象：2026年度 / 基準日 2026-09-02

**0044** リスク管理・コンプライアンス > 法令・契約・標準・ガイドライン ｜ 難易度：標準

外部標準を社内規程へ採用する場合の監査上の確認として最も適切なものはどれか。

ア．標準名だけ規程に書けば十分とする
イ．改訂版が出ても永久に見直さない
ウ．標準の全項目を業務目的に関係なく強制する
エ．採用する版・適用範囲・例外・社内責任者が明確で、改訂を継続的に把握しているか

**答え・解説** 正答：エ

ア：具体的な適用範囲や版が不明確になる。
イ：新たなリスクや要求を反映できない。
ウ：適用性を評価する必要がある。
エ：外部標準は更新されるため、どの版をどこまで採用したかを管理する必要がある。
総合解説：監査では標準・ガイドラインの選定、版管理、適用宣言、例外承認、改訂モニタリングが整備されているかを確認する。

対象：2026年度 / 基準日 2026-09-02

0045 リスク管理・コンプライアンス > 法令・契約・標準・ガイドライン ｜ 難易度：標準

委託契約に『再委託は事前承認を要する』とあるのに、事業者が無断再委託していた。最も直接的な監査評価はどれか。

ア．契約上の再委託統制に対する準拠性の不備
イ．システム性能の不備
ウ．必ず刑事犯罪である
エ．契約に関係しないので監査対象外

答え・解説 正答：ア

ア：契約条項に反する運用は契約準拠上の問題である。
イ：契約違反の直接的論点ではない。
ウ：契約違反だけから刑事犯罪とは断定できない。
エ：委託管理監査では重要な論点である。
総合解説：監査では再委託の承認、再委託先への同等統制要求、情報管理、責任分界を契約と実態で確認する。

対象：2026年度 / 基準日 2026-09-02

0046 リスク管理・コンプライアンス > 法令・契約・標準・ガイドライン ｜ 難易度：標準

ライセンス条件のあるOSSを業務システムで利用する際、コンプライアンス監査で最も適切な確認はどれか。

ア．無償なので利用条件は存在しないとみなす
イ．使用しているOSSとライセンス条件を把握し、必要な表示・ソース提供等の義務に対応しているか
ウ．開発者個人だけがライセンスを把握すればよい
エ．OSSのバージョンを記録しない

答え・解説 正答：イ

ア：OSSにもライセンス条件がある。
イ：OSSもライセンス契約・著作権条件の順守が必要である。
ウ：組織として管理する必要がある。
エ：脆弱性・ライセンス管理にも影響する。
総合解説：監査ではソフトウェア資産台帳、ライセンス条件、配布形態、改変有無、承認プロセス等を確認する。

対象：2026年度 / 基準日 2026-09-02

0047 リスク管理・コンプライアンス > 法令・契約・標準・ガイドライン ｜ 難易度：標準

システム監査基準とシステム管理基準の関係として最も適切なものはどれか。

ア．両者は同一文書で内容も完全に同じである

イ．システム管理基準は監査人の倫理だけを定める

ウ．システム監査基準は監査人の行動・実施・報告の基準を示し、システム管理基準はITガバナンス・ITマネジメントの管理上の着眼点を示す

エ．システム監査基準はIT運用手順を詳細に規定するだけである

答え・解説 正答：ウ

ア：別の目的と構成を持つ。

イ：倫理はシステム監査基準側の主要領域である。

ウ：両基準は役割が異なり、システム管理基準は監査の評価基準として活用できる。

エ：監査の属性・実施・報告を定める。

総合解説：2023年改訂版ではシステム監査基準とシステム管理基準が相互補完し、監査人は管理基準等を評価尺度として活用できる。

対象：2026年度 / 基準日 2026-09-02

0048 リスク管理・コンプライアンス > 法令・契約・標準・ガイドライン ｜ 難易度：標準

ガイドラインを監査基準として使う際の最も適切な考え方はどれか。

ア．全ガイドライン違反を自動的に違法と判断する

イ．任意ガイドラインは監査で一切参照しない

ウ．組織の採用方針を確認しない

エ．法的義務か任意指針かを確認し、組織が採用している場合やリスク評価上有用な場合に評価尺度として活用する

答え・解説 正答：エ

ア：法的拘束力は文書ごとに異なる。

イ：ベストプラクティスや管理基準として有用な場合がある。

ウ：どの基準を遵守すると定めたかは監査上重要である。

エ：ガイドラインの位置付けを確認せず法令と同一視してはならない。

総合解説：監査では一次情報から文書の法的位置付けを確認し、法令・契約・社内規程との関係を整理して評価する。

対象：2026年度 / 基準日 2026-09-02

0049 リスク管理・コンプライアンス > 法令・契約・標準・ガイドライン ｜ 難易度：応用

クラウド契約終了時のコンプライアンス監査で最も重要な確認はどれか。

ア．契約に基づきデータの返却・移行・削除と、その証跡が適切に管理されているか
イ．契約終了後も全データを事業者へ永久保存させる
ウ．終了時の責任分界を契約で定めない
エ．データ移行可能性を事前確認しない

答え・解説 正答：ア

ア：契約終了時はデータ残存や利用不能のリスクが顕在化しやすい。
イ：契約・法令・目的に反する可能性がある。
ウ：移行・削除時の責任が曖昧になる。
エ：ベンダロックインや事業継続リスクが高まる。
総合解説：監査ではデータ返却形式、削除証明、バックアップ残存、移行支援、秘密保持の継続等を確認する。

対象：2026年度 / 基準日 2026-09-02

0050 リスク管理・コンプライアンス > 法令・契約・標準・ガイドライン ｜ 難易度：応用

法令や標準の改訂情報を把握する仕組みの監査で最も適切な確認はどれか。

ア．改訂情報を担当者の個人的なSNS閲覧だけに依存する
イ．情報源、担当者、確認頻度、影響分析、規程・システムへの反映手順が定められているか
ウ．改訂を把握しても影響分析しない
エ．旧版規程を更新せず並存させる

答え・解説 正答：イ

ア：継続性・網羅性が弱い。
イ：改訂情報を知るだけでなく、適用要件を実務へ反映するプロセスが必要である。
ウ：必要な対応を特定できない。
エ：利用者がどの基準に従うべきか不明確になる。
総合解説：監査では法令・契約・標準・ガイドラインの変更を継続的に把握し、影響評価と統制変更へ結び付ける仕組みを確認する。

対象：2026年度 / 基準日 2026-09-02

0051 リスク管理・コンプライアンス > 個人情報・マイナンバー・GDPR等 ｜ 難易度：基礎

個人情報保護法上、個人情報を取得した場合の利用目的に関する原則として最も適切なものはどれか。

ア．利用目的は事業者内部だけで把握すればよい
イ．取得後は目的を定めなくてもよい
ウ．あらかじめ公表している場合を除き、速やかに利用目的を本人へ通知又は公表する
エ．個人情報であれば必ず無制限に二次利用できる

答え・解説 正答：ウ

ア：本人への通知又は公表が原則として必要である。
イ：利用目的をできる限り特定して取り扱う必要がある。
ウ：個人情報保護法ガイドラインは、取得時の利用目的の通知・公表を定めている。
エ：利用目的による制限がある。
総合解説：監査では利用目的の特定、通知・公表、目的外利用の管理がガイドラインどおり実施されているかを確認する。

対象：2026年度 / 基準日 2026-09-02

0052 リスク管理・コンプライアンス > 個人情報・マイナンバー・GDPR等 ｜ 難易度：基礎

個人データの安全管理措置を監査する際、最も適切な考え方はどれか。

ア．暗号化だけ実施していれば他の管理は不要とする
イ．個人データの重要性に関係なく全て同じ措置とする
ウ．委託先へ渡した個人データは安全管理対象外とする
エ．取扱規程、組織的・人的・物理的・技術的な措置をリスクに応じて総合的に確認する

答え・解説 正答：エ

ア：権限、教育、物理管理等も必要である。
イ：取扱状況・リスクに応じた管理が必要である。
ウ：委託先の監督も必要である。
エ：安全管理は一つの技術対策だけでなく、組織・人・物理・技術の複数面から実施する。
総合解説：個人情報保護委員会ガイドラインに基づき、組織体制、従業者教育、区域・媒体管理、アクセス制御等を確認する。

対象：2026年度 / 基準日 2026-09-02

**0053** リスク管理・コンプライアンス > 個人情報・マイナンバー・GDPR等 ｜ 難易度：基礎

個人データの漏えい等が法令上の報告対象事態に該当する場合の対応として最も適切なものはどれか。

ア．個人情報保護委員会への報告と、原則として本人への通知を適切に行う
イ．社内で隠して外部へ一切報告しない
ウ．全ての事実が確定するまで本人通知を必ず待つ
エ．委託先で発生した場合は委託元に一切関係しない

**答え・解説** 正答：ア

ア：法第26条に基づく報告対象事態では委員会への報告と本人通知が求められる。
イ：法令上の義務に反する可能性がある。
ウ：ガイドラインは状況に応じ速やかな通知を求めている。
エ：委託元・委託先の責任関係を確認する必要がある。
総合解説：監査では報告対象の判定、社内報告、被害拡大防止、原因究明、影響範囲、委員会報告、本人通知のプロセスを確認する。

対象：2026年度 / 基準日 2026-09-02

**0054** リスク管理・コンプライアンス > 個人情報・マイナンバー・GDPR等 ｜ 難易度：標準

特定個人情報の定義として最も適切なものはどれか。

ア．マイナンバーカードそのものだけ
イ．個人番号をその内容に含む個人情報
ウ．企業の法人番号を含む全情報
エ．氏名だけの情報は全て特定個人情報

**答え・解説** 正答：イ

ア：カード以外の媒体にある個人番号を含む個人情報も対象となる。
イ：番号法上、個人番号を含む個人情報は特定個人情報として特別な保護措置の対象となる。
ウ：法人番号は個人番号とは異なる。
エ：個人番号を含まない氏名情報は通常の個人情報であり、特定個人情報とは限らない。
総合解説：監査では通常の個人情報と特定個人情報を区別し、番号法に基づくより厳格な利用・提供・保管管理を確認する。

対象：2026年度 / 基準日 2026-09-02

0055 リスク管理・コンプライアンス > 個人情報・マイナンバー・GDPR等 ｜ 難易度：標準

事業者が従業員の個人番号を取り扱う際、最も適切な原則はどれか。

ア．本人同意があればあらゆるマーケティングに利用できる
イ．社内識別番号として全システムで自由に使う
ウ．法令で認められた個人番号関係事務等の範囲で利用する
エ．便利であれば取引先番号として公開する

答え・解説 正答：ウ

ア：番号法の利用制限は本人同意だけで解除されない。
イ：法定の利用目的を超える利用はできない。
ウ：個人番号は一般の個人情報より利用範囲が限定されている。
エ：個人番号の提供・利用には厳しい制限がある。
総合解説：監査では取得目的、利用事務、アクセス範囲、保管・廃棄が番号法とガイドラインの範囲内かを確認する。

対象：2026年度 / 基準日 2026-09-02

0056 リスク管理・コンプライアンス > 個人情報・マイナンバー・GDPR等 ｜ 難易度：標準

特定個人情報の取扱いで、法定保存期間を経過し個人番号を保管する必要がなくなった場合の管理として最も適切なものはどれか。

ア．念のため永久保存する
イ．アクセス権があれば保存期間は無制限とする
ウ．紙だけ廃棄し電子データは無期限保管する
エ．個人番号をできるだけ速やかに廃棄又は削除する仕組みを運用する

答え・解説 正答：エ

ア：不要な保有は漏えいリスクを高める。
イ：利用・保管の必要性を管理する必要がある。
ウ：媒体を問わず不要な個人番号を適切に削除する必要がある。
エ：必要性がなくなった個人番号を漫然と保持し続けないことが重要である。
総合解説：監査では保存期限を把握し、対象ファイル・バックアップ・紙媒体を含む削除・廃棄手続と記録を確認する。

