0001 情報資産管理 > 情報資産の特定・価値評価 ｜ 難易度：基礎

部門の情報資産を洗い出すとき、対象として最も適切なものはどれか。

ア：業務データや情報システムだけでなく、文書、施設、業務知識を持つ人材なども含めて検討する。

イ：サーバとPCだけを対象にし、紙文書や人材は除外する。

ウ：購入価格が高い機器だけを対象にする。

エ：自社所有物だけを対象とし、利用中のクラウド上データは除外する。

答え・解説 正答：ア

ア：IPAシラバスでは、情報システム、データ、文書、施設、人材などを部門で利用する情報資産として特定することが求められています。

イ：情報資産はIT機器だけに限定されません。

ウ：情報資産の価値は取得価格だけで決まりません。

エ：利用・管理する情報も保護対象となり得ます。

総合解説：IPAシラバスでは、情報システム、データ、文書、施設、人材などを部門で利用する情報資産として特定することが求められています。 情報資産管理では、システムやデータだけでなく文書・施設・人材なども対象になり得ます。機密性・完全性・可用性の観点と事業影響を用い、保護の優先順位を決められるよう価値を明確化します。

対象：2026年度 / 基準日 2026-09-05

0002 情報資産管理 > 情報資産の特定・価値評価 ｜ 難易度：基礎

情報資産の特定方法として最も適切なものはどれか。

ア：IT部門の記憶だけで一覧を作り、現場には確認しない。

イ：文書精査や業務担当者へのヒアリングを組み合わせ、実際の業務で利用する資産を確認する。

ウ：資産名を推測して登録し、存在確認は行わない。

エ：障害が起きた資産だけを事後的に登録する。

答え・解説 正答：イ

ア：現場固有の資産や利用実態を見落とすおそれがあります。

イ：シラバスは、文書精査やヒアリングなどによって情報資産の価値を明確化できることを求めています。実態把握には複数の調査方法を組み合わせることが有効です。

ウ：実在性・利用状況の確認が必要です。

エ：平常時から網羅的に把握する必要があります。

総合解説：シラバスは、文書精査やヒアリングなどによって情報資産の価値を明確化できることを求めています。実態把握には複数の調査方法を組み合わせることが有効です。 情報資産管理では、システムやデータだけでなく文書・施設・人材なども対象になり得ます。機密性・完全性・可用性の観点と事業影響を用い、保護の優先順位を決められるよう価値を明確化します。

対象：2026年度 / 基準日 2026-09-05

0003 情報資産管理 > 情報資産の特定・価値評価 ｜ 難易度：基礎

顧客の個人情報を格納したデータベースの価値を評価する観点として、最も適切な組合せはどれか。

ア：ファイル容量と保存年数だけで評価する。

イ：購入価格と保守費用だけで評価する。

ウ：機密性・完全性・可用性のそれぞれが損なわれた場合の影響を評価する。

エ：利用者数だけで評価する。

答え・解説 正答：ウ

ア：容量や年数だけでは情報セキュリティ上の重要度を表せません。

イ：金銭価値だけでなく情報の漏えい・改ざん・利用不能の影響を考慮します。

ウ：情報資産の重要度は、機密性・完全性・可用性の三つの側面から評価することが基本です。

エ：利用者数は一要素になり得ますが、CIAの影響評価を代替しません。

総合解説：情報資産の重要度は、機密性・完全性・可用性の三つの側面から評価することが基本です。情報資産管理では、システムやデータだけでなく文書・施設・人材なども対象になり得ます。機密性・完全性・可用性の観点と事業影響を用い、保護の優先順位を決められるよう価値を明確化します。

対象：2026年度 / 基準日 2026-09-05

0004 情報資産管理 > 情報資産の特定・価値評価 ｜ 難易度：標準

同じ価格の二つのサーバA・Bがある。Aは停止しても翌営業日まで影響が小さいが、Bは停止すると受注処理が即時停止する。可用性の観点で適切な評価はどれか。

ア：購入価格が同じなので必ず同一の重要度とする。

イ：利用者が少ない方を常に高く評価する。

ウ：どちらもサーバなので価値評価を省略する。

エ：購入価格が同じでも、業務停止の影響が大きいBをより高い重要度として評価する。

答え・解説 正答：エ

ア：取得価格だけでは業務影響を反映できません。

イ：利用者数だけで重要度は決まりません。

ウ：資産ごとの影響を評価する必要があります。

エ：情報資産の価値は取得価格だけではなく、機密性・完全性・可用性が損なわれたときの事業影響で判断します。

総合解説：情報資産の価値は取得価格だけではなく、機密性・完全性・可用性が損なわれたときの事業影響で判断します。 情報資産管理では、システムやデータだけでなく文書・施設・人材なども対象になり得ます。機密性・完全性・可用性の観点と事業影響を用い、保護の優先順位を決められるよう価値を明確化します。

対象：2026年度 / 基準日 2026-09-05

0005 情報資産管理 > 情報資産の特定・価値評価 ｜ 難易度：標準

単独では重要度が低く見えるDNSサーバが、複数の重要業務システムの名前解決に使われている。価値評価として最も適切なものはどれか。

ア：業務システムとの依存関係を考慮し、停止時の波及影響を含めて重要度を見直す。

イ：DNSサーバは業務データを保存しないため無価値とする。

ウ：サーバ名の文字数で重要度を決める。

エ：依存関係はリスク評価に関係しないので無視する。

答え・解説 正答：ア

ア：情報資産の価値は単体だけでなく、他資産や業務プロセスとの依存関係による波及影響も考慮すると適切です。

イ：可用性などの観点で重要な依存関係を見落とします。

ウ：合理的な価値評価基準ではありません。

エ：依存関係は障害・攻撃の影響範囲に直結します。

総合解説：情報資産の価値は単体だけでなく、他資産や業務プロセスとの依存関係による波及影響も考慮すると適切です。 情報資産管理では、システムやデータだけでなく文書・施設・人材なども対象になり得ます。機密性・完全性・可用性の観点と事業影響を用い、保護の優先順位を決められるよう価値を明確化します。

対象：2026年度 / 基準日 2026-09-05

0006 情報資産管理 > 情報資産の特定・価値評価 ｜ 難易度：標準

情報資産を「公開」「社内限定」「機密」などに分類する主な目的として最も適切なものはどれか。

ア：すべての情報を同じ方法で扱うため。

イ：資産の重要度に応じて、アクセス制御や取扱方法など必要な保護レベルを定めやすくする。

ウ：資産台帳を不要にするため。

エ：利用者の判断で保護レベルを毎回自由に変えるため。

答え・解説 正答：イ

ア：分類は重要度に応じた差異を設けるための基盤です。

イ：分類は、資産の価値や保護要件を取扱ルールへ結び付けるために用います。

ウ：分類と台帳は補完関係にあります。

エ：組織の基準に基づく一貫した取扱いが必要です。

総合解説：分類は、資産の価値や保護要件を取扱ルールへ結び付けるために用います。 情報資産管理では、システムやデータだけでなく文書・施設・人材なども対象になり得ます。機密性・完全性・可用性の観点と事業影響を用い、保護の優先順位を決められるよう価値を明確化します。

対象：2026年度 / 基準日 2026-09-05

0007 情報資産管理 > 情報資産の特定・価値評価 ｜ 難易度：標準

営業部が会社未承認のクラウドストレージを顧客資料の共有に使っていることが判明した。最初の対応として最も適切なものはどれか。

ア：未承認なので存在しないものとして台帳に載せない。

イ：利用者全員に同じサービスの管理者権限を与える。

ウ：利用実態と保存情報を確認して情報資産として把握し、リスク評価と利用可否の判断につなげる。

エ：保存情報を確認せずに永久利用を認める。

答え・解説 正答：ウ

ア：管理対象外にするとリスクを把握できません。

イ：過大権限はリスクを高めます。

ウ：未承認サービスであっても業務で情報を扱っているなら、まず実態を把握し、資産・リスク管理の対象に取り込む必要があります。

エ：情報の重要度とサービスの安全性を評価する必要があります。

総合解説：未承認サービスであっても業務で情報を扱っているなら、まず実態を把握し、資産・リスク管理の対象に取り込む必要があります。 情報資産管理では、システムやデータだけでなく文書・施設・人材なども対象になり得ます。機密性・完全性・可用性の観点と事業影響を用い、保護の優先順位を決められるよう価値を明確化します。