対象：2026年度 / 基準日 2026-09-02

0057 リスク管理・コンプライアンス > 個人情報・マイナンバー・GDPR等 ｜ 難易度：標準

GDPR第5条の『データ最小化』の考え方として最も適切なものはどれか。

ア．処理目的の達成に必要な範囲へ個人データを限定する
イ．取得可能なデータは将来のため全て収集する
ウ．個人データを永久に保有する
エ．目的を定めず後から自由に利用する

答え・解説 正答：ア

ア：GDPRは個人データが目的に照らして適切・関連し、必要な範囲に限定されることを求めている。
イ：目的に不要な過剰収集はデータ最小化に反する。
ウ：保存制限の原則にも反する可能性がある。
エ：目的制限の原則に反する。
総合解説：監査では目的制限、データ最小化、正確性、保存制限、完全性・機密性、説明責任などGDPRの基本原則を確認する。

対象：2026年度 / 基準日 2026-09-02

0058 リスク管理・コンプライアンス > 個人情報・マイナンバー・GDPR等 ｜ 難易度：標準

GDPRにおける個人データ侵害について、監督機関への通知として最も適切なものはどれか。

ア．全ての侵害は1年以内に報告すればよい
イ．自然人の権利・自由にリスクを生じる可能性がある場合、原則として認識後72時間以内に通知する
ウ．プロセッサは侵害を知ってもコントローラへ連絡しなくてよい
エ．本人への通知と監督機関への通知は常に同一条件である

答え・解説 正答：イ

ア：GDPRの期限と異なる。
イ：GDPR Article 33は、リスクがないと考えられる場合を除き、遅滞なく可能なら72時間以内の通知を求めている。
ウ：プロセッサはコントローラへ不当な遅延なく通知する。
エ：本人通知は高リスク等、条件が異なる。
総合解説：監査では侵害判定、認識時刻、72時間管理、監督機関への通知、必要に応じ本人通知、記録を確認する。

対象：2026年度 / 基準日 2026-09-02

0059 リスク管理・コンプライアンス > 個人情報・マイナンバー・GDPR等 ｜ 難易度：応用

GDPRの下でEEAから第三国へ個人データを移転する際、最も適切な考え方はどれか。

ア．インターネット経由なら国際移転規制は適用されない
イ．本人データなら自由に第三国へ移転できる
ウ．十分性認定又は標準契約条項等の適切な移転根拠・保護措置を確認する
エ．クラウド事業者が有名企業なら移転条件を確認しなくてよい

答え・解説 正答：ウ

ア：保存・受領場所や処理主体に応じて評価が必要である。
イ：移転根拠と保護措置が必要である。
ウ：GDPR Chapter Vは第三国移転で保護水準が損なわれないための条件を定めている。
エ：サービス提供者の知名度は法的根拠の代替にならない。
総合解説：監査ではデータフロー、移転先国、十分性認定、SCC、BCR等の根拠と補完措置を確認する。

対象：2026年度 / 基準日 2026-09-02

0060 リスク管理・コンプライアンス > 個人情報・マイナンバー・GDPR等 ｜ 難易度：応用

日本企業が個人情報・マイナンバー・GDPRを横断的に監査する際、最も適切な進め方はどれか。

ア．全データに一つの法律だけを適用する
イ．マイナンバーと一般の個人情報を同じ利用範囲とみなす
ウ．海外拠点の処理を監査対象外とする
エ．データ種類・対象者・処理目的・所在・移転先を整理し、各法令の適用関係をデータフロー単位で確認する

答え・解説 正答：エ

ア：法域・データ種類によって適用関係が異なる。
イ：番号法には特別な利用制限がある。
ウ：GDPR等の域外適用や国際移転を検討する必要がある。
エ：同じシステムでもデータ種類や対象者、処理場所により異なる法令が関係する。
総合解説：監査ではデータマッピングを行い、APPI、番号法、GDPR等の義務を処理活動へ対応付け、重複・差異を管理する。

対象：2026年度 / 基準日 2026-09-02

0061 情報セキュリティ監査 > 認証・アクセス制御・権限管理 ｜ 難易度：基礎

アクセス制御の基本原則として最も適切なものはどれか。

ア．利用者には業務上必要な最小限の権限だけを付与する
イ．全利用者に管理者権限を付与する
ウ．一度付与した権限は退職まで見直さない
エ．権限付与理由を記録しない

答え・解説 正答：ア

ア：最小権限の原則により、誤操作やアカウント侵害時の影響範囲を抑える。
イ：不要な高権限はリスクを高める。
ウ：異動や業務変更に応じた見直しが必要である。
エ：承認・妥当性を追跡できない。
総合解説：監査では、権限が職務に必要な範囲か、承認されているか、定期レビューされているかを確認する。

対象：2026年度 / 基準日 2026-09-02

0062 情報セキュリティ監査 > 認証・アクセス制御・権限管理 ｜ 難易度：基礎

管理者向けポータルに多要素認証を導入する場合、異なる認証要素を組み合わせた例はどれか。

ア．異なる二つのパスワードを入力する
イ．パスワードと認証アプリによるワンタイムコードを組み合わせる
ウ．同じ指紋を二回読み取る
エ．ユーザIDとメールアドレスを入力する

答え・解説 正答：イ

ア：どちらも知識要素であり、要素の種類は増えていない。
イ：知識要素と所持要素という異なる種類の認証要素を組み合わせている。
ウ：同一の生体要素を繰り返している。
エ：一般にいずれも本人だけが保有する認証要素とはいえない。
総合解説：重要システムや特権アクセスでは、パスワード単独より複数要素を用いた認証により不正利用リスクを低減できる。

対象：2026年度 / 基準日 2026-09-02

0063 情報セキュリティ監査 > 認証・アクセス制御・権限管理 ｜ 難易度：基礎

入社・異動・退職に伴う権限管理を監査する際、最も適切な確認はどれか。

ア．退職後もアカウントを予備として残す
イ．異動前の権限を追加したまま新権限も付与する
ウ．人事イベントとアカウントの作成・変更・無効化が適時に連動しているか
エ．権限変更を口頭だけで実施する

答え・解説 正答：ウ

ア：不正利用のリスクがある。
イ：権限蓄積が起こる。
ウ：利用者ライフサイクルと権限管理が連携していないと不要権限が残存する。
エ：承認と追跡性が不足する。
総合解説：監査では入社・異動・退職データとアカウント台帳を突合し、不要ID・過剰権限・処理遅延を確認する。

対象：2026年度 / 基準日 2026-09-02

0064 情報セキュリティ監査 > 認証・アクセス制御・権限管理 ｜ 難易度：標準

特権IDの監査で最も適切な証拠の組合せはどれか。

ア．管理者の自己申告だけ
イ．特権IDの名称一覧だけ
ウ．システムの性能ログだけ
エ．特権ID台帳、付与承認、利用ログ、定期レビュー記録

答え・解説 正答：エ

ア：客観的な運用証拠が不足する。
イ：付与の妥当性や利用状況を確認できない。
ウ：特権アクセスの適正性を直接評価できない。
エ：特権IDは付与から利用・見直しまで一連の統制を証拠で確認する必要がある。
総合解説：高権限アカウントは個人識別、申請承認、利用目的、操作ログ、定期棚卸、緊急利用を重点的に監査する。

対象：2026年度 / 基準日 2026-09-02

0065 情報セキュリティ監査 > 認証・アクセス制御・権限管理 ｜ 難易度：標準

共有IDの利用に関する主な監査上の問題はどれか。

ア．操作した個人を特定しにくく、説明責任と追跡性が低下する
イ．必ず処理性能が低下する
ウ．パスワードが不要になる
エ．データベースが自動的に破損する

答え・解説 正答：ア

ア：共有IDは誰が操作したかの特定を困難にするため、原則として個人IDの利用が望ましい。
イ：共有IDの主な問題ではない。
ウ：通常は認証情報を使用する。
エ：直接的な因果関係はない。
総合解説：やむを得ず共有IDを使う場合は利用者限定、追加認証、貸出記録、詳細ログ等で追跡性を補う必要がある。

対象：2026年度 / 基準日 2026-09-02

0066 情報セキュリティ監査 > 認証・アクセス制御・権限管理 ｜ 難易度：標準

ロールベースアクセス制御（RBAC）の主な利点はどれか。

ア．全利用者を同じロールにする
イ．職務に対応するロールへ権限をまとめ、利用者の権限付与・見直しを一貫して管理しやすい
ウ．権限レビューが不要になる
エ．職務分掌を考慮しなくてよい

答え・解説 正答：イ

ア：職務に応じたアクセス制御にならない。
イ：個別権限の直接付与を減らし、職務と権限の対応を標準化できる。
ウ：ロール自体と利用者への割当てを定期的に見直す必要がある。
エ：競合ロールの組合せ管理が必要である。
総合解説：監査ではロール定義、ロール所有者、職務との対応、競合権限、例外付与、定期レビューを確認する。

対象：2026年度 / 基準日 2026-09-02

0067 情報セキュリティ監査 > 認証・アクセス制御・権限管理 ｜ 難易度：標準

定期的なアクセス権レビューで最も適切な方法はどれか。

ア．情報システム部門だけが業務内容を確認せず承認する

イ．レビュー結果を記録しない

ウ．権限の業務上の必要性を判断できる責任者が、利用者・ロール・特権権限を確認し不要権限を削除する

エ．全権限を自動継続する

答え・解説 正答：ウ

ア：業務上の必要性を判断できない場合がある。

イ：実施証跡と是正状況を確認できない。

ウ：単に一覧を配布するだけでなく、業務責任者による妥当性判断と是正が必要である。

エ：レビューの意味がない。

総合解説：監査ではレビュー対象の網羅性、責任者、頻度、例外、削除完了までの追跡を確認する。

対象：2026年度 / 基準日 2026-09-02

0068 情報セキュリティ監査 > 認証・アクセス制御・権限管理 ｜ 難易度：標準

緊急時に一時的な高権限を付与する仕組みで最も重要な統制はどれか。

ア．緊急権限は期限を設定しない

イ．利用ログを無効にする

ウ．誰でも自己承認できる

エ．利用目的を承認し、時間制限を設け、操作ログを記録し、事後レビューする

答え・解説 正答：エ

ア：不要権限が残存する。

イ：不正や誤操作を追跡できない。

ウ：相互牽制が機能しない。

エ：緊急アクセスは必要性がある一方、通常統制を迂回するため厳格な補完統制が必要である。

総合解説：いわゆるブレークグラス権限は、限定的な付与、強い認証、短い有効期限、全操作記録、事後承認・レビューが重要である。

対象：2026年度 / 基準日 2026-09-02

0069 情報セキュリティ監査 > 認証・アクセス制御・権限管理 ｜ 難易度：応用

認証ログの監査で、短時間に多数の失敗後に成功ログインが発生している。最も適切な対応はどれか。

ア．ブルートフォース等の可能性を踏まえ、送信元・対象ID・成功後の操作を追加分析する
イ．成功ログインなので問題なしとする
ウ．ログを削除して容量を空ける
エ．全利用者のアカウントを無条件に削除する

答え・解説 正答：ア

ア：認証失敗の集中と成功の組合せは攻撃兆候となり得るため、文脈を確認する。
イ：侵害後の成功である可能性がある。
ウ：証拠と検知情報を失う。
エ：影響評価なしの過剰対応である。
総合解説：監査では認証失敗回数、ロックアウト、MFA、地理的・時間的異常、成功後の特権操作などを分析する。

対象：2026年度 / 基準日 2026-09-02

0070 情報セキュリティ監査 > 認証・アクセス制御・権限管理 ｜ 難易度：応用

アクセス制御監査で、職務分掌違反を効率的に検出する方法として最も適切なものはどれか。

ア．利用者名の先頭一文字だけを見る
イ．利用者とロールの全件データを分析し、競合権限ルールに該当する組合せを抽出する
ウ．無作為に一人だけ確認する
エ．権限表を印刷するだけで分析しない

答え・解説 正答：イ

ア：権限競合を判断できない。
イ：CAATによる権限データ分析は大量利用者のSoD違反を効率的に検出できる。
ウ：重要な競合を見逃す可能性が高い。
エ：競合ルールとの照合が必要である。
総合解説：利用者、ロール、権限、所属、承認情報を結合し、自己承認や申請・支払など競合する権限を全件検索する。