対象：2026年度 / 基準日 2026-09-05

0008 情報資産管理 > 情報資産の特定・価値評価 ｜ 難易度：標準

情報資産の価値評価を一度決めた後も見直す必要がある理由として最も適切なものはどれか。

ア：価値評価は資産購入時だけ有効で、その後の利用状況とは無関係だから。

イ：システムは時間がたつほど必ず重要度が下がるから。

ウ：評価を変更すると監査できなくなるから。

エ：業務内容、法的要件、保存情報、利用者、システム構成などが変化し、漏えい・改ざん・停止時の影響も変わるため。

答え・解説 正答：エ

ア：利用状況の変化こそ見直し理由になります。

イ：必ず下がるとは限りません。

ウ：変更履歴を管理すれば監査可能です。

エ：情報資産の価値は固定ではなく、業務や技術、利用状況の変化に応じて変わり得ます。

総合解説：情報資産の価値は固定ではなく、業務や技術、利用状況の変化に応じて変わり得ます。 情報資産管理では、システムやデータだけでなく文書・施設・人材なども対象になり得ます。機密性・完全性・可用性の観点と事業影響を用い、保護の優先順位を決められるよう価値を明確化します。

対象：2026年度 / 基準日 2026-09-05

0009 情報資産管理 > 情報資産の特定・価値評価 ｜ 難易度：応用

限られた予算で優先的に保護すべき情報資産を決める際、最も妥当な判断基準はどれか。

ア：機密性・完全性・可用性が損なわれた場合の事業影響と、当該資産への依存度を総合して判断する。

イ：ファイル数が最も多い資産を無条件に最優先とする。

ウ：最も新しく購入した機器を最優先とする。

エ：担当者の好みだけで決める。

答え・解説 正答：ア

ア：重要資産の選定では単一指標に依存せず、CIAと事業影響、依存関係を総合して優先順位を付けます。

イ：量と重要度は一致しません。

ウ：購入時期は保護優先度の本質的基準ではありません。

エ：組織で定めた客観的基準が必要です。

総合解説：重要資産の選定では単一指標に依存せず、CIAと事業影響、依存関係を総合して優先順位を付けます。 情報資産管理では、システムやデータだけでなく文書・施設・人材なども対象になり得ます。機密性・完全性・可用性の観点と事業影響を用い、保護の優先順位を決められるよう価値を明確化します。

対象：2026年度 / 基準日 2026-09-05

0010 情報資産管理 > 情報資産の特定・価値評価 ｜ 難易度：応用

極めて重要な顧客DBが、外部接続のない堅牢な環境で厳格に管理されている。情報資産の「価値」と「リスク」の関係として最も適切なものはどれか。

ア：価値が高い資産は、どのような環境でもリスクが必ず最大になる。

イ：資産価値が高いこととリスクが高いことは同義ではなく、脅威や脆弱性、発生可能性なども含めてリスクを評価する。

ウ：管理策がある資産は価値をゼロと評価する。

エ：外部接続がない資産は情報資産ではない。

答え・解説 正答：イ

ア：脅威や脆弱性、管理策によりリスクは変わります。

イ：資産価値はリスクを構成する重要要素ですが、それだけでリスクの大きさは決まりません。脅威・脆弱性や発生可能性も考慮します。

ウ：管理策はリスクを下げ得ますが、資産価値を消しません。

エ：外部接続の有無は情報資産該当性を決めません。

総合解説：資産価値はリスクを構成する重要要素ですが、それだけでリスクの大きさは決まりません。脅威・脆弱性や発生可能性も考慮します。 情報資産管理では、システムやデータだけでなく文書・施設・人材なども対象になり得ます。機密性・完全性・可用性の観点と事業影響を用い、保護の優先順位を決められるよう価値を明確化します。

対象：2026年度 / 基準日 2026-09-05

0011 情報資産管理 > 情報資産台帳・棚卸・媒体管理 ｜ 難易度：基礎

情報資産台帳を作成する主な目的として最も適切なものはどれか。

ア：すべての情報資産を公開情報にする。

イ：資産の存在を記録せず、利用者の記憶に任せる。

ウ：組織が保有・利用する情報資産の所在、管理責任、分類などを把握し、適切な管理につなげる。

エ：購入価格だけを管理し、セキュリティ情報は記録しない。

答え・解説 正答：ウ

ア：台帳は公開を目的とするものではありません。

イ：把握漏れや責任不明確につながります。

ウ：情報資産台帳は、何を、どこで、誰が、どのような重要度で管理しているかを可視化する基盤です。

エ：セキュリティ管理には分類や責任者なども重要です。

総合解説：情報資産台帳は、何を、どこで、誰が、どのような重要度で管理しているかを可視化する基盤です。 情報資産台帳は、資産の存在・所在・管理責任・分類・利用状況を把握する基盤です。定期的な棚卸と媒体の持出し・保管・再利用・廃棄管理を組み合わせ、実態と記録のずれを減らします。

対象：2026年度 / 基準日 2026-09-05

0012 情報資産管理 > 情報資産台帳・棚卸・媒体管理 ｜ 難易度：基礎

情報資産台帳の項目として特に有用な組合せはどれか。

ア：資産名を省略し、担当者の好きな色だけを記録する。

イ：購入日のみを記録する。

ウ：資産の存在は記録せず、廃棄予定日だけを記録する。

エ：資産名、所在、管理責任者、重要度・分類、利用状況など。

答え・解説 正答：エ

ア：資産を識別できず管理に使えません。

イ：所在や責任、分類が分かりません。

ウ：ライフサイクル全体の管理に不足します。

エ：台帳には資産を一意に把握し、責任と保護レベルを追跡できる情報を記録します。

総合解説：台帳には資産を一意に把握し、責任と保護レベルを追跡できる情報を記録します。 情報資産台帳は、資産の存在・所在・管理責任・分類・利用状況を把握する基盤です。定期的な棚卸と媒体の持出し・保管・再利用・廃棄管理を組み合わせ、実態と記録のずれを減らします。

対象：2026年度 / 基準日 2026-09-05

0013 情報資産管理 > 情報資産台帳・棚卸・媒体管理 ｜ 難易度：基礎

情報資産の棚卸を定期的に行う主な目的はどれか。

ア：台帳の記録と実際の資産・利用状況を照合し、紛失、未登録、不要資産などを把握する。

イ：台帳の記録を一切確認せず、資産を増やす。

ウ：すべての資産を毎回廃棄する。

エ：棚卸後は責任者を不明にする。

答え・解説 正答：ア

ア：棚卸は台帳と実態の整合性を確認し、管理漏れや不要資産を発見するために行います。

イ：棚卸は照合・確認が中心です。

ウ：棚卸の目的は全廃棄ではありません。

エ：むしろ責任の明確化に役立ちます。

総合解説：棚卸は台帳と実態の整合性を確認し、管理漏れや不要資産を発見するために行います。 情報資産台帳は、資産の存在・所在・管理責任・分類・利用状況を把握する基盤です。定期的な棚卸と媒体の持出し・保管・再利用・廃棄管理を組み合わせ、実態と記録のずれを減らします。

対象：2026年度 / 基準日 2026-09-05

0014 情報資産管理 > 情報資産台帳・棚卸・媒体管理 ｜ 難易度：標準

棚卸で、台帳にない外付けSSDが部署内から見つかった。最も適切な対応はどれか。

ア：台帳にないので中身を確認せず自由利用を認める。

イ：所有者、保存情報、利用目的を確認し、承認状況とリスクを評価して台帳登録又は適切な処置を行う。

ウ：見つけた事実を記録せず元の場所へ戻す。

エ：全社員に同じSSDの共用を推奨する。

答え・解説 正答：イ

ア：未管理の媒体利用は情報漏えい等のリスクになります。

イ：未登録資産を見つけた場合は、単に放置せず、実態を確認して管理対象へ取り込むことが重要です。

ウ：差異が解消されません。

エ：利用範囲・責任がさらに不明確になります。

総合解説：未登録資産を見つけた場合は、単に放置せず、実態を確認して管理対象へ取り込むことが重要です。 情報資産台帳は、資産の存在・所在・管理責任・分類・利用状況を把握する基盤です。定期的な棚卸と媒体の持出し・保管・再利用・廃棄管理を組み合わせ、実態と記録のずれを減らします。