対象：2026年度 / 基準日 2026-09-02

0071 情報セキュリティ監査 > 脆弱性・攻撃・インシデント対応 ｜ 難易度：基礎

脆弱性管理の基本的な流れとして最も適切なものはどれか。

ア．脆弱性診断を一度実施すれば以後不要とする
イ．資産台帳がなくても全て把握できるとする
ウ．資産把握、脆弱性情報の収集・検出、リスク評価、対応、再確認を継続する
エ．パッチ適用後の確認を行わない

答え・解説 正答：ウ

ア：新たな脆弱性は継続的に発見される。
イ：対象漏れが起こりやすい。
ウ：脆弱性管理は一度の診断ではなく、資産と脅威の変化に応じた継続的プロセスである。
エ：適用失敗や残存脆弱性を見逃す。
総合解説：監査では対象資産、情報源、診断頻度、優先順位、パッチ・代替策、再スキャン、例外管理を確認する。

対象：2026年度 / 基準日 2026-09-02

0072 情報セキュリティ監査 > 脆弱性・攻撃・インシデント対応 ｜ 難易度：基礎

脆弱性対応の優先順位付けで最も適切な考え方はどれか。

ア．CVSSが低ければ必ず対応不要とする
イ．全脆弱性を同じ期限で処理する
ウ．インターネット公開の有無を無視する
エ．技術的深刻度に加え、対象資産の重要性、外部公開状況、悪用情報、代替統制を考慮する

答え・解説 正答：エ

ア：重要資産や実悪用状況によっては優先対応が必要である。
イ：リスクに応じた優先度設定が必要である。
ウ：攻撃可能性に大きく影響する。
エ：脆弱性スコアだけでは組織固有のリスクを十分に評価できない。
総合解説：監査では組織が技術情報と事業コンテキストを組み合わせ、リスクベースで対応期限を決めているかを確認する。

対象：2026年度 / 基準日 2026-09-02

0073 情報セキュリティ監査 > 脆弱性・攻撃・インシデント対応 ｜ 難易度：基礎

脆弱性診断とペネトレーションテストの関係として最も適切なものはどれか。

ア．脆弱性診断は弱点の発見・評価を広く行い、ペネトレーションテストは想定攻撃経路を実際に検証する性格が強い

イ．両者は必ず完全に同じ作業である

ウ．ペネトレーションテストは許可なく本番へ実施する

エ．脆弱性診断は資産情報を一切必要としない

答え・解説 正答：ア

ア：目的・範囲・方法が異なるため、監査目的に応じて使い分ける。
イ：侵入試験は攻撃シナリオの実証を含む場合がある。
ウ：業務影響があるため範囲と承認が必要である。
エ：対象範囲を明確にする必要がある。
総合解説：監査では診断・侵入試験の目的、対象、実施権限、業務影響、結果フォローが適切かを確認する。

対象：2026年度 / 基準日 2026-09-02

0074 情報セキュリティ監査 > 脆弱性・攻撃・インシデント対応 ｜ 難易度：標準

ランサムウェア感染が疑われる端末を発見した従業員の初動として、証拠保全と被害拡大防止の観点から最も適切なものはどれか。

ア．不審ファイルを全て削除して証拠を消す

イ．定めた手順に従いネットワークから隔離し、むやみにファイル削除や電源断をせずCSIRT等へ報告する

ウ．調査せず業務を続ける

エ．自己判断で初期化する

答え・解説 正答：イ

ア：原因調査に必要な証拠を失う。
イ：IPAの2026年プラクティスでは、証拠保全が必要な事案でネットワーク切断、メール・ファイルを削除しない、PCの電源を切らない等を例示している。
ウ：被害拡大のおそれがある。
エ：証拠消失と影響範囲の把握困難につながる。
総合解説：初動は組織の手順と専門家の指示に従い、封じ込めと証拠保全を両立させる必要がある。

対象：2026年度 / 基準日 2026-09-02

0075 情報セキュリティ監査 > 脆弱性・攻撃・インシデント対応 ｜ 難易度：標準

CSIRTを整備する主な目的として最も適切なものはどれか。

ア．全てのシステム開発をCSIRTが担当する
イ．事故が発生した場合だけ臨時に責任者を探す
ウ．インシデントの検知・報告・封じ込め・復旧を組織横断で調整する司令塔を確保する
エ．社外への説明を禁止する

答え・解説 正答：ウ

ア：CSIRTの主目的ではない。
イ：初動が遅れる。
ウ：迅速な対応には役割・連絡先・意思決定経路を平時から定めておく必要がある。
エ：必要な法令報告・顧客連絡等を適切に行う体制が必要である。
総合解説：IPAは影響範囲・損害の特定、被害拡大防止、再発防止を適時に行うためCSIRT等の体制整備を求めている。

対象：2026年度 / 基準日 2026-09-02

0076 情報セキュリティ監査 > 脆弱性・攻撃・インシデント対応 ｜ 難易度：標準

インシデント対応訓練を監査する際、最も適切な確認はどれか。

ア．毎回同じ簡単なシナリオで課題を記録しない
イ．訓練結果を関係者へ共有しない
ウ．経営層が関係する重大事故でも技術部門だけで訓練する
エ．想定シナリオに対して連絡・意思決定・技術対応・外部報告を実践し、課題を改善しているか

答え・解説 正答：エ

ア：能力向上につながりにくい。
イ：改善が組織へ反映されない。
ウ：経営判断・広報・法務等も含む必要がある。
エ：訓練は手順書の存在確認だけでなく、実際に機能するかを検証するために行う。
総合解説：監査では訓練頻度、現実性、参加部門、評価基準、発見課題、手順改訂までのフォローを確認する。

対象：2026年度 / 基準日 2026-09-02

0077 情報セキュリティ監査 > 脆弱性・攻撃・インシデント対応 ｜ 難易度：標準

**インシデント発生後の『封じ込め』の主な目的はどれか。**

ア．攻撃や被害の拡大を抑え、影響範囲を制限する
イ．全ての原因分析を完了すること
ウ．平常サービスを完全復旧すること
エ．証拠を全て削除すること

答え・解説 正答：ア

ア：感染端末の隔離や不正通信の遮断などにより被害拡大を防ぐ段階である。
イ：原因分析は並行・後続して行われる。
ウ：復旧は封じ込め後の段階である。
エ：証拠保全に反する。
総合解説：IPAの実践例では検知、報告、封じ込め、復旧という流れを示し、封じ込めでネットワーク遮断等の暫定対応を行う。

対象：2026年度 / 基準日 2026-09-02

0078 情報セキュリティ監査 > 脆弱性・攻撃・インシデント対応 ｜ 難易度：標準

**パッチを直ちに適用できない重要システムの脆弱性に対する最も適切な対応はどれか。**

ア．対応不能として記録もせず放置する
イ．リスクを評価し、アクセス制限やWAF等の代替統制を実施して期限付きで例外管理する
ウ．テストせず本番へ必ず即時適用する
エ．脆弱性情報を削除する

答え・解説 正答：イ

ア：残存リスクを管理できない。
イ：業務制約があってもリスクを放置せず、代替策と正式な例外承認を行う。
ウ：可用性に重大な影響を与える可能性がある。
エ：リスクそのものは消えない。
総合解説：監査では例外理由、リスク所有者、代替策、監視、再評価日、恒久対応期限を確認する。

対象：2026年度 / 基準日 2026-09-02

0079 情報セキュリティ監査 > 脆弱性・攻撃・インシデント対応 ｜ 難易度：応用

**サプライチェーン経由のサイバー攻撃へ備える監査で最も適切な着眼点はどれか。**

ア．自社境界内だけを監査し委託先を無視する

イ．委託先は有名企業なら評価不要とする

ウ．委託先・ソフトウェア供給者を含む依存関係を把握し、契約・アクセス・事故連絡・継続対応を管理しているか

エ．事故連絡条件を契約に定めない

答え・解説 正答：ウ

ア：重要な攻撃経路を見逃す。

イ：組織固有の依存リスクを評価する必要がある。

ウ：自組織外の弱点が攻撃経路となるため、サプライチェーン全体のリスク管理が必要である。

エ：初動が遅れる可能性がある。

総合解説：監査では重要委託先の選定・評価、セキュリティ要件、再委託、アクセス、インシデント連携、代替手段等を確認する。

対象：2026年度 / 基準日 2026-09-02

0080 情報セキュリティ監査 > 脆弱性・攻撃・インシデント対応 ｜ 難易度：応用

**インシデント対応後の再発防止で最も適切な活動はどれか。**

ア．復旧したら記録を全て削除する

イ．担当者個人の注意だけを求める

ウ．同じ事故が起きるまで手順を変更しない

エ．原因・影響・対応の有効性を振り返り、統制・手順・教育・リスク評価を更新する

答え・解説 正答：エ

ア：学習と証拠を失う。

イ：根本原因や仕組みの改善が不足する。

ウ：継続的改善にならない。

エ：復旧だけで終了せず、得られた教訓を組織の統制へフィードバックする。

総合解説：監査ではポストインシデントレビュー、原因分析、再発防止策、責任者・期限、訓練やリスク登録簿への反映を確認する。

対象：2026年度 / 基準日 2026-09-02

0081 情報セキュリティ監査 > 不正調査・デジタルフォレンジックス ｜ 難易度：基礎

デジタル・フォレンジックの説明として最も適切なものはどれか。

ア．インシデントや法的紛争に関連する電磁的記録を保全し、調査・分析する科学的手法・技術

イ．障害端末を最短時間で初期化する作業だけ

ウ．ネットワーク性能を最適化する技術

エ．全ての不正を自動判定するAIの名称

答え・解説 正答：ア

ア：デジタルフォレンジックは電磁的証拠の保全、調査、分析を通じて事実関係の解明を支援する。

イ：証拠保全・分析が中心であり初期化は証拠を失う場合がある。

ウ：主目的が異なる。

エ：特定のAI製品を意味しない。

総合解説：IPAの情報セキュリティサービス基準における定義でも、電磁的記録の証拠保全、調査・分析、改ざん・毀損等の分析を含む。

対象：2026年度 / 基準日 2026-09-02

0082 情報セキュリティ監査 > 不正調査・デジタルフォレンジックス ｜ 難易度：基礎

電磁的証拠を保全する際に最も重要な考え方はどれか。

ア．分析しやすいよう原本を直接編集する

イ．取得したデータが元データと同一であり、作業中に不適切な変更がないことを説明できるようにする

ウ．取得手順を記録しない

エ．証拠を担当者の個人端末だけに保存する

答え・解説 正答：イ

ア：証拠の状態を変えてしまう。

イ：証拠の原本同一性に疑義が生じると、その後の分析結果の信頼性が低下する。

ウ：同一性・信頼性を説明できない。

エ：管理・完全性・秘密保持に問題がある。

総合解説：証拠保全では取得方法、日時、担当者、対象、ハッシュ等を記録し、原本又は保全コピーの完全性を確認できるようにする。

対象：2026年度 / 基準日 2026-09-02

**0083** 情報セキュリティ監査 > 不正調査・デジタルフォレンジックス ｜ 難易度：基礎

ディスクのフォレンジックコピーを取得する際、書込み防止機能を利用する主な理由はどれか。

ア．コピー速度を必ず倍にするため
イ．暗号化を自動解除するため
ウ．証拠媒体への意図しない書込みを防ぎ、原本の状態変化を抑えるため
エ．証拠媒体の容量を増やすため

**答え・解説** 正答：ウ

ア：主目的ではない。
イ：書込み防止機能の役割ではない。
ウ：証拠取得作業自体が原本へ変更を加えないようにすることが重要である。
エ：容量には影響しない。
総合解説：監査・不正調査では、適切な証拠保全装置や手順を使用し、取得前後の状態と作業内容を記録する。

対象：2026年度 / 基準日 2026-09-02

**0084** 情報セキュリティ監査 > 不正調査・デジタルフォレンジックス ｜ 難易度：標準

Chain of Custody（CoC）を記録する主な目的はどれか。

ア．証拠の内容を自動的に暗号化するため
イ．分析結果を必ず有罪判定にするため
ウ．証拠を自由に共有するため
エ．証拠を誰がいつ取得・保管・移送・受渡ししたかを連続的に追跡するため