対象：2026年度 / 基準日 2026-09-05

0015 情報資産管理 > 情報資産台帳・棚卸・媒体管理 ｜ 難易度：標準

機密情報を保存したUSBメモリの社外持出し管理として最も適切なものはどれか。

ア：誰でも無記録で持ち出せるようにする。

イ：機密情報ほど暗号化を禁止する。

ウ：業務上の必要性と承認を確認し、暗号化、持出し記録、返却確認などを組み合わせる。

エ：返却確認をせず、持出し後は管理対象外とする。

答え・解説 正答：ウ

ア：紛失時に利用者や内容を追跡できません。

イ：紛失時の機密性保護に反します。

ウ：可搬媒体は紛失・盗難リスクが高いため、持出しの必要性、承認、保護、追跡を一連で管理します。

エ：媒体の所在管理ができません。

総合解説：可搬媒体は紛失・盗難リスクが高いため、持出しの必要性、承認、保護、追跡を一連で管理します。 情報資産台帳は、資産の存在・所在・管理責任・分類・利用状況を把握する基盤です。定期的な棚卸と媒体の持出し・保管・再利用・廃棄管理を組み合わせ、実態と記録のずれを減らします。

対象：2026年度 / 基準日 2026-09-05

0016 情報資産管理 > 情報資産台帳・棚卸・媒体管理 ｜ 難易度：標準

バックアップ媒体の保管として最も適切なものはどれか。

ア：誰でも出入りできる場所に内容表示付きで放置する。

イ：原本と同じ場所だけに保管し、災害リスクを考慮しない。

ウ：保管中は台帳から削除する。

エ：情報の重要度に応じてアクセスを制限し、環境条件や災害を考慮した保管場所を選ぶ。

答え・解説 正答：エ

ア：不正閲覧・持出しのリスクが高まります。

イ：同一災害で同時に失う可能性があります。

ウ：所在・責任の管理が必要です。

エ：バックアップ媒体も情報資産であり、機密性・完全性・可用性を維持できる保管が必要です。

総合解説：バックアップ媒体も情報資産であり、機密性・完全性・可用性を維持できる保管が必要です。 情報資産台帳は、資産の存在・所在・管理責任・分類・利用状況を把握する基盤です。定期的な棚卸と媒体の持出し・保管・再利用・廃棄管理を組み合わせ、実態と記録のずれを減らします。

対象：2026年度 / 基準日 2026-09-05

0017 情報資産管理 > 情報資産台帳・棚卸・媒体管理 ｜ 難易度：標準

機密情報を保存していたストレージを別部署で再利用する。最も適切な対応はどれか。

ア：媒体の種類と情報の機密性に応じたサニタイズを行い、必要に応じて実施結果を記録する。

イ：ファイル名だけ変更して再利用する。

ウ：ごみ箱に移動しただけで完全消去とみなす。

エ：保存情報が機密でも何もせず譲渡する。

答え・解説 正答：ア

ア：再利用時には以前の情報を復元されないよう、媒体特性と機密性に応じた消去・サニタイズを実施します。

イ：データ本体が残る可能性があります。

ウ：論理削除だけでは復元可能な場合があります。

エ：情報漏えいにつながるおそれがあります。

総合解説：再利用時には以前の情報を復元されないよう、媒体特性と機密性に応じた消去・サニタイズを実施します。 情報資産台帳は、資産の存在・所在・管理責任・分類・利用状況を把握する基盤です。定期的な棚卸と媒体の持出し・保管・再利用・廃棄管理を組み合わせ、実態と記録のずれを減らします。

対象：2026年度 / 基準日 2026-09-05

0018 情報資産管理 > 情報資産台帳・棚卸・媒体管理 ｜ 難易度：標準

SaaSを利用している場合の情報資産台帳の考え方として最も適切なものはどれか。

ア：自社所有サーバではないので一切管理しない。

イ：自社保有機器でなくても、利用するサービスや保存データ、管理責任、契約・利用状況を把握する。

ウ：クラウド上の情報は資産ではないとみなす。

エ：サービス名だけ記録し、保存情報や責任者を確認しない。

答え・解説 正答：イ

ア：外部サービス利用のリスクを把握できません。

イ：クラウドでは物理機器を所有しなくても、サービスとそこで扱う情報は資産・リスク管理の対象です。

ウ：業務情報は保護対象です。

エ：管理に必要な情報が不足します。

総合解説：クラウドでは物理機器を所有しなくても、サービスとそこで扱う情報は資産・リスク管理の対象です。 情報資産台帳は、資産の存在・所在・管理責任・分類・利用状況を把握する基盤です。定期的な棚卸と媒体の持出し・保管・再利用・廃棄管理を組み合わせ、実態と記録のずれを減らします。

対象：2026年度 / 基準日 2026-09-05

0019 情報資産管理 > 情報資産台帳・棚卸・媒体管理 ｜ 難易度：応用

情報資産の棚卸頻度を決める考え方として最も適切なものはどれか。

ア：重要度や変更頻度に関係なく、二度と棚卸しない。

イ：資産が多いほど棚卸を完全に廃止する。

ウ：資産の重要度、移動・変更の頻度、紛失リスクなどを考慮し、必要な頻度と方法を定める。

エ：利用者が退職したときだけ棚卸する。

答え・解説 正答：ウ

ア：台帳と実態の差異が累積します。

イ：資産数が多い場合は効率化が必要で、廃止が適切とは限りません。

ウ：棚卸は形式的に同一頻度とするより、資産特性とリスクに応じて実効性のある方法を設計することが重要です。

エ：他の変更・紛失を把握できません。

総合解説：棚卸は形式的に同一頻度とするより、資産特性とリスクに応じて実効性のある方法を設計することが重要です。 情報資産台帳は、資産の存在・所在・管理責任・分類・利用状況を把握する基盤です。定期的な棚卸と媒体の持出し・保管・再利用・廃棄管理を組み合わせ、実態と記録のずれを減らします。

対象：2026年度 / 基準日 2026-09-05

0020 情報資産管理 > 情報資産台帳・棚卸・媒体管理 ｜ 難易度：応用

ノートPCと暗号化USBを頻繁に社外へ持ち出す部門で、紛失事故の追跡ができない。最も有効な改善策の組合せはどれか。

ア：持出し記録だけ廃止し、自己申告に任せる。

イ：台帳から可搬媒体を除外する。

ウ：全媒体の識別番号を同じにする。

エ：資産台帳で識別・責任者・分類を管理し、持出し記録と定期棚卸を連携させる。

答え・解説 正答：エ

ア：追跡性が低下します。

イ：紛失リスクの高い資産を管理対象外にしてしまいます。

ウ：個々の資産を追跡できません。

エ：台帳だけ、持出し記録だけではなく、資産識別と移動履歴、定期的な実在確認を連携すると所在追跡性が高まります。

総合解説：台帳だけ、持出し記録だけではなく、資産識別と移動履歴、定期的な実在確認を連携すると所在追跡性が高まります。 情報資産台帳は、資産の存在・所在・管理責任・分類・利用状況を把握する基盤です。定期的な棚卸と媒体の持出し・保管・再利用・廃棄管理を組み合わせ、実態と記録のずれを減らします。

対象：2026年度 / 基準日 2026-09-05

0021 情報資産管理 > 管理責任・利用範囲・変更・廃棄 ｜ 難易度：基礎

情報資産の管理責任者に期待される役割として最も適切なものはどれか。

ア：資産の価値や利用目的を踏まえ、取扱ルールや利用範囲を明確にし、適切に管理されるようにする。

イ：資産を誰が利用してもよい状態にする。

ウ：資産の所在や利用状況を把握しない。

エ：廃棄時だけ関与し、利用中は一切管理しない。

答え・解説 正答：ア

ア：管理責任者は、情報資産の取扱いに関する責任と判断主体を明確にするために重要です。

イ：利用範囲は業務上の必要性に基づき管理します。

ウ：管理責任と矛盾します。

エ：ライフサイクル全体で管理が必要です。

総合解説：管理責任者は、情報資産の取扱いに関する責任と判断主体を明確にするために重要です。 情報資産には管理責任を明確にし、受入れ、利用、変更、返却、保存、廃棄までのライフサイクルを通じてルールを適用します。変更時には価値や利用範囲、アクセス権も再評価します。

対象：2026年度 / 基準日 2026-09-05

0022 情報資産管理 > 管理責任・利用範囲・変更・廃棄 ｜ 難易度：基礎

情報資産の「利用の許容範囲」を明確にする目的として最も適切なものはどれか。

ア：利用目的に関係なく全社員へ無制限に公開する。

イ：誰が、どの目的で、どのような条件の下で情報資産を利用できるかを定める。

ウ：資産の分類を無視して同一ルールにする。

エ：退職者にも従来どおり利用を認める。

答え・解説 正答：イ

ア：最小限の利用原則に反します。

イ：利用許容範囲は、業務上必要な利用と禁止・制限すべき利用の境界を明確にするために定めます。

ウ：重要度に応じた取扱いが必要です。

エ：利用資格がなくなれば見直しが必要です。

総合解説：利用許容範囲は、業務上必要な利用と禁止・制限すべき利用の境界を明確にするために定めます。 情報資産には管理責任を明確にし、受入れ、利用、変更、返却、保存、廃棄までのライフサイクルを通じてルールを適用します。変更時には価値や利用範囲、アクセス権も再評価します。

対象：2026年度 / 基準日 2026-09-05

0023 情報資産管理 > 管理責任・利用範囲・変更・廃棄 ｜ 難易度：基礎

外部委託先から新しいデータセットを受け入れる際の管理として最も適切なものはどれか。

ア：内容を確認せず共有フォルダへ置く。

イ：提供元を記録せず、責任者も決めない。

ウ：内容、提供元、利用目的、分類・重要度、保管場所、管理責任を確認して受入れ記録を残す。

エ：利用目的が不明でも永久保存する。

答え・解説 正答：ウ

ア：誤データや機密情報の無管理につながります。

イ：追跡性と責任が不明確になります。

ウ：情報資産の受入れ時点で、何をどの条件で管理するかを明確にすると、その後の利用・変更・廃棄まで一貫して管理できます。

エ：必要性と保存方針を確認すべきです。

総合解説：情報資産の受入れ時点で、何をどの条件で管理するかを明確にすると、その後の利用・変更・廃棄まで一貫して管理できます。 情報資産には管理責任を明確にし、受入れ、利用、変更、返却、保存、廃棄までのライフサイクルを通じてルールを適用します。変更時には価値や利用範囲、アクセス権も再評価します。

対象：2026年度 / 基準日 2026-09-05

0024 情報資産管理 > 管理責任・利用範囲・変更・廃棄 ｜ 難易度：標準

担当者がプロジェクトから外れた後も機密設計書へアクセスできる状態が残っている。最も適切な対応はどれか。

ア：過去に担当していたので永久にアクセスを認める。

イ：権限は本人が自主的に返却するまで維持する。

ウ：権限を削除する代わりにログ取得を停止する。

エ：担当変更を契機に利用許容範囲とアクセス権を見直し、不要な権限を速やかに削除する。

答え・解説 正答：エ

ア：現在の業務上の必要性に基づくべきです。

イ：組織側で確実に変更管理する必要があります。

ウ：ログ停止は適切な代替策ではありません。

エ：情報資産の利用範囲は人事・業務変更に応じて見直し、不要なアクセスを残さないことが重要です。

総合解説：情報資産の利用範囲は人事・業務変更に応じて見直し、不要なアクセスを残さないことが重要です。 情報資産には管理責任を明確にし、受入れ、利用、変更、返却、保存、廃棄までのライフサイクルを通じてルールを適用します。変更時には価値や利用範囲、アクセス権も再評価します。

対象：2026年度 / 基準日 2026-09-05

0025 情報資産管理 > 管理責任・利用範囲・変更・廃棄 ｜ 難易度：標準

顧客DBに新しい外部連携APIを追加する変更を行う。情報資産管理上、最も適切な対応はどれか。

ア：変更前に新たな利用経路やアクセス主体、データ項目を確認し、価値・リスク・利用範囲・管理策を再評価する。

イ：機能追加なのでセキュリティ評価は不要とする。

ウ：変更後も資産台帳や利用範囲は必ず旧内容のままにする。

エ：API利用者を無制限に増やしてから検討する。

答え・解説 正答：ア

ア：システム変更により情報の流れや脅威面が変わるため、変更管理にはセキュリティ影響の確認が必要です。

イ：外部連携は新たな攻撃面やデータ利用を生み得ます。

ウ：実態と管理情報がずれます。

エ：事前評価が必要です。

総合解説：システム変更により情報の流れや脅威面が変わるため、変更管理にはセキュリティ影響の確認が必要です。 情報資産には管理責任を明確にし、受入れ、利用、変更、返却、保存、廃棄までのライフサイクルを通じてルールを適用します。変更時には価値や利用範囲、アクセス権も再評価します。

対象：2026年度 / 基準日 2026-09-05

0026 情報資産管理 > 管理責任・利用範囲・変更・廃棄 ｜ 難易度：標準

業務上の利用が終了した機密データについて、最も適切な考え方はどれか。

ア：利用終了後は保存要件を確認せず永久保存する。

イ：法令・契約・業務上の保存要件を確認し、不要になった時点で承認された方法により安全に廃棄する。

ウ：保存期限前でも担当者の気分で削除する。

エ：機密性に関係なく単純削除だけで十分とする。

答え・解説 正答：イ

ア：不要情報の蓄積はリスクを増やします。

イ：不要な情報を無期限に保持すると漏えい時の影響が増えるため、保存要件と廃棄手順を明確にします。

ウ：法令・契約・業務要件に違反するおそれがあります。

エ：媒体・機密性に応じた廃棄方法が必要です。

総合解説：不要な情報を無期限に保持すると漏えい時の影響が増えるため、保存要件と廃棄手順を明確にします。 情報資産には管理責任を明確にし、受入れ、利用、変更、返却、保存、廃棄までのライフサイクルを通じてルールを適用します。変更時には価値や利用範囲、アクセス権も再評価します。

対象：2026年度 / 基準日 2026-09-05

0027 情報資産管理 > 管理責任・利用範囲・変更・廃棄 ｜ 難易度：標準

業務委託契約が終了する。委託先に顧客データのコピーが残っている可能性がある場合、最も適切な対応はどれか。

ア：契約終了と同時に委託先のコピーは自動消滅すると仮定する。

イ：データが機密でも廃棄確認は不要とする。

ウ：契約・手順に基づき返却又は安全な消去を求め、必要に応じて完了確認の証跡を得る。

エ：委託先のアカウントを永続的に有効にする。

答え・解説 正答：ウ

ア：実際に残存している可能性があります。

イ：漏えいリスクを残します。

ウ：委託終了時も情報資産の管理責任は消えません。返却・消去・アクセス停止を確認して残存リスクを抑えます。

エ：不要なアクセス経路が残ります。

総合解説：委託終了時も情報資産の管理責任は消えません。返却・消去・アクセス停止を確認して残存リスクを抑えます。 情報資産には管理責任を明確にし、受入れ、利用、変更、返却、保存、廃棄までのライフサイクルを通じてルールを適用します。変更時には価値や利用範囲、アクセス権も再評価します。