**答え・解説** 正答：エ

ア：CoCは管理履歴であり暗号化機能ではない。
イ：証拠管理と結論は別である。
ウ：むしろ管理された受渡しを記録する。
エ：証拠の管理履歴を残すことで、紛失・改ざんの疑いを抑え信頼性を説明しやすくなる。
総合解説：IDFガイドラインにはCoCシート例があり、証拠の取扱者・時刻・場所・受渡しを追跡可能にする。

対象：2026年度 / 基準日 2026-09-02

0085 情報セキュリティ監査 > 不正調査・デジタルフォレンジックス ｜ 難易度：標準

不正アクセス調査で端末の揮発性メモリに重要情報が残っている可能性がある。最も適切な考え方はどれか。

ア．電源操作で消失する情報があることを踏まえ、専門手順に従い必要な揮発性データの取得を検討する

イ．必ず最初に電源を切る

ウ．メモリ情報は証拠にならない

エ．取得前に端末を通常利用へ戻す

答え・解説 正答：ア

ア：メモリ上のプロセスや通信情報などは電源断で失われる可能性がある。
イ：揮発性証拠を失う可能性がある。
ウ：重要な調査情報となり得る。
エ：状態を大きく変化させる可能性がある。
総合解説：初動時は被害拡大防止と証拠保全を両立させ、対象の状態に応じて専門家が取得順序・方法を判断する。

対象：2026年度 / 基準日 2026-09-02

0086 情報セキュリティ監査 > 不正調査・デジタルフォレンジックス ｜ 難易度：標準

フォレンジック分析を原本媒体ではなく検証済みコピーで行う主な理由はどれか。

ア．コピーならハッシュ確認は不要になる

イ．原本の状態を保護し、分析作業による変更リスクを避けるため

ウ．原本は取得後すぐ廃棄してよい

エ．コピーでは分析結果が必ず異なる

答え・解説 正答：イ

ア：コピーの同一性確認が必要である。
イ：原本又は一次保全物を保護し、同一性を確認したコピーで分析することで証拠信頼性を維持しやすい。
ウ：証拠管理方針に従い適切に保管する。
エ：正しく取得・検証されたコピーなら同一データを分析できる。
総合解説：取得・保全・分析の役割を分け、原本を保護しながら再現可能な分析を行うことが望ましい。

対象：2026年度 / 基準日 2026-09-02

0087 情報セキュリティ監査 > 不正調査・デジタルフォレンジックス ｜ 難易度：標準

不正調査で収集したログの時刻がサーバごとに大きくずれていた。最も直接的な問題はどれか。

ア．ログ容量が必ず不足する
イ．暗号鍵が自動的に失効する
ウ．複数システムの事象を時系列で正確に関連付けることが難しくなる
エ．全ログが法的に無効になると自動判定される

答え・解説 正答：ウ

ア：時刻ずれと容量は直接関係しない。
イ：通常そのような関係はない。
ウ：インシデントの流れを復元するにはログ時刻の整合性が重要である。
エ：証拠価値は状況に応じ評価されるが、時刻ずれは分析上重大な問題である。
総合解説：監査では平時から時刻同期、ログ源、タイムゾーン、保持期間を管理し、調査時に補正根拠を記録できるかを確認する。

対象：2026年度 / 基準日 2026-09-02

0088 情報セキュリティ監査 > 不正調査・デジタルフォレンジックス ｜ 難易度：標準

クラウド環境のフォレンジック準備として最も適切なものはどれか。

ア．事故発生後に初めてログの有無を調べればよい
イ．クラウド事業者が全証拠を自動保存すると仮定する
ウ．利用者側の権限設計を確認しない
エ．必要ログの種類・保存期間・取得権限・取得方法を平時から確認し、責任分界を明確にする

答え・解説 正答：エ

ア：既に保持期間を過ぎている可能性がある。
イ：サービス・設定により取得可能性は異なる。
ウ：証拠取得に必要なロールが不足することがある。
エ：クラウドでは事後に取得できないログがあるため、インシデント前の準備が特に重要である。
総合解説：第10版の参考情報では責任共有、ログ取得、保持期間、権限、時刻同期、設定保護等を事前に検討する重要性を示している。

対象：2026年度 / 基準日 2026-09-02

0089 情報セキュリティ監査 > 不正調査・デジタルフォレンジックス ｜ 難易度：応用

デジタル証拠を外部フォレンジック事業者へ引き渡す際、最も適切な対応はどれか。

ア．対象物・状態・ハッシュ等を確認し、受渡し日時・担当者を記録して管理する
イ．口頭で渡して記録を残さない
ウ．証拠を通常宅配で無管理に送る
エ．委託後は組織側で証拠管理を確認しない

答え・解説 正答：ア

ア：外部委託しても証拠の連続的な管理と同一性を維持する必要がある。
イ：Chain of Custodyが途切れる。
ウ：紛失・改ざん・秘密漏えいリスクがある。
エ：委託元として管理状況を把握する必要がある。
総合解説：フォレンジック委託では秘密保持、輸送、保管、CoC、分析範囲、成果物、返却・廃棄を契約・手順で管理する。

対象：2026年度 / 基準日 2026-09-02

0090 情報セキュリティ監査 > 不正調査・デジタルフォレンジックス ｜ 難易度：応用

不正調査でデジタル証拠を保全した後、分析結果の再現性を高めるため最も重要な記録はどれか。

ア．結論だけを記録する
イ．使用ツール・バージョン、分析条件、対象データ、実施者、日時、結果へ至る手順
ウ．使用ツール名を意図的に隠す
エ．途中の分析条件を毎回変更して記録しない

答え・解説 正答：イ

ア：どのように結論へ至ったか検証できない。
イ：分析プロセスを記録することで第三者レビューや再分析が可能になる。
ウ：再現性が低下する。
エ：結果の信頼性を確認できない。
総合解説：証拠保全だけでなく、検査・分析・報告の各段階で作業内容と判断根拠を記録し、追跡可能にする。

対象：2026年度 / 基準日 2026-09-02

0091 データ・AI・先端技術監査 > データ品質・データガバナンス ｜ 難易度：基礎

**複数部門が顧客データを独自管理している企業で、全社データガバナンスの監査を始める際に最も優先して確認すべきものはどれか。**

ア．データ件数が多いほどガバナンスが有効と判断する

イ．データ管理を各担当者の個人的判断に任せる

ウ．重要データについて責任者、利用目的、品質基準、アクセス、変更、保存・廃棄のルールが組織的に定められているか

エ．データの利用目的を定めず自由利用を認める

答え・解説 正答：ウ

ア：件数だけでは責任、品質、統制の有効性を評価できない。

イ：組織横断で一貫した責任とルールが必要である。

ウ：データガバナンスでは、データを価値ある資産として活用しつつ、責任・統制・リスク管理を明確にする必要がある。

エ：目的外利用や法令違反、品質問題のリスクが高まる。

総合解説：監査ではデータ所有者・管理責任、方針、品質、セキュリティ、ライフサイクル、利用状況のモニタリングが整備されているかを確認する。

対象：2026年度 / 基準日 2026-09-02

0092 データ・AI・先端技術監査 > データ品質・データガバナンス ｜ 難易度：基礎

**データ品質の『完全性』を評価する例として最も適切なものはどれか。**

ア．値が最新時点を反映しているか確認する

イ．同じ顧客が重複登録されていないか確認する

ウ．値が業務ルール上正しいか確認する

エ．必須項目の欠損や、本来存在すべきレコードの欠落がないか確認する

答え・解説 正答：エ

ア：主に適時性・最新性の観点である。

イ：主に一意性・重複の観点である。

ウ：主に正確性・妥当性の観点である。

エ：完全性は必要なデータが欠けずに存在しているかという品質観点である。

総合解説：データ品質監査では、正確性、完全性、一貫性、適時性、一意性などを利用目的に応じて評価する。

対象：2026年度 / 基準日 2026-09-02

0093 データ・AI・先端技術監査 > データ品質・データガバナンス ｜ 難易度：基礎

**複数システムで同じ顧客に異なる住所が登録されている。最も直接的なデータ品質上の問題はどれか。**

ア．システム間の一貫性が確保されていない
イ．可用性が必ず低下している
ウ．暗号化方式が不適切である
エ．データ件数が不足している

答え・解説 正答：ア

ア：同一対象について矛盾する値が存在する場合、データの一貫性に問題がある。
イ：住所不一致から可用性低下は直接導けない。
ウ：品質の矛盾とは別問題である。
エ：件数ではなく値の整合性が問題である。
総合解説：監査ではマスターデータの正本、同期ルール、更新順序、エラー処理を確認し、矛盾が発生・放置されない仕組みを評価する。

対象：2026年度 / 基準日 2026-09-02

0094 データ・AI・先端技術監査 > データ品質・データガバナンス ｜ 難易度：標準

**データリネージュを整備する主な目的はどれか。**

ア．データを必ず匿名化するため
イ．データがどこから取得され、どの処理・変換を経て、どこで利用されるかを追跡できるようにする
ウ．データ保存容量を削減するため
エ．利用者認証を代替するため

答え・解説 正答：イ

ア：リネージュの主目的ではない。
イ：データリネージュはデータの由来と変換経路を可視化し、品質問題や利用影響の分析に役立つ。
ウ：追跡性の確保が主目的である。
エ：アクセス制御とは別の仕組みである。
総合解説：監査では重要レポートやAI入力データについて、取得元、変換ロジック、中間処理、出力先を追跡できるかを確認する。

対象：2026年度 / 基準日 2026-09-02

0095 データ・AI・先端技術監査 > データ品質・データガバナンス ｜ 難易度：標準

**複数の業務システムで顧客コード体系がばらばらになっている。データガバナンス上、最も適切な改善はどれか。**

ア．各システムが独自に同じマスターを自由編集する
イ．変更履歴を残さない
ウ．正本となるデータ源を定め、変更権限・承認・配信・重複統合のルールを管理する
エ．重複レコードを無条件に残す

答え・解説 正答：ウ

ア：不整合が発生しやすい。
イ：誤変更の原因追跡が困難になる。
ウ：マスターデータは複数システムの処理基準となるため、正本と変更統制が重要である。
エ：同一対象の識別や集計に影響する。
総合解説：監査ではデータオーナー、正本、コード体系、変更承認、配信、同期、例外・重複管理を確認する。

対象：2026年度 / 基準日 2026-09-02

0096 データ・AI・先端技術監査 > データ品質・データガバナンス ｜ 難易度：標準

**経営ダッシュボードの数値について、元データから集計結果まで追跡できない。最も重要な監査上の問題はどれか。**

ア．ダッシュボードの色が統一されていない
イ．データ量が多すぎることだけが問題である
ウ．必ず不正が行われている
エ．経営判断に用いる数値の根拠と変換過程を検証できず、信頼性を評価しにくい

答え・解説 正答：エ

ア：表示デザインより数値の信頼性が重要である。
イ：量そのものではなく追跡不能が主問題である。
ウ：追跡不能は統制不備だが不正と即断はできない。
エ：重要な意思決定データは、出所・変換・集計の追跡性が必要である。
総合解説：監査ではデータソース、ETL、計算式、手修正、承認、版管理を確認し、経営数値が再現可能かを検証する。

対象：2026年度 / 基準日 2026-09-02

0097 データ・AI・先端技術監査 > データ品質・データガバナンス ｜ 難易度：標準

**データ品質ルールを設定する際、最も適切な考え方はどれか。**

ア．データの利用目的と業務上の重要性に応じて、測定可能な品質基準と許容水準を定める
イ．全データに同じ品質水準を無条件で要求する
ウ．品質基準を定めず問題発生時だけ対応する
エ．利用者ごとに非公開の独自基準を持つ

答え・解説 正答：ア

ア：データ品質は利用文脈に依存するため、目的とリスクに応じた基準が必要である。
イ：コストと重要性を考慮できない。
ウ：継続的な品質管理にならない。
エ：組織的な比較・改善が難しい。
総合解説：監査では品質指標、閾値、測定頻度、責任者、逸脱時対応が定められ、重要データへ優先適用されているかを確認する。

対象：2026年度 / 基準日 2026-09-02

0098 データ・AI・先端技術監査 > データ品質・データガバナンス ｜ 難易度：標準

**データ品質の問題が繰り返し発生している場合、最も適切な改善はどれか。**

ア．毎回出力時に手修正だけ行う
イ．個々の誤データ修正だけでなく、発生源・入力工程・変換処理の根本原因を分析して統制を改善する
ウ．品質問題を利用部門だけの責任にする
エ．問題データを削除して原因を記録しない

答え・解説 正答：イ

ア：再発を防げない。
イ：品質問題を持続的に減らすには、原因工程へ対策を入れる必要がある。
ウ：発生源やデータ管理プロセスも評価すべきである。
エ：改善に必要な情報が失われる。
総合解説：監査では品質インシデントの記録、原因分析、是正措置、再発確認が品質マネジメントへ組み込まれているかを見る。

対象：2026年度 / 基準日 2026-09-02

0099 データ・AI・先端技術監査 > データ品質・データガバナンス ｜ 難易度：応用

外部データをAI学習に利用する際、データガバナンス上最も適切な確認はどれか。

ア．入手できれば利用条件を確認せず使う
イ．データ件数だけで品質を判断する
ウ．出所、利用権限、品質、偏り、更新時点、利用条件を確認し、採用判断を記録する
エ．提供者が有名なら検証を省略する

答え・解説 正答：ウ

ア：契約・知的財産・個人情報等の問題があり得る。
イ：大量でも偏りや誤りがある場合がある。
ウ：外部データは品質・権利・来歴の不確実性があるため、利用前評価が重要である。
エ：目的適合性と品質評価は必要である。
総合解説：監査ではデータのプロベナンス、権利、品質評価、バージョン、更新、使用範囲を確認し、AIの信頼性への影響を評価する。

対象：2026年度 / 基準日 2026-09-02

0100 データ・AI・先端技術監査 > データ品質・データガバナンス ｜ 難易度：応用

データ品質を継続的に監視する仕組みとして最も適切なものはどれか。

ア．年に一度データ件数だけ確認する
イ．品質エラーを記録せず都度修正する
ウ．品質監視をシステム運用から切り離して担当者の記憶に任せる
エ．重要データの品質指標を定期測定し、閾値逸脱を責任者へ通知して是正状況を追跡する

答え・解説 正答：エ

ア：重要な品質問題を早期検知できない。
イ：傾向分析や再発防止ができない。
ウ：継続性と証跡が不足する。
エ：持続的なデータ品質には測定・検知・是正・再評価のサイクルが必要である。
総合解説：監査では品質KPI、検知ルール、エスカレーション、是正期限、再測定が定常業務として運用されているかを確認する。

対象：2026年度 / 基準日 2026-09-02

0101 データ・AI・先端技術監査 > AI・生成AI・モデル／利用リスク ｜ 難易度：基礎

AIガバナンスを監査する際、最も重要な確認はどれか。

ア．AIの利用目的、責任者、リスク評価、承認、監視、問題発生時の対応がライフサイクルを通じて管理されているか

イ．AIを導入した件数だけを確認する

ウ．モデル開発者だけに全責任を置く

エ．本番導入後は評価を行わない

答え・解説 正答：ア

ア：AIガバナンスでは導入時だけでなく、開発・提供・利用・運用中の継続的なリスク管理が必要である。

イ：導入量は安全性・適切性を示さない。

ウ：提供者・利用者など各主体の役割もある。

エ：環境・データ・モデル性能の変化を監視する必要がある。

総合解説：AI事業者ガイドラインはリスクベースの取組と、各主体によるガバナンス・安全性・透明性等の確保を求めている。

対象：2026年度 / 基準日 2026-09-02

0102 データ・AI・先端技術監査 > AI・生成AI・モデル／利用リスク ｜ 難易度：基礎

生成AIの『ハルシネーション』に対する統制として最も適切なものはどれか。

ア．AI出力は常に正しいと利用者へ周知する

イ．重要な判断に使う出力は根拠資料と照合し、人による確認を必須にする

ウ．出典確認を禁止する

エ．高リスク業務でも自動出力を無審査で確定する

答え・解説 正答：イ

ア：誤情報リスクを高める。

イ：生成AIは事実と異なる内容を生成する可能性があるため、用途に応じた検証が必要である。

ウ：信頼性検証ができない。

エ：人の監督や追加検証が必要である。

総合解説：監査では利用場面の重要度に応じて、出典参照、検索連携、人手レビュー、利用制限等が設計されているかを見る。

対象：2026年度 / 基準日 2026-09-02

0103 データ・AI・先端技術監査 > AI・生成AI・モデル／利用リスク ｜ 難易度：基礎

従業員が顧客の機密情報を公開型生成AIへ入力していることが判明した。最も適切な対応はどれか。

ア．利便性を優先して全ての情報入力を許可する

イ．従業員個人の判断だけに任せる

ウ．利用ルールと許可サービスを明確化し、機密データ入力を制限するとともに教育・技術的統制を行う

エ．問題が起きるまで利用実態を把握しない

答え・解説 正答：ウ

ア：秘密保持・個人情報等のリスクが高い。

イ：組織的なガバナンスが不足する。

ウ：生成AI利用では入力情報が外部処理・学習等に利用される可能性を踏まえ、情報管理が必要である。

エ：シャドーAIのリスクを管理できない。

総合解説：監査では承認済みAI、入力可能データ区分、ログ、DLP等の技術対策、教育、例外承認を確認する。

対象：2026年度 / 基準日 2026-09-02

0104 データ・AI・先端技術監査 > AI・生成AI・モデル／利用リスク ｜ 難易度：標準

AIモデルの公平性を監査する際、最も適切な確認はどれか。

ア．全利用者へ完全に同じ出力を返すかだけを見る

イ．学習データの件数だけを確認する

ウ．モデル精度が高ければ公平性評価を省略する

エ．対象となる集団ごとの出力差を分析し、業務目的に照らして不合理な偏りがないか評価する

答え・解説 正答：エ

ア：正当な差異が必要な場合もあり、公平性の評価として不十分である。

イ：代表性やラベル偏り等も重要である。

ウ：全体精度が高くても特定集団に不利益が偏る可能性がある。

エ：公平性は一律の数値だけでなく、利用文脈と影響を踏まえて評価する必要がある。

総合解説：監査ではデータ偏り、評価指標、集団別性能、影響、是正手続を確認し、利用目的に応じた公平性を評価する。

対象：2026年度 / 基準日 2026-09-02

0105 データ・AI・先端技術監査 > AI・生成AI・モデル／利用リスク ｜ 難易度：標準

AIモデルの性能が時間経過とともに低下している。最も考えられる監査上の論点はどれか。

ア．データや業務環境の変化によるモデルドリフトを監視し、再評価・再学習の基準があるか
イ．モデルは一度検証すれば永久に同じ性能を維持する
ウ．性能低下時はログを削除する
エ．再学習は承認や検証なしに自動で行う

答え・解説 正答：ア

ア：本番環境では入力分布や業務条件が変わり、導入時の性能が維持されない場合がある。
イ：環境変化を無視している。
ウ：原因分析ができなくなる。
エ：新たな品質・安全リスクが生じる。
総合解説：監査では性能KPI、ドリフト検知、閾値、再学習・モデル更新の承認、再検証、ロールバックを確認する。

対象：2026年度 / 基準日 2026-09-02

0106 データ・AI・先端技術監査 > AI・生成AI・モデル／利用リスク ｜ 難易度：標準

生成AIを社内検索に使うRAGシステムで、監査上最も重要なアクセス制御はどれか。

ア．全社文書を一つの権限で全利用者へ検索可能にする
イ．利用者が元々閲覧権限を持つ文書だけを検索・回答生成に利用できるようにする
ウ．回答画面だけ認証し、検索元文書の権限は無視する
エ．アクセスログを保存しない

答え・解説 正答：イ

ア：機密情報の漏えいにつながる。
イ：検索拡張生成でも元データのアクセス権を越えて情報が露出しない統制が必要である。
ウ：権限昇格による情報露出が起こる。
エ：不正利用の追跡が困難になる。
総合解説：監査では検索インデックス、文書ACL、利用者権限、キャッシュ、プロンプト・回答ログを含めた情報アクセス境界を確認する。

対象：2026年度 / 基準日 2026-09-02

0107 データ・AI・先端技術監査 > AI・生成AI・モデル／利用リスク ｜ 難易度：標準

AIシステムに対するプロンプトインジェクションのリスクとして最も適切なものはどれか。

ア．モデルの電源消費が必ず増加すること
イ．データベースの正規化が崩れること
ウ．悪意ある入力により本来の指示を上書きさせ、機密情報の開示や不正な外部操作を誘発すること
エ．AIが必ず学習不能になること

答え・解説 正答：ウ

ア：主要な攻撃リスクではない。
イ：直接関係しない。
ウ：生成AIやAIエージェントでは入力内容が挙動を変え、想定外の処理につながる可能性がある。
エ：プロンプトインジェクションの定義ではない。
総合解説：監査では外部入力の隔離、ツール実行権限、出力フィルタ、人の承認、秘密情報へのアクセス制限等を確認する。

対象：2026年度 / 基準日 2026-09-02

0108 データ・AI・先端技術監査 > AI・生成AI・モデル／利用リスク ｜ 難易度：標準

AIエージェントが外部システムへ自律的に操作を行う場合、最も重要な追加統制はどれか。

ア．AIへ管理者権限を常時付与する
イ．操作履歴を保存しない
ウ．自律動作だから人が停止できない設計にする
エ．実行可能な操作範囲を最小化し、高影響操作には人の承認や停止機構を設ける

答え・解説 正答：エ

ア：誤動作・攻撃時の影響が過大になる。
イ：事後検証や責任追跡ができない。
ウ：安全上の制御手段が不足する。
エ：AIエージェントは外部環境へ影響を与えるため、観測・制御と権限境界が重要になる。
総合解説：AISI第1.20版ではAIエージェントの普及を踏まえ、観測と制御、自律的挙動、外部環境との相互作用を評価観点に追加している。

対象：2026年度 / 基準日 2026-09-02

0109 データ・AI・先端技術監査 > AI・生成AI・モデル／利用リスク ｜ 難易度：応用

AIモデルを外部ベンダから調達する場合、監査上最も適切な確認はどれか。

ア．利用条件、データ取扱い、モデル変更、性能・安全性情報、障害・事故連絡、終了時対応を契約と運用で確認する
イ．ベンダが大手ならリスク評価を省略する
ウ．モデル更新の通知を不要とする
エ．入力データの利用条件を確認しない

答え・解説 正答：ア

ア：外部AI利用ではモデル自体を直接管理できないため、契約・第三者情報・モニタリングが重要である。
イ：知名度は自組織の利用リスクを保証しない。
ウ：性能や挙動が変わる可能性がある。
エ：機密性・知的財産・個人情報等の問題が生じる。
総合解説：監査では責任分界、SLA、データ利用、モデルバージョン、説明情報、インシデント、退出可能性を確認する。

対象：2026年度 / 基準日 2026-09-02

0110 データ・AI・先端技術監査 > AI・生成AI・モデル／利用リスク ｜ 難易度：応用

高リスクなAI利用で人によるレビューを設けているが、担当者がAI出力をほぼ無条件に承認している。最も適切な監査評価はどれか。

ア．承認ボタンがあるので統制は必ず有効である
イ．形式上のHuman-in-the-loopはあるが、実質的な人間の監督が機能していない可能性がある
ウ．AIの精度が高ければ人の役割は一切不要である
エ．レビュー記録は不要である

答え・解説 正答：イ

ア：形式だけでは有効性を評価できない。
イ：人が介在していても、判断能力・時間・根拠情報がなければ有効な監督にならない。
ウ：用途のリスクに応じた監督が必要である。
エ：高リスク判断では誰が何を確認したかの追跡性が重要である。
総合解説：監査ではレビュー基準、担当者能力、AIの不確実性表示、差戻し権限、実際の修正・却下状況を確認する。