対象：2026年度 / 基準日 2026-09-05

0028 情報資産管理 > 管理責任・利用範囲・変更・廃棄 ｜ 難易度：標準

通常は禁止している私物端末への機密資料保存を、緊急業務のため一時的に認める必要が生じた。最も適切な管理はどれか。

ア：緊急なので承認も期限も設けない。

イ：一人に例外を認めたら全社員へ自動適用する。

ウ：例外利用の記録を残さない。

エ：例外の必要性とリスクを評価し、承認者、期限、条件、代替策、終了時のデータ消去を明確にする。

答え・解説 正答：エ

ア：例外が恒久化し、リスクを統制できません。

イ：個別リスクの評価が必要です。

ウ：事後確認や見直しができません。

エ：例外は無制限なルール逸脱ではなく、目的・期限・責任・補完策を定めて管理する必要があります。

総合解説：例外は無制限なルール逸脱ではなく、目的・期限・責任・補完策を定めて管理する必要があります。 情報資産には管理責任を明確にし、受入れ、利用、変更、返却、保存、廃棄までのライフサイクルを通じてルールを適用します。変更時には価値や利用範囲、アクセス権も再評価します。

対象：2026年度 / 基準日 2026-09-05

0029 情報資産管理 > 管理責任・利用範囲・変更・廃棄 ｜ 難易度：応用

基幹システムを廃止して新システムへ移行する際、情報資産管理として最も適切な一連の対応はどれか。

ア：データ移行の完全性を確認し、利用者権限と台帳を更新し、旧媒体・旧バックアップの保存要件を確認した上で安全に廃棄する。

イ：新システムが動けば旧データと旧媒体は管理しない。

ウ：旧システムの全アカウントを新システムへ無条件で複製する。

エ：台帳を更新せず、旧システムを現役として残す。

答え・解説 正答：ア

ア：システム移行では、移行データ、権限、台帳、旧媒体までを一つのライフサイクルとして管理することが重要です。

イ：残存データが漏えい源になり得ます。

ウ：不要権限まで引き継ぐおそれがあります。

エ：実態と記録が不一致になります。

総合解説：システム移行では、移行データ、権限、台帳、旧媒体までを一つのライフサイクルとして管理することが重要です。 情報資産には管理責任を明確にし、受入れ、利用、変更、返却、保存、廃棄までのライフサイクルを通じてルールを適用します。変更時には価値や利用範囲、アクセス権も再評価します。

対象：2026年度 / 基準日 2026-09-05

0030 情報資産管理 > 管理責任・利用範囲・変更・廃棄 ｜ 難易度：応用

人事部の給与データをIT部門が技術的に保管・バックアップしている。給与データの利用範囲や重要度を決める責任主体として最も妥当な考え方はどれか。

ア：バックアップを担当するIT部門だけが、業務目的に関係なく利用範囲を自由に決める。

イ：業務上の価値と利用目的を把握する人事側の管理責任者が判断し、IT部門は技術的管理を支援する。

ウ：給与データを閲覧する全社員が個別に重要度を決める。

エ：データの重要度は誰も決めず、障害後に決める。

答え・解説 正答：イ

ア：業務上の必要性を判断する責任者との連携が必要です。

イ：資産の業務価値・利用範囲を決める責任と、システムを技術的に運用する責任は分けて考えると統制が明確になります。

ウ：組織として一貫した責任体制が必要です。

エ：事前に価値と管理方針を明確化すべきです。

総合解説：資産の業務価値・利用範囲を決める責任と、システムを技術的に運用する責任は分けて考えると統制が明確になります。 情報資産には管理責任を明確にし、受入れ、利用、変更、返却、保存、廃棄までのライフサイクルを通じてルールを適用します。変更時には価値や利用範囲、アクセス権も再評価します。

対象：2026年度 / 基準日 2026-09-05

0031 リスクマネジメント > リスク特定・分析・評価 ｜ 難易度：基礎

情報セキュリティリスクアセスメントにおける「リスク特定」の説明として最も適切なものはどれか。

ア：既に選んだ管理策を導入する工程である。

イ：リスク受容基準と比較して受容可否を決める工程である。

ウ：対象資産に対して、どのような脅威や脆弱性、事象が損失につながり得るかを洗い出す。

エ：発生可能性と影響度を算定する工程だけを指す。

答え・解説 正答：ウ

ア：これはリスク対応に関する活動です。

イ：これはリスク評価に相当します。

ウ：リスク特定は、分析・評価に先立ってリスクの候補を明らかにする工程です。

エ：これは主にリスク分析です。

総合解説：リスク特定は、分析・評価に先立ってリスクの候補を明らかにする工程です。 リスクアセスメントは、リスク特定、リスク分析、リスク評価を区別して進めます。資産価値、脅威、脆弱性、発生可能性、結果の大きさを把握し、あらかじめ定めたリスク基準と比較して対応の必要性を判断します。

対象：2026年度 / 基準日 2026-09-05

0032 リスクマネジメント > リスク特定・分析・評価 ｜ 難易度：基礎

特定済みの情報セキュリティリスクについて、リスク分析で行うこととして最も適切なものはどれか。

ア：資産を廃棄してリスクをなくすことだけを指す。

イ：監査結果を経営会議へ報告することだけを指す。

ウ：リスクを受容するか否かを最終承認する工程だけを指す。

エ：特定したリスクについて、発生可能性と結果の大きさなどを見積もり、リスクレベルを求める。

答え・解説 正答：エ

ア：これはリスク回避の一例です。

イ：リスク分析の定義ではありません。

ウ：これはリスク評価や受容判断に関係します。

エ：分析では、特定されたリスクの性質と大きさを理解するため、可能性と影響を定性的又は定量的に評価します。

総合解説：分析では、特定されたリスクの性質と大きさを理解するため、可能性と影響を定性的又は定量的に評価します。 リスクアセスメントは、リスク特定、リスク分析、リスク評価を区別して進めます。資産価値、脅威、脆弱性、発生可能性、結果の大きさを把握し、あらかじめ定めたリスク基準と比較して対応の必要性を判断します。

対象：2026年度 / 基準日 2026-09-05

0033 リスクマネジメント > リスク特定・分析・評価 ｜ 難易度：基礎

分析によって得たリスクレベルを、組織のリスク基準と照合する段階で行うこととして最も適切なものはどれか。

ア：分析で得たリスクレベルをリスク基準と比較し、対応の必要性や優先度を判断する。

イ：資産一覧を作ることだけを指す。

ウ：バックアップを取得することだけを指す。

エ：脅威を発見した時点で全て同じ優先度にする。

答え・解説 正答：ア

ア：リスク評価は、分析結果を組織のリスク受容基準などと比較して意思決定につなげる工程です。

イ：これは資産管理・リスク特定の準備に当たります。

ウ：これは管理策の一例です。

エ：リスク基準と比較して優先度を判断します。

総合解説：リスク評価は、分析結果を組織のリスク受容基準などと比較して意思決定につなげる工程です。 リスクアセスメントは、リスク特定、リスク分析、リスク評価を区別して進めます。資産価値、脅威、脆弱性、発生可能性、結果の大きさを把握し、あらかじめ定めたリスク基準と比較して対応の必要性を判断します。

対象：2026年度 / 基準日 2026-09-05

0034 リスクマネジメント > リスク特定・分析・評価 ｜ 難易度：基礎

「外部からの不正アクセス」という脅威が存在しても、対象システムの脆弱性や露出状況によってリスクが変わる理由として最も適切なものはどれか。

ア：脅威が存在すれば全資産のリスクは必ず同一になるため。

イ：リスクは脅威の存在だけでなく、脆弱性、資産価値、発生可能性、結果の大きさなどの組合せで変化するため。

ウ：脆弱性はリスクに影響しないため。

エ：資産価値はリスク評価では考慮しないため。

答え・解説 正答：イ

ア：資産ごとの条件により異なります。

イ：脅威とリスクは同義ではありません。同じ脅威でも、脆弱性や資産の重要度、対策状況によってリスクレベルは異なります。

ウ：脆弱性は重要な要素です。

エ：シラバスでも資産価値を分析要素としています。

総合解説：脅威とリスクは同義ではありません。同じ脅威でも、脆弱性や資産の重要度、対策状況によってリスクレベルは異なります。 リスクアセスメントは、リスク特定、リスク分析、リスク評価を区別して進めます。資産価値、脅威、脆弱性、発生可能性、結果の大きさを把握し、あらかじめ定めたリスク基準と比較して対応の必要性を判断します。

対象：2026年度 / 基準日 2026-09-05

0035 リスクマネジメント > リスク特定・分析・評価 ｜ 難易度：標準

発生可能性を「低・中・高」、影響度を「小・中・大」で評価し、その組合せでリスクレベルを決める方法として最も近いものはどれか。

ア：公開鍵暗号方式による評価。

イ：パリティチェックによる評価。

ウ：リスクマトリックスを用いた定性的又は半定量的な評価。

エ：ラウンドロビンによる評価。

答え・解説 正答：ウ

ア：暗号方式でありリスク評価法ではありません。

イ：データ誤り検出の仕組みです。

ウ：リスクマトリックスは、発生可能性と影響度などの区分を組み合わせてリスクレベルを可視化する方法です。

エ：処理割当て等の方式でありリスク評価法ではありません。

総合解説：リスクマトリックスは、発生可能性と影響度などの区分を組み合わせてリスクレベルを可視化する方法です。 リスクアセスメントは、リスク特定、リスク分析、リスク評価を区別して進めます。資産価値、脅威、脆弱性、発生可能性、結果の大きさを把握し、あらかじめ定めたリスク基準と比較して対応の必要性を判断します。

対象：2026年度 / 基準日 2026-09-05

0036 リスクマネジメント > リスク特定・分析・評価 ｜ 難易度：標準

1回の事故による予想損失額が200万円、年間発生率が0.25回と見積もられた。単純化した年間予想損失額（ALE）の考え方として最も適切なものはどれか。

ア：1回当たり損失額と年間発生率を加算し、200.25万円／年と見積もる。

イ：1回当たり損失額を年間発生率で割り、800万円／年と見積もる。

ウ：年間発生率が1未満なら損失額は0円とする。

エ：1回当たり損失額に年間発生率を乗じ、50万円／年と見積もる。

答え・解説 正答：エ

ア：ALEは損失額と発生率を加算して求めるものではありません。

イ：ALEは1回当たり損失額を年間発生率で除算して求めるものではありません。

ウ：年間発生率が1未満でも期待損失は0にはなりません。

エ：単純化した定量評価では、1回当たり損失額に年間発生率を乗じて年間予想損失額を求めます。

総合解説：単純化した定量評価では、1回当たり損失額に年間発生率を乗じて年間予想損失額を求める考え方があります。 リスクアセスメントは、リスク特定、リスク分析、リスク評価を区別して進めます。資産価値、脅威、脆弱性、発生可能性、結果の大きさを把握し、あらかじめ定めたリスク基準と比較して対応の必要性を判断します。

対象：2026年度 / 基準日 2026-09-05

0037 リスクマネジメント > リスク特定・分析・評価 ｜ 難易度：標準

リスク受容基準をリスク評価の前に明確にしておく利点として最も適切なものはどれか。

ア：担当者ごとの場当たり的な判断を減らし、分析結果を一貫した基準で比較・評価できる。

イ：全てのリスクを必ずゼロにできる。

ウ：リスク分析自体を不要にできる。

エ：管理策の費用を必ず0円にできる。

答え・解説 正答：ア

ア：リスク基準は、どの程度のリスクを受容できるかを組織として判断する物差しになります。

イ：基準を定めてもリスクが自動的にゼロにはなりません。

ウ：基準との比較には分析結果が必要です。

エ：費用とは無関係です。

総合解説：リスク基準は、どの程度のリスクを受容できるかを組織として判断する物差しになります。リスクアセスメントは、リスク特定、リスク分析、リスク評価を区別して進めます。資産価値、脅威、脆弱性、発生可能性、結果の大きさを把握し、あらかじめ定めたリスク基準と比較して対応の必要性を判断します。

対象：2026年度 / 基準日 2026-09-05

0038 リスクマネジメント > リスク特定・分析・評価 ｜ 難易度：標準

社内だけで利用していたシステムをインターネット公開することになった。リスクマネジメント上、最も適切な対応はどれか。

ア：同じシステムなので過去の評価を永久に固定する。

イ：公開により脅威・攻撃面・発生可能性が変わるため、新たなリスクを特定し再評価する。

ウ：公開後に事故が起きるまで評価しない。

エ：公開した時点で全リスクが自動的に受容済みとなる。

答え・解説 正答：イ

ア：利用環境の変更でリスクは変化します。

イ：シラバスは、情報システムや組織の変更、新種の脅威に伴う新たなリスクも特定・評価できることを求めています。

ウ：事前に評価すべきです。

エ：受容には基準と判断が必要です。

総合解説：シラバスは、情報システムや組織の変更、新種の脅威に伴う新たなリスクも特定・評価できることを求めています。 リスクアセスメントは、リスク特定、リスク分析、リスク評価を区別して進めます。資産価値、脅威、脆弱性、発生可能性、結果の大きさを把握し、あらかじめ定めたリスク基準と比較して対応の必要性を判断します。

対象：2026年度 / 基準日 2026-09-05

0039 リスクマネジメント > リスク特定・分析・評価 ｜ 難易度：標準

リスク所有者（リスクオーナー）の説明として最も適切なものはどれか。

ア：リスクを発見した利用者は全員、自動的に同一の最終承認権を持つ。

イ：システムの利用者数を数えるだけの担当者。

ウ：特定のリスクについて、管理・対応に関する説明責任と権限を持つ者。

エ：リスクを隠蔽する権限を持つ者。

答え・解説 正答：ウ

ア：組織として責任と権限を定める必要があります。

イ：リスク管理の責任主体という役割ではありません。

ウ：リスク所有者を明確にすることで、対応方針や受容判断が誰の責任で行われるかを明確にできます。

エ：リスクは適切に報告・管理する必要があります。

総合解説：リスク所有者を明確にすることで、対応方針や受容判断が誰の責任で行われるかを明確にできます。 リスクアセスメントは、リスク特定、リスク分析、リスク評価を区別して進めます。資産価値、脅威、脆弱性、発生可能性、結果の大きさを把握し、あらかじめ定めたリスク基準と比較して対応の必要性を判断します。

対象：2026年度 / 基準日 2026-09-05

0040 リスクマネジメント > リスク特定・分析・評価 ｜ 難易度：標準

リスク登録簿を利用する主な目的として最も適切なものはどれか。

ア：リスクを登録した時点で対応不要とする。

イ：インシデントが起きたリスクだけを後から登録する。

ウ：所有者や対応状況を記録しない。

エ：特定したリスク、評価結果、所有者、対応状況などを記録し、継続的に追跡できるようにする。

答え・解説 正答：エ

ア：登録は管理開始であり対応完了ではありません。

イ：将来リスクも事前に管理します。

ウ：追跡性が低下します。

エ：リスク登録簿は、リスクを一過性の評価で終わらせず、責任・対応・進捗を継続的に管理するための記録です。

総合解説：リスク登録簿は、リスクを一過性の評価で終わらせず、責任・対応・進捗を継続的に管理するための記録です。 リスクアセスメントは、リスク特定、リスク分析、リスク評価を区別して進めます。資産価値、脅威、脆弱性、発生可能性、結果の大きさを把握し、あらかじめ定めたリスク基準と比較して対応の必要性を判断します。

対象：2026年度 / 基準日 2026-09-05

0041 リスクマネジメント > リスク特定・分析・評価 ｜ 難易度：応用

リスクAは「発生可能性は高いが影響は小」、リスクBは「発生可能性は低いが影響は極めて大」。どちらを優先すべきか問われた。最も適切な答えはどれか。

ア：組織のリスク基準に従い、発生可能性と影響度を組み合わせて両方を評価して決める。

イ：発生可能性だけを見て必ずAを優先する。

ウ：影響度だけを見て必ずBを優先する。

エ：どちらも条件が異なるため評価不能として放置する。

答え・解説 正答：ア

ア：一方の要素だけで優先順位を決めると、重大事故や頻発事故を適切に比較できません。組織の基準に基づく総合評価が必要です。

イ：影響度を無視しています。

ウ：発生可能性を無視しています。

エ：定めたリスク基準で比較します。

総合解説：一方の要素だけで優先順位を決めると、重大事故や頻発事故を適切に比較できません。組織の基準に基づく総合評価が必要です。 リスクアセスメントは、リスク特定、リスク分析、リスク評価を区別して進めます。資産価値、脅威、脆弱性、発生可能性、結果の大きさを把握し、あらかじめ定めたリスク基準と比較して対応の必要性を判断します。