対象：2026年度 / 基準日 2026-09-02

**0111** データ・AI・先端技術監査 > IoT・モバイル・RPA・ビッグデータ ｜ 難易度：基礎

IoT機器のセキュリティ監査で、資産台帳に含める情報として最も適切なものはどれか。

ア．機器の外装色だけ
イ．購入価格だけ
ウ．機器識別子、設置場所、所有者、ファームウェア版、通信先、サポート期限
エ．資産台帳を作らずネットワーク探索だけに依存する

**答え・解説** 正答：ウ

ア：セキュリティ管理にはほぼ寄与しない。
イ：リスク管理に必要な技術・運用情報が不足する。
ウ：IoT機器は多数・分散しやすいため、脆弱性対応や影響分析の基礎となる資産情報が必要である。
エ：オフライン機器や責任情報を把握しにくい。
総合解説：IPAのIoT手引きはIoT構成要素ごとの脅威・リスク分析を重視しており、対象機器を把握することが前提となる。

対象：2026年度 / 基準日 2026-09-02

**0112** データ・AI・先端技術監査 > IoT・モバイル・RPA・ビッグデータ ｜ 難易度：基礎

IoT機器の初期パスワードが全台同一のまま運用されている。最も適切な改善はどれか。

ア．パスワードを公開して利用者間で共有する
イ．認証機能を無効にする
ウ．変更記録を残さず担当者が自由に設定する
エ．初期認証情報を変更し、機器ごと又は管理された方式で強固な認証を設定する

**答え・解説** 正答：エ

ア：不正アクセスリスクが高まる。
イ：アクセス制御を失う。
ウ：管理不能になる。
エ：共通初期パスワードは大量侵害の原因となり得る。
総合解説：監査では初期設定、認証強度、不要サービス、遠隔管理、更新機能などセキュアな導入設定を確認する。

対象：2026年度 / 基準日 2026-09-02

**0113** データ・AI・先端技術監査 > IoT・モバイル・RPA・ビッグデータ ｜ 難易度：基礎

サポート終了したIoT機器を重要業務で継続利用する場合、最も適切な対応はどれか。

ア．脆弱性修正不能のリスクを評価し、隔離・通信制限等の代替策と更新・廃止計画を定める
イ．動作している限り無期限でそのまま使う
ウ．サポート終了情報を資産台帳へ反映しない
エ．重要ネットワークへ直接公開する

**答え・解説** 正答：ア

ア：サポート終了機器は新たな脆弱性に対応できないため、残存リスクを管理する必要がある。
イ：リスクが蓄積する。
ウ：対象機器を追跡できない。
エ：攻撃面を拡大する。
総合解説：監査では製品寿命、アップデート提供、ネットワーク分離、監視、代替機への移行期限を確認する。

対象：2026年度 / 基準日 2026-09-02

**0114** データ・AI・先端技術監査 > IoT・モバイル・RPA・ビッグデータ ｜ 難易度：標準

会社支給スマートフォンの情報漏えい対策として最も適切なものはどれか。

ア．画面ロックを無効にして利便性を上げる
イ．端末暗号化、画面ロック、MDM、リモートワイプ、アプリ配布制御を組み合わせる
ウ．利用者へ管理者権限を常時付与する
エ．紛失時の連絡手順を設けない

**答え・解説** 正答：イ

ア：紛失時の情報漏えいリスクが高まる。
イ：モバイル端末は紛失・盗難や不正アプリのリスクがあるため、複数の管理策が必要である。
ウ：設定変更・不正アプリ導入のリスクが高まる。
エ：初動が遅れる。
総合解説：監査ではMDM等による設定強制、暗号化、認証、アプリ制御、紛失時対応、OS更新を確認する。

対象：2026年度 / 基準日 2026-09-02

**0115** データ・AI・先端技術監査 > IoT・モバイル・RPA・ビッグデータ ｜ 難易度：標準

BYODを認める組織で最も重要な監査上の確認はどれか。

ア．私物端末なので会社は一切ルールを定めない

イ．個人データも含め端末全体を無条件で会社が閲覧する

ウ．業務データと私用領域の分離、端末要件、アクセス条件、紛失・退職時のデータ消去方法が定められているか

エ．退職後も業務データを端末に残す

**答え・解説** 正答：ウ

ア：業務情報を扱う以上、必要な統制が必要である。
イ：プライバシー等への配慮が必要である。
ウ：私物端末では組織の統制権限と個人所有権の境界を明確にする必要がある。
エ：情報漏えいリスクがある。
総合解説：監査では利用同意、コンテナ化、MDM/MAM、端末適合性、認証、リモート削除範囲、退職処理を確認する。

対象：2026年度 / 基準日 2026-09-02

**0116** データ・AI・先端技術監査 > IoT・モバイル・RPA・ビッグデータ ｜ 難易度：標準

RPAロボット用アカウントの管理として最も適切なものはどれか。

ア．複数ロボットで一つの管理者IDを共有する

イ．資格情報をスクリプトへ平文で埋め込む

ウ．ロボット処理は自動なのでログを残さない

エ．ロボットごとに識別可能な専用IDを用い、必要最小権限・資格情報保護・利用ログを管理する

**答え・解説** 正答：エ

ア：追跡性と最小権限が損なわれる。
イ：漏えいリスクが高い。
ウ：異常・不正処理を追跡できない。
エ：RPAは人に代わって大量処理するため、共有資格情報や過剰権限は影響が大きい。
総合解説：監査ではRPAの所有者、専用ID、秘密情報管理、権限、実行ログ、例外処理を確認する。

対象：2026年度 / 基準日 2026-09-02

**0117** データ・AI・先端技術監査 > IoT・モバイル・RPA・ビッグデータ ｜ 難易度：標準

RPAシナリオの変更管理として最も適切なものはどれか。

ア．変更申請、レビュー、テスト、承認、本番反映、ロールバックを管理する
イ．作成者が本番シナリオを直接自由に変更する
ウ．変更履歴を残さない
エ．業務ルール変更をRPAへ反映する前にテストしない

**答え・解説** 正答：ア

ア：RPA変更は大量の取引を誤処理する可能性があるため、通常のシステム変更と同様の統制が必要である。
イ：誤り・不正を牽制できない。
ウ：原因追跡と再現が困難になる。
エ：大量誤処理につながる。
総合解説：監査では開発・本番分離、版管理、テストデータ、承認者、緊急変更、停止手順を確認する。

対象：2026年度 / 基準日 2026-09-02

**0118** データ・AI・先端技術監査 > IoT・モバイル・RPA・ビッグデータ ｜ 難易度：標準

ビッグデータ分析で、データ量が非常に多いことだけをもって分析結果を信頼できるとする判断の問題点はどれか。

ア．データ量が多いほど必ずバイアスがなくなる
イ．大量データでも偏り・欠損・誤り・来歴不明があれば、結果の信頼性は低下する
ウ．大量データでは品質管理が不要になる
エ．ビッグデータは個人情報を含まない

**答え・解説** 正答：イ

ア：収集方法に偏りがあれば大量でも偏る。
イ：量の多さは品質や代表性を保証しない。
ウ：むしろ自動品質監視が重要になる。
エ：データ内容によって個人情報を含み得る。
総合解説：監査ではVolumeだけでなく、出所、品質、代表性、更新頻度、権利、目的適合性を評価する。

対象：2026年度 / 基準日 2026-09-02

0119 データ・AI・先端技術監査 > IoT・モバイル・RPA・ビッグデータ ｜ 難易度：応用

ストリーミングデータをリアルタイム分析する仕組みで、入力形式が変更され一部項目を誤読していた。最も適切な統制はどれか。

ア．入力形式は永久に変わらないと仮定する
イ．誤読しても大量データなので影響は小さいとみなす
ウ．スキーマ変更を検知・承認し、互換性テストと異常値監視を行う
エ．異常値を記録せず捨てる

答え・解説 正答：ウ

ア：実運用では変更が起こり得る。
イ：広範な誤判断につながる可能性がある。
ウ：高速データ連携では上流変更が下流分析へ即時に影響するため、スキーマ管理が重要である。
エ：原因分析と品質改善ができない。
総合解説：監査ではデータ契約、スキーマ版管理、互換性、エラーハンドリング、品質監視を確認する。

対象：2026年度 / 基準日 2026-09-02

0120 データ・AI・先端技術監査 > IoT・モバイル・RPA・ビッグデータ ｜ 難易度：応用

IoT・RPA・モバイルを組み合わせた業務自動化で最も重要な監査観点はどれか。

ア．各製品単体が動作すれば全体統制は不要とする
イ．異常時も完全自動で処理を継続させる
ウ．技術ごとにログ時刻や識別子を統一しない
エ．各技術間の責任分界・認証・データ連携・例外時の人手介入を端から端まで確認する

答え・解説 正答：エ

ア：インターフェースや責任の隙間を見逃す。
イ：誤処理を拡大する可能性がある。
ウ：障害・不正の追跡が困難になる。
エ：複数技術を連携すると、一つの統制不備が連鎖して業務全体へ影響する。
総合解説：監査では機器・モバイル・ロボット・基幹システムを横断し、認証、データ品質、ログ、例外、停止・復旧を一連で評価する。

対象：2026年度 / 基準日 2026-09-02

0121 監査基準・他監査との連携 > システム監査基準・管理基準 ｜ 難易度：基礎

クラウド運用管理をシステム監査する際、システム監査基準とシステム管理基準の使い分けとして最も適切なものはどれか。

ア．システム監査基準は監査人の実施・報告等の基準を示し、システム管理基準はITガバナンス・ITマネジメントの管理上の着眼点を示す

イ．両者は完全に同一内容である

ウ．システム管理基準は監査人の倫理だけを定める

エ．システム監査基準は業務執行手順だけを定める

答え・解説 正答：ア

ア：両者は目的が異なるが、システム管理基準は監査の評価尺度として活用できる。

イ：役割・構成が異なる。

ウ：管理基準はITガバナンス・ITマネジメントを対象とする。

エ：監査人の属性・実施・報告を含む。

総合解説：2023年改訂の両基準を組み合わせることで、監査の進め方と評価対象の管理上の着眼点を整理できる。

対象：2026年度 / 基準日 2026-09-02

0122 監査基準・他監査との連携 > システム監査基準・管理基準 ｜ 難易度：基礎

システム管理基準を監査の評価尺度として使う際、最も適切な考え方はどれか。

ア．全項目を全ての組織へ同じ深さで適用する

イ．監査目的・対象の特性に応じて必要な項目を選定し、組織固有の基準と組み合わせて評価する

ウ．管理基準にない事項は監査で一切扱わない

エ．対象部門の希望する項目だけを評価する

答え・解説 正答：イ

ア：規模・業態・リスクによる違いを反映できない。

イ：管理基準を機械的なチェックリストとして全項目一律適用するのではなく、リスクと目的に応じて使う必要がある。

ウ：法令・契約・社内規程等も評価基準になり得る。

エ：監査人が独立して必要な評価尺度を設計する。

総合解説：監査ではシステム管理基準、法令、契約、社内基準などを組み合わせ、監査目的に適した評価基準を明確にする。

対象：2026年度 / 基準日 2026-09-02

0123 監査基準・他監査との連携 > システム監査基準・管理基準 ｜ 難易度：基礎

システム監査基準に基づく監査で、監査対象のリスクが大きく変化した場合に最も適切な対応はどれか。

ア．承認済み計画は一切変更しない
イ．全ての手続を増やす
ウ．リスク評価を更新し、監査範囲・手続・資源配分を必要に応じて見直す
エ．監査対象部門へ計画変更を全面委任する

答え・解説 正答：ウ

ア：新たな重要リスクを見逃す可能性がある。
イ：リスクに応じた選択が必要である。
ウ：システム監査はリスク・アプローチにより重要リスクへ監査資源を配分する。
エ：監査側が独立して判断する必要がある。
総合解説：基準は監査目的・リスクに基づく監査計画と十分な証拠を重視しており、状況変化へ適切に対応することが必要である。