対象：2026年度 / 基準日 2026-09-05

0042 リスクマネジメント > リスク特定・分析・評価 ｜ 難易度：応用

新しい脅威で発生可能性の実績データが乏しい場合のリスク評価として最も適切なものはどれか。

ア：データが少ないのでリスクは必ず0とする。

イ：利用可能な情報と専門家判断を用いて仮定や不確実性を明示し、追加情報に応じて再評価する。

ウ：最悪値だけを根拠なく固定し、二度と見直さない。

エ：不確実性を隠して確定値として報告する。

答え・解説 正答：イ

ア：未知を安全とみなす根拠はありません。

イ：不確実性があるから評価を中止するのではなく、前提を明確にした上で判断し、情報更新に応じて見直すことが実務的です。

ウ：新情報に応じた再評価が必要です。

エ：意思決定者が評価の限界を理解できません。

総合解説：不確実性があるから評価を中止するのではなく、前提を明確にした上で判断し、情報更新に応じて見直すことが実務的です。 リスクアセスメントは、リスク特定、リスク分析、リスク評価を区別して進めます。資産価値、脅威、脆弱性、発生可能性、結果の大きさを把握し、あらかじめ定めたリスク基準と比較して対応の必要性を判断します。

対象：2026年度 / 基準日 2026-09-05

0043 リスクマネジメント > リスク対応策・管理策の選択 ｜ 難易度：基礎

あるオンライン機能の提供によるリスクが組織の受容範囲を大きく超えるため、その機能の提供自体を中止した。この対応に最も近いものはどれか。

ア：ファイアウォールを追加して発生可能性を下げる。

イ：サイバー保険に加入する。

ウ：許容できないリスクを伴う業務や機能そのものを中止し、リスクの原因となる活動を行わない。

エ：何もせずリスクを受け入れる。

答え・解説 正答：ウ

ア：これは主にリスク低減です。

イ：これは損失の一部を共有・移転する対応です。

ウ：リスク回避は、リスクを生む活動を開始しない又は中止することで、そのリスクを避ける対応です。

エ：これはリスク保有・受容です。

総合解説：リスク回避は、リスクを生む活動を開始しない又は中止することで、そのリスクを避ける対応です。 リスク対応は、回避、低減・修正、共有・移転、保有などから状況に応じて選択します。管理策は組織的・人的・物理的・技術的な観点を組み合わせ、費用だけでなくリスク低減効果と実行可能性を評価します。

対象：2026年度 / 基準日 2026-09-05

0044 リスクマネジメント > リスク対応策・管理策の選択 ｜ 難易度：基礎

不正ログインのリスクに対して多要素認証とアクセス制御を導入し、発生可能性を下げた。この対応に最も近いものはどれか。

ア：対象サービスを廃止する。

イ：リスクを理解した上で何も追加対策せず受容する。

ウ：保険だけで全ての攻撃を防げるとみなす。

エ：多要素認証やアクセス制御を導入し、不正アクセスの発生可能性又は影響を小さくする。

答え・解説 正答：エ

ア：これはリスク回避に当たります。

イ：これはリスク保有です。

ウ：保険は技術的な攻撃防止策ではありません。

エ：管理策を導入してリスクの可能性や影響を下げることは、代表的なリスク低減・修正です。

総合解説：管理策を導入してリスクの可能性や影響を下げることは、代表的なリスク低減・修正です。リスク対応は、回避、低減・修正、共有・移転、保有などから状況に応じて選択します。管理策は組織的・人的・物理的・技術的な観点を組み合わせ、費用だけでなくリスク低減効果と実行可能性を評価します。

対象：2026年度 / 基準日 2026-09-05

0045 リスクマネジメント > リスク対応策・管理策の選択 ｜ 難易度：基礎

リスク共有（移転）の例として最も適切なものはどれか。

ア：サイバー保険を利用し、事故発生時の財務的損失の一部を保険会社と共有する。

イ：脆弱な機能を廃止する。

ウ：アクセス権を必要最小限にする。

エ：事故損失を全額自社で負担すると決める。

答え・解説 正答：ア

ア：保険や契約は、損失の一部を第三者と共有・移転する手段になり得ます。ただしリスクや責任が完全に消えるわけではありません。

イ：これは回避の例です。

ウ：これは低減の例です。

エ：これは保有の例です。

総合解説：保険や契約は、損失の一部を第三者と共有・移転する手段になり得ます。ただしリスクや責任が完全に消えるわけではありません。 リスク対応は、回避、低減・修正、共有・移転、保有などから状況に応じて選択します。管理策は組織的・人的・物理的・技術的な観点を組み合わせ、費用だけでなくリスク低減効果と実行可能性を評価します。

対象：2026年度 / 基準日 2026-09-05

0046 リスクマネジメント > リスク対応策・管理策の選択 ｜ 難易度：標準

年間予想損失が小さい低リスクに対し、非常に高額な対策案しかない。最も適切な考え方はどれか。

ア：対策費が高いほど必ず最適なので無条件で導入する。

イ：リスク受容基準と対策の費用・効果を比較し、低減以外の対応も含めて合理的に選択する。

ウ：低リスクなので評価記録を削除する。

エ：受容基準に関係なく、全リスクを同じ対策で処理する。

答え・解説 正答：イ

ア：費用対効果やリスク水準を無視しています。

イ：全リスクに最大コストの管理策を適用するのではなく、リスクの大きさと対策効果・コストを比較して選びます。

ウ：判断根拠の記録は重要です。

エ：リスクに応じた選択が必要です。

総合解説：全リスクに最大コストの管理策を適用するのではなく、リスクの大きさと対策効果・コストを比較して選びます。 リスク対応は、回避、低減・修正、共有・移転、保有などから状況に応じて選択します。管理策は組織的・人的・物理的・技術的な観点を組み合わせ、費用だけでなくリスク低減効果と実行可能性を評価します。

対象：2026年度 / 基準日 2026-09-05

0047 リスクマネジメント > リスク対応策・管理策の選択 ｜ 難易度：標準

情報セキュリティ管理策を「組織的・人的・物理的・技術的」に分けて検討する目的として最も適切なものはどれか。

ア：技術的管理策だけで全リスクを必ず解決するため。

イ：分類ごとに相互連携を禁止するため。

ウ：一つの観点に偏らず、リスクに対して複数の側面から必要な対策を検討する。

エ：管理策の有効性評価を不要にするため。

答え・解説 正答：ウ

ア：人的・物理的・組織的なリスクもあります。

イ：実務では組み合わせて対策します。

ウ：シラバスは、組織的、人的、物理的、技術的な管理策の区分を示しており、複数層の対策設計に役立ちます。

エ：導入後の評価は必要です。

総合解説：シラバスは、組織的、人的、物理的、技術的な管理策の区分を示しており、複数層の対策設計に役立ちます。 リスク対応は、回避、低減・修正、共有・移転、保有などから状況に応じて選択します。管理策は組織的・人的・物理的・技術的な観点を組み合わせ、費用だけでなくリスク低減効果と実行可能性を評価します。