対象：2026年度 / 基準日 2026-09-02

0124 監査基準・他監査との連携 > システム監査基準・管理基準 ｜ 難易度：標準

システム管理基準のITガバナンス編を評価する監査で、最も適切な着眼点はどれか。

ア．個々のプログラムのコーディング規約だけ
イ．一台の端末の画面設定だけ
ウ．日々のジョブ監視だけ
エ．経営戦略とIT戦略の整合、意思決定権限、ITパフォーマンス、リスク・資源の監督

答え・解説 正答：エ

ア：主に実装・開発管理の論点である。
イ：経営レベルのガバナンス評価として不十分である。
ウ：運用管理の詳細でありガバナンス全体を表さない。
エ：ITガバナンス編は経営レベルでITを方向付け・監督する仕組みを対象とする。
総合解説：監査では取締役会等による方向付け、説明責任、投資・リスク・成果の監督を経営目標と関連付けて確認する。

対象：2026年度 / 基準日 2026-09-02

0125 監査基準・他監査との連携 > システム監査基準・管理基準 ｜ 難易度：標準

システム管理基準のITマネジメント編を監査する際、最も適切な考え方はどれか。

ア．ガバナンス方針を具体的な企画・開発・運用・セキュリティ等の管理活動へ落とし込めているか確認する

イ．経営戦略との関係を無視する

ウ．管理活動の実施証跡を確認しない

エ．業務部門との責任分界を定めない

答え・解説 正答：ア

ア：ITマネジメントはガバナンスの方向付けを実務へ展開する役割を持つ。

イ：ガバナンスとの整合が必要である。

ウ：実効性を評価できない。

エ：管理漏れ・重複が生じる。

総合解説：監査では方針・責任・手続・モニタリングが一貫し、ITサービスのライフサイクルで管理されているかを確認する。

対象：2026年度 / 基準日 2026-09-02

0126 監査基準・他監査との連携 > システム監査基準・管理基準 ｜ 難易度：標準

システム監査基準に基づく監査報告で、最も重要なことはどれか。

ア．監査調書の全文をそのまま報告書にする

イ．監査目的・範囲・証拠・結論の関係を明確にし、重要事項を利用者が理解できるよう報告する

ウ．証拠にない推測を断定する

エ．重要な範囲制約を記載しない

答え・解説 正答：イ

ア：利用者に必要な情報へ整理する必要がある。

イ：監査報告は監査の結論を適切な利用者へ伝え、意思決定に役立てる必要がある。

ウ：客観性を損なう。

エ：結論の誤解につながる。

総合解説：報告では事実と評価を区別し、監査の前提、重要な発見、結論、改善提案等を明確にする。

対象：2026年度 / 基準日 2026-09-02

0127 監査基準・他監査との連携 > システム監査基準・管理基準 ｜ 難易度：標準

システム管理基準に自社固有の管理基準を追加する場合、最も適切な理由はどれか。

ア．管理基準の要求を恣意的に弱めるため
イ．監査人の好みだけを反映するため
ウ．業種規制、契約、技術構成、リスク許容度など組織固有の要求を反映するため
エ．法令要件を無視するため

答え・解説 正答：ウ

ア：リスクに応じた合理的な調整が必要である。
イ：客観的根拠が必要である。
ウ：汎用的な管理基準だけでは個別組織の全リスクを網羅できない。
エ：むしろ適用法令を追加評価する。
総合解説：監査ではシステム管理基準を共通の参照軸としつつ、法令・契約・社内規程・技術要件を加えて評価尺度を構成する。

対象：2026年度 / 基準日 2026-09-02

0128 監査基準・他監査との連携 > システム監査基準・管理基準 ｜ 難易度：標準

2023年改訂のシステム管理基準を監査で利用する際、旧版のチェックリストだけを継続利用する問題点はどれか。

ア．旧版は必ず違法になる
イ．新旧版の差分確認は不要である
ウ．監査基準は一度作れば更新不要である
エ．ITガバナンスや最新のデジタル環境を踏まえた改訂内容を監査へ反映できない可能性がある

答え・解説 正答：エ

ア：旧版使用自体が直ちに違法とは限らない。
イ：改訂点の影響を評価する必要がある。
ウ：制度・技術環境の変化に応じて見直す必要がある。
エ：評価基準は現行版を確認し、監査対象期間・目的に適した内容を使う必要がある。
総合解説：監査部門は利用する基準の版、適用日、改訂内容を管理し、監査プログラムやテンプレートへ反映する。

対象：2026年度 / 基準日 2026-09-02

**0129** 監査基準・他監査との連携 > システム監査基準・管理基準 ｜ 難易度：応用

システム監査基準と法令要件が同じ監査対象に関係する場合、最も適切な対応はどれか。

ア．システム監査基準に沿った監査手続で、法令を含む適切な評価基準への準拠を検証する

イ．システム監査基準があれば法令は無視する

ウ．法令があれば監査証拠は不要とする

エ．両者がある場合は監査を行わない

**答え・解説** 正答：ア

ア：監査の実施方法と評価尺度は区別して組み合わせることができる。

イ：法的義務の評価が欠ける。

ウ：準拠状況を証拠で検証する必要がある。

エ：役割を整理して適用する。

総合解説：監査人はシステム監査基準に従って計画・実施・報告し、法令・契約・管理基準等を判断尺度として利用する。

対象：2026年度 / 基準日 2026-09-02

**0130** 監査基準・他監査との連携 > システム監査基準・管理基準 ｜ 難易度：応用

監査対象部門が『システム管理基準に完全一致していないから直ちに重大不備だ』と評価された。最も適切な再評価はどれか。

ア．基準の文言と一文字でも違えば重大不備とする

イ．監査目的、組織特性、リスク、代替統制を確認し、基準の趣旨を満たしているか実質的に評価する

ウ．代替統制は一切認めない

エ．対象部門の自己評価だけで適合とする

**答え・解説** 正答：イ

ア：実効性・リスクを考慮していない。

イ：管理基準はリスクや組織特性に応じて適用し、形式的一致だけで結論を出すべきではない。

ウ：異なる方法で同じ統制目的を達成する場合がある。

エ：監査人の独立した検証が必要である。

総合解説：監査では統制目的、リスク低減効果、運用証拠を見て、基準への適合性を合理的に判断する。

対象：2026年度 / 基準日 2026-09-02

**0131** 監査基準・他監査との連携 > 情報セキュリティ監査・内部監査基準 ｜ 難易度：基礎

情報セキュリティ監査の準拠規範を設定する場面で、最も適切な考え方はどれか。

ア．脆弱性診断だけを意味する
イ．監査人がセキュリティ運用を代行する
ウ．情報セキュリティに関する管理・対策を、合意した準拠規範に照らして独立的に検証・評価する
エ．管理基準を定めず担当者の感覚で判断する

**答え・解説** 正答：ウ

ア：監査は技術診断より広い管理・統制評価を含む。
イ：独立評価と業務執行は区別する。
ウ：情報セキュリティ監査では監査目的に応じた判断尺度を定め、セキュリティ管理の状況を評価する。
エ：準拠規範を明確にする必要がある。
総合解説：情報セキュリティ監査基準と実施基準ガイドラインは、監査目的・契約に応じて準拠規範を合意し評価する考え方を示している。

対象：2026年度 / 基準日 2026-09-02

**0132** 監査基準・他監査との連携 > 情報セキュリティ監査・内部監査基準 ｜ 難易度：基礎

令和7年改正版の情報セキュリティ監査基準で強調された考え方として最も適切なものはどれか。

ア．全管理策を必ず同じ深さで監査する
イ．監査証拠を取得しない
ウ．監査対象のリスクを考慮しない
エ．リスクベースで監査目標・重点領域を設定する

**答え・解説** 正答：エ

ア：リスクに応じた重点化と逆である。
イ：客観的評価には証拠が必要である。
ウ：改訂趣旨に反する。
エ：改訂ではリスクベース監査を行うべきことが明記された。
総合解説：監査では組織の情報セキュリティリスクを把握し、重要リスクに対応した監査目標・手続を設計する。

対象：2026年度 / 基準日 2026-09-02

0133 監査基準・他監査との連携 > 情報セキュリティ監査・内部監査基準 ｜ 難易度：基礎

情報セキュリティ管理基準の令和7年改正版の特徴として最も適切なものはどれか。

ア．従来のマネジメント基準・管理策基準に加え、ガバナンス基準が追加された

イ．アクセス制御に関する項目が全て削除された

ウ．管理基準が監査人の倫理だけを扱うようになった

エ．リスク管理が不要になった

答え・解説 正答：ア

ア：改訂ではJIS Q 27001/27002改訂を反映するとともにガバナンス基準が追加された。

イ：そのような改訂ではない。

ウ：情報セキュリティ管理の基準である。

エ：むしろガバナンス・リスク管理が重要である。

総合解説：監査ではガバナンス、マネジメント、管理策を階層的に評価し、経営とセキュリティ管理のつながりを見る。

対象：2026年度 / 基準日 2026-09-02

0134 監査基準・他監査との連携 > 情報セキュリティ監査・内部監査基準 ｜ 難易度：標準

情報セキュリティ監査と脆弱性診断の関係として最も適切なものはどれか。

ア．両者は完全に同一である

イ．脆弱性診断は技術的弱点を検出する手段の一つであり、監査ではその結果を管理プロセスやリスク対応と合わせて評価する

ウ．監査では技術的証拠を一切利用しない

エ．診断で脆弱性がなければ管理体制も必ず有効である

答え・解説 正答：イ

ア：目的・範囲が異なる。

イ：監査は診断結果だけでなく、責任・手続・対応・継続改善まで含めて評価する。

ウ：診断結果やログ等も証拠になり得る。

エ：資産漏れや手続不備など別のリスクがある。

総合解説：監査では脆弱性管理の方針、対象網羅性、優先順位、是正期限、例外管理等を診断結果と組み合わせて評価する。

対象：2026年度 / 基準日 2026-09-02

**0135** 監査基準・他監査との連携 > 情報セキュリティ監査・内部監査基準 ｜ 難易度：標準

内部監査の目的として最も適切なものはどれか。

ア．業務執行を内部監査部門が代行する

イ．経営者の希望する結論を作成する

ウ．独立したアシュアランスとアドバイザリーを通じて、組織のガバナンス・リスク管理・コントロールの改善に貢献する

エ．会計数値だけを監査対象とする

**答え・解説** 正答：ウ

ア：独立性を損なう。

イ：客観性が必要である。

ウ：内部監査は組織の価値の創造・保全を支える専門機能である。

エ：内部監査の対象はより広い。

総合解説：グローバル内部監査基準は内部監査の目的を中心に、倫理、ガバナンス、部門管理、業務実施の枠組みを示している。

対象：2026年度 / 基準日 2026-09-02

**0136** 監査基準・他監査との連携 > 情報セキュリティ監査・内部監査基準 ｜ 難易度：標準

グローバル内部監査基準の構成として最も適切なものはどれか。

ア．財務・税務・法務の3ドメインだけ

イ．IT開発・運用・保守だけ

ウ．監査報告だけの単一ドメイン

エ．内部監査の目的、倫理と専門職としての気質、内部監査部門のガバナンス、部門管理、内部監査業務の実施の5ドメイン

**答え・解説** 正答：エ

ア：GIASの構成ではない。

イ：内部監査全体を対象とする。

ウ：複数の原則・要求事項で構成される。

エ：2024年版GIASは5つのドメインで構成される。

総合解説：内部監査人は個別業務だけでなく、倫理、独立性・客観性、部門ガバナンス、品質、業務実施を体系的に管理する。

対象：2026年度 / 基準日 2026-09-02

**0137** 監査基準・他監査との連携 > 情報セキュリティ監査・内部監査基準 ｜ 難易度：標準

内部監査人の客観性に対する脅威が生じた場合、最も適切な対応はどれか。

ア．脅威を評価し、担当変更・独立レビュー・開示など適切な防御措置を講じる
イ．影響を隠してそのまま監査する
ウ．経験が豊富なら利益相反は無視する
エ．監査対象部門に結論を決めてもらう

**答え・解説** 正答：ア

ア：客観性は実質だけでなく、影響を与え得る関係を認識し管理する必要がある。
イ：監査の信頼性を損なう。
ウ：経験は客観性の代替にならない。
エ：独立性が失われる。
総合解説：日本内部監査協会の適用ガイダンスでも客観性の防御と客観性侵害の開示が扱われている。

対象：2026年度 / 基準日 2026-09-02

**0138** 監査基準・他監査との連携 > 情報セキュリティ監査・内部監査基準 ｜ 難易度：標準

内部監査部門の品質を継続的に高める方法として最も適切なものはどれか。

ア．監査件数だけ増やす
イ．基準への適合、レビュー結果、利用者の期待、監査実績を評価し、品質改善計画へ反映する
ウ．レビューで見つかった問題を記録しない
エ．基準の改訂を把握しない

**答え・解説** 正答：イ

ア：品質や価値を保証しない。
イ：内部監査部門は品質の評価と改善を継続的に行う必要がある。
ウ：再発防止につながらない。
エ：現行基準への適合性を維持できない。
総合解説：監査部門の品質は個別業務のレビューだけでなく、部門レベルの能力・方法論・成果を継続的に評価して改善する。

対象：2026年度 / 基準日 2026-09-02

**0139** 監査基準・他監査との連携 > 情報セキュリティ監査・内部監査基準 ｜ 難易度：応用

情報セキュリティ監査と内部監査を連携させる際、最も適切な考え方はどれか。

ア．どちらか一方の監査を必ず廃止する

イ．一方の結果を無検証でそのまま採用する

ウ．監査目的・基準・専門性の違いを明確にし、リスク評価・対象・証拠を共有できる範囲で調整する

エ．監査スケジュールを共有しない

**答え・解説** 正答：ウ

ア：監査目的が異なる場合がある。

イ：信頼性・適合性の評価が必要である。

ウ：連携により重複を減らせるが、各監査の責任と目的を曖昧にしてはならない。

エ：対象部門の負荷や重複が増える。

総合解説：監査ユニバース、リスク、時期、成果物、専門家を調整しつつ、各基準に基づく責任を維持することが重要である。

対象：2026年度 / 基準日 2026-09-02

**0140** 監査基準・他監査との連携 > 情報セキュリティ監査・内部監査基準 ｜ 難易度：応用

内部監査人が監査で取得した機密情報を扱う際、最も適切な対応はどれか。

ア．興味のある同僚へ自由に共有する

イ．退職後なら自由に利用する

ウ．監査調書を個人クラウドへ保存する

エ．業務目的に必要な範囲で利用し、アクセス・保管・共有・廃棄を組織のルールに従って保護する

**答え・解説** 正答：エ

ア：正当な必要性のない開示は不適切である。

イ：守秘義務が継続する場合がある。

ウ：認可されない保管は漏えいリスクがある。

エ：内部監査基準では情報保護が専門職としての重要な要求となる。

総合解説：日本内部監査協会の適用ガイダンスには情報の保護に関する項目があり、監査情報の秘密保持と適切な取扱いが求められる。

対象：2026年度 / 基準日 2026-09-02

0141 監査基準・他監査との連携 > 会計監査・内部統制監査・外部専門家連携 ｜ 難易度：基礎

システム監査と会計監査が同じ基幹システムを対象とする場合、連携の主な利点はどれか。

ア．IT統制に関する情報や監査時期を調整し、重複を抑えながら重要リスクのカバレッジを高められる
イ．システム監査の責任を会計監査人へ全て移せる
ウ．会計監査があればシステム監査は必ず不要になる
エ．相互の監査結果を一切確認しない

答え・解説 正答：ア

ア：複数監査が同一統制を扱う場合、計画・証拠の調整により効率化できる。
イ：各監査の目的と責任は残る。
ウ：監査目的・範囲が異なる。
エ：重複・漏れが生じやすい。
総合解説：監査では対象統制、評価期間、成果物、依存可能性を調整し、必要な監査証拠の重複収集を減らす。

対象：2026年度 / 基準日 2026-09-02

0142 監査基準・他監査との連携 > 会計監査・内部統制監査・外部専門家連携 ｜ 難易度：基礎

財務報告に係る内部統制監査でIT全般統制が重視される理由として最も適切なものはどれか。

ア．IT全般統制が財務諸表の数値を直接作成するから
イ．財務報告に関係する自動統制やデータ処理の継続的な信頼性をIT全般統制が支えるため
ウ．IT全般統制が有効なら業務処理統制の評価は全て不要になる
エ．財務報告とITは無関係だから

答え・解説 正答：イ

ア：基盤統制として支える役割が中心である。
イ：変更管理・アクセス管理等が弱いと、業務処理統制のロジックやデータの信頼性に影響する。
ウ：重要な業務処理統制の評価は必要である。
エ：現代の財務報告はITへ大きく依存する。
総合解説：金融庁実施基準ではIT全般統制とIT業務処理統制を区分し、財務報告に係る内部統制のITへの対応を評価する。

対象：2026年度 / 基準日 2026-09-02

0143 監査基準・他監査との連携 > 会計監査・内部統制監査・外部専門家連携 ｜ 難易度：基礎

会計監査人がシステム監査部門の作業結果を利用しようとする場合、最も適切な考え方はどれか。

ア．内部監査の報告書があれば無条件で全面利用する
イ．同じ会社の監査なら証拠評価は不要とする
ウ．作業の目的・範囲・能力・客観性・証拠の品質を評価し、利用可能な範囲を判断する
エ．利用した作業について会計監査人は一切責任を持たない

答え・解説 正答：ウ

ア：目的や品質が異なる可能性がある。
イ：信頼性評価が必要である。
ウ：他者の作業を利用する場合でも、自らの監査目的に適合するかを評価する必要がある。
エ：最終的な監査意見への責任は残る。
総合解説：監査連携では相手の独立性・能力・方法論・証拠を確認し、自分の監査目的への適合性を判断する。

対象：2026年度 / 基準日 2026-09-02

0144 監査基準・他監査との連携 > 会計監査・内部統制監査・外部専門家連携 ｜ 難易度：標準

AIモデルの高度な技術評価で外部専門家を利用する場合、監査責任者が最も重要に確認すべきことはどれか。

ア．専門家へ監査結論の全責任を移す
イ．専門家の説明を理解せずそのまま報告する
ウ．専門家の利益相反を確認しない
エ．専門家の能力・客観性・役割・成果物を評価し、監査人自身が結果を理解して結論へ統合する

答え・解説 正答：エ

ア：監査責任者の責任は残る。
イ：証拠として適切に評価できない。
ウ：客観性への影響があり得る。
エ：専門家の利用は監査人の責任を移転するものではない。
総合解説：監査では専門家の選定基準、契約、独立性、作業範囲、成果物レビュー、秘密保持を管理する。

対象：2026年度 / 基準日 2026-09-02

0145 監査基準・他監査との連携 > 会計監査・内部統制監査・外部専門家連携 ｜ 難易度：標準

デジタルフォレンジック専門家へ不正調査を委託する際、最も適切な連携はどれか。

ア．証拠保全方法、調査範囲、Chain of Custody、報告形式、秘密保持を事前に合意する
イ．証拠媒体を記録なしで引き渡す
ウ．専門家が調べた内容は監査調書に残さない
エ．調査範囲を無制限にして個人情報を全て取得する

答え・解説 正答：ア

ア：専門調査では証拠の信頼性と監査目的への適合性を確保する必要がある。
イ：証拠管理の連続性が失われる。
ウ：結論の裏付けを追跡できない。
エ：目的・法令・必要性を考慮する必要がある。
総合解説：監査人は専門家の作業を監査証拠として利用できるよう、保全・分析・報告プロセスを監査目的と整合させる。

対象：2026年度 / 基準日 2026-09-02

0146 監査基準・他監査との連携 > 会計監査・内部統制監査・外部専門家連携 ｜ 難易度：標準

内部統制監査とシステム監査の評価結果が異なる場合、最も適切な対応はどれか。

ア．常にシステム監査の結論を優先する
イ．目的・評価基準・対象期間・母集団・証拠の違いを整理し、差異の原因を確認する
ウ．結果が違えば両方無効とする
エ．相互に情報共有せず放置する

答え・解説 正答：イ

ア：監査目的によって適切な評価が異なる。
イ：異なる監査は目的や基準が異なるため、結論だけを比較して一方を誤りと決めつけるべきではない。
ウ：差異の合理的な理由がある場合がある。
エ：組織のリスク認識に混乱を生じる。
総合解説：監査ではスコープ、重要性、テスト時期、サンプル、評価基準を比較し、必要に応じ追加手続や統合的な報告を行う。

対象：2026年度 / 基準日 2026-09-02

0147 監査基準・他監査との連携 > 会計監査・内部統制監査・外部専門家連携 ｜ 難易度：標準

会計監査で利用するシステム生成レポートについて、システム監査人が支援する最も適切な内容はどれか。

ア．レポートの印刷品質だけを確認する
イ．出力された数値を無条件に正しいとする
ウ．レポート生成ロジック、元データ、アクセス・変更統制を確認し、情報の信頼性評価を支援する
エ．会計監査人にシステム情報を一切提供しない

答え・解説 正答：ウ

ア：証拠の信頼性とは関係が薄い。
イ：システム設定や元データに誤りがあり得る。
ウ：監査証拠として利用するシステム情報は、完全性・正確性を評価する必要がある。
エ：適切な連携で監査品質を高められる。
総合解説：システム監査人はIT全般統制やレポートロジックの評価を通じ、会計監査人が利用する情報の信頼性判断を支援できる。

対象：2026年度 / 基準日 2026-09-02

0148 監査基準・他監査との連携 > 会計監査・内部統制監査・外部専門家連携 ｜ 難易度：標準

複数の監査・専門家が同じ組織を監査する場合、監査対象部門の負荷を下げつつ品質を維持する方法として最も適切なものはどれか。

ア．全監査で同じ質問を別々に繰り返す
イ．負荷軽減のため重要な監査を全て省略する
ウ．一つの監査報告書を全監査目的へ無条件で流用する
エ．監査カレンダー、資料要求、インタビュー、利用可能な証拠を調整し、重複を減らす

答え・解説 正答：エ

ア：不要な重複負荷が生じる。
イ：リスクを放置する。
ウ：目的・基準の適合性確認が必要である。
エ：監査間の連携により効率性を高められるが、各監査の必要証拠は確保する必要がある。
総合解説：監査ユニバースと年間計画を共有し、証拠の再利用可能性を評価しながら、対象部門への依頼を整理する。

対象：2026年度 / 基準日 2026-09-02

**0149** 監査基準・他監査との連携 > 会計監査・内部統制監査・外部専門家連携 ｜ 難易度：応用

外部専門家の報告書に重要な前提条件や制約が記載されている場合、監査人の最も適切な対応はどれか。

ア．前提・制約が監査目的と結論へ与える影響を評価し、必要なら追加手続を行う
イ．専門家の報告なので制約を無視する
ウ．制約があれば報告書を必ず廃棄する
エ．監査報告で制約を隠す

**答え・解説** 正答：ア

ア：専門家の成果物も監査証拠として適合性・十分性を評価する必要がある。
イ：結論の適用範囲を誤る可能性がある。
ウ：利用可能な範囲を評価すべきである。
エ：利用者の誤解につながる。
総合解説：監査人は専門家の方法、前提、データ、範囲制約を理解し、自らの監査結論への影響を判断する。

対象：2026年度 / 基準日 2026-09-02

**0150** 監査基準・他監査との連携 > 会計監査・内部統制監査・外部専門家連携 ｜ 難易度：応用

システム監査人、会計監査人、内部監査人、外部専門家の役割分担を決める際、最も適切な原則はどれか。

ア．全員が同じ責任を負うとして役割を定めない
イ．各者の監査目的・専門性・独立性・責任を明確にし、最終判断の責任主体を曖昧にしない
ウ．最も外部の者へ全責任を移す
エ．専門性を考慮せず均等に作業を割り当てる

**答え・解説** 正答：イ

ア：作業漏れ・責任不明確を招く。
イ：連携は責任の空白や重複を減らすために行い、責任転嫁の手段にしてはならない。
ウ：各監査主体の責任は残る。
エ：品質と効率が低下する。
総合解説：監査計画では各者が行う手続、利用する成果物、レビュー、報告経路を定め、監査目的ごとの責任を維持する。

対象：2026年度 / 基準日 2026-09-02