対象：2026年度 / 基準日 2026-09-05

0048 リスクマネジメント > リスク対応策・管理策の選択 ｜ 難易度：標準

ランサムウェア対策として、予防・検知・是正の観点を組み合わせた例として最も適切なものはどれか。

ア：バックアップだけ用意し、アクセス制御も監視も不要とする。

イ：ログ監視だけ行い、復旧手段を用意しない。

ウ：パッチ適用だけで全ての攻撃を完全に防げるとする。

エ：パッチ適用や権限制御で予防し、EDRやログ監視で検知し、バックアップからの復旧手順で是正・復旧に備える。

答え・解説 正答：エ

ア：予防・検知が欠けます。

イ：検知後の復旧が困難です。

ウ：未知の脅威や他の侵入経路があります。

エ：一種類の管理策に依存せず、予防、検知、是正・復旧を組み合わせると、単一策が破られた場合の影響を抑えやすくなります。

総合解説：一種類の管理策に依存せず、予防、検知、是正・復旧を組み合わせると、単一策が破られた場合の影響を抑えやすくなります。 リスク対応は、回避、低減・修正、共有・移転、保有などから状況に応じて選択します。管理策は組織的・人的・物理的・技術的な観点を組み合わせ、費用だけでなくリスク低減効果と実行可能性を評価します。

対象：2026年度 / 基準日 2026-09-05

0049 リスクマネジメント > リスク対応策・管理策の選択 ｜ 難易度：標準

クラウド事業者と契約し、一部のセキュリティ運用を委託した。リスク対応として最も適切な考え方はどれか。

ア：一部の作業や損失を共有できても、自組織の説明責任や残留リスクの確認まで消えるわけではない。

イ：契約した時点で自組織はセキュリティ確認を一切しなくてよい。

ウ：委託先で事故が起きても自組織への影響は絶対にない。

エ：リスク共有は必ずリスク回避と同じ結果になる。

答え・解説 正答：ア

ア：委託や保険によるリスク共有は、自組織の責任を完全に消滅させるものではありません。契約・責任分担と残留リスクを確認します。

イ：利用者側に残る責任があります。

ウ：データや業務への影響があり得ます。

エ：活動自体をやめる回避とは異なります。

総合解説：委託や保険によるリスク共有は、自組織の責任を完全に消滅させるものではありません。契約・責任分担と残留リスクを確認します。 リスク対応は、回避、低減・修正、共有・移転、保有などから状況に応じて選択します。管理策は組織的・人的・物理的・技術的な観点を組み合わせ、費用だけでなくリスク低減効果と実行可能性を評価します。

対象：2026年度 / 基準日 2026-09-05

0050 リスクマネジメント > リスク対応策・管理策の選択 ｜ 難易度：標準

新たなリスク対応策を決める前に、現在の管理策の実施状況を確認する理由として最も適切なものはどれか。

ア：既存管理策はリスクに影響しないため確認不要である。

イ：既に実施している対策と不足部分を把握し、重複投資や対策漏れを避けるため。

ウ：同じ製品を重複購入することが目的である。

エ：確認するとリスク受容基準が不要になる。

答え・解説 正答：イ

ア：既存管理策は現状リスクに影響します。

イ：シラバスは、検討した対応策について現在の実施状況を把握できることも求めています。

ウ：重複投資を避けるべきです。

エ：受容基準は別途必要です。

総合解説：シラバスは、検討した対応策について現在の実施状況を把握できることも求めています。 リスク対応は、回避、低減・修正、共有・移転、保有などから状況に応じて選択します。管理策は組織的・人的・物理的・技術的な観点を組み合わせ、費用だけでなくリスク低減効果と実行可能性を評価します。

対象：2026年度 / 基準日 2026-09-05

0051 リスクマネジメント > リスク対応策・管理策の選択 ｜ 難易度：応用

機密ファイルの誤送信リスクに対し、利用者教育だけでは事故が続いている。次の一手として最も適切なものはどれか。

ア：教育を中止し、何の対策も追加しない。

イ：全社員に管理者権限を与える。

ウ：教育を継続しつつ、宛先確認、DLP、送信保留、権限・共有設定など技術的・組織的管理策を組み合わせる。

エ：誤送信を検知したログを全て削除する。

答え・解説 正答：ウ

ア：事故が続いているリスクを放置します。

イ：誤操作や不正の影響を拡大します。

ウ：人的対策だけで十分でない場合、組織的・技術的な管理策を組み合わせて防御を多層化します。

エ：改善に必要な証跡を失います。

総合解説：人的対策だけで十分でない場合、組織的・技術的な管理策を組み合わせて防御を多層化します。 リスク対応は、回避、低減・修正、共有・移転、保有などから状況に応じて選択します。管理策は組織的・人的・物理的・技術的な観点を組み合わせ、費用だけでなくリスク低減効果と実行可能性を評価します。

対象：2026年度 / 基準日 2026-09-05

0052 リスクマネジメント > リスク対応策・管理策の選択 ｜ 難易度：応用

管理策を導入した後のリスクマネジメントとして最も適切なものはどれか。

ア：導入した時点でリスクは必ず0になるとみなす。

イ：導入後はリスク登録簿を削除する。

ウ：有効性が低くても同じ対策を永久に固定する。

エ：管理策が想定どおり実施されているか、有効かを確認し、残留リスクを再評価して必要なら追加対応する。

答え・解説 正答：エ

ア：完全に消えないリスクが一般的です。

イ：継続的な追跡が必要です。

ウ：見直しと改善が必要です。

エ：管理策導入は終点ではありません。実施状況と有効性を確認し、残留リスクを評価して対応を更新します。

総合解説：管理策導入は終点ではありません。実施状況と有効性を確認し、残留リスクを評価して対応を更新します。 リスク対応は、回避、低減・修正、共有・移転、保有などから状況に応じて選択します。管理策は組織的・人的・物理的・技術的な観点を組み合わせ、費用だけでなくリスク低減効果と実行可能性を評価します。

対象：2026年度 / 基準日 2026-09-05

0053 リスクマネジメント > 残留リスク・優先順位・リスク対応計画 ｜ 難易度：基礎

アクセス制御などの対策を実施した後にも一定の危険が残っている。この「対策後に残るリスク」を表す用語はどれか。

ア：リスク対応策を実施した後にも残っているリスク。

イ：まだ特定されていないリスクだけを指す。

ウ：既に完全に消滅したリスクを指す。

エ：資産価値そのものを指す。

答え・解説 正答：ア

ア：管理策を導入してもリスクが完全に消えるとは限らず、残ったリスクを残留リスクとして評価します。

イ：残留リスクは対応後に残るリスクです。

ウ：消滅したリスクではありません。

エ：資産価値とリスクは別概念です。

総合解説：管理策を導入してもリスクが完全に消えるとは限らず、残ったリスクを残留リスクとして評価します。 管理策を実施しても残るリスクが残留リスクです。受容可否を権限ある者が判断し、リスクの大きさ、期限、資源などを踏まえて優先順位を付け、実施項目・資源・責任者・完了予定時期・評価方法を対応計画に落とし込みます。

対象：2026年度 / 基準日 2026-09-05

0054 リスクマネジメント > 残留リスク・優先順位・リスク対応計画 ｜ 難易度：基礎

リスク対応計画に記載する内容として最も適切な組合せはどれか。

ア：問題名だけを書き、責任者や期限は記載しない。

イ：実施項目、必要な資源、責任者、完了予定時期、実施結果の評価方法。

ウ：担当者の私的な感想だけを記載する。

エ：完了予定時期を永久に未定とし、評価方法も決めない。

答え・解説 正答：イ

ア：実行管理に必要な情報が不足します。

イ：IPAシラバスは、リスク対応計画の記載内容として実施項目、資源、責任者、完了予定時期、実施結果の評価方法などを示しています。

ウ：計画として必要な実施情報がありません。

エ：進捗・効果を管理できません。

総合解説：IPAシラバスは、リスク対応計画の記載内容として実施項目、資源、責任者、完了予定時期、実施結果の評価方法などを示しています。 管理策を実施しても残るリスクが残留リスクです。受容可否を権限ある者が判断し、リスクの大きさ、期限、資源などを踏まえて優先順位を付け、実施項目・資源・責任者・完了予定時期・評価方法を対応計画に落とし込みます。

対象：2026年度 / 基準日 2026-09-05

0055 リスクマネジメント > 残留リスク・優先順位・リスク対応計画 ｜ 難易度：標準

管理策導入後の残留リスクが組織の受容基準以下になった。次の対応として最も適切なものはどれか。

ア：基準以下なら記録を全て削除する。

イ：誰の承認もなく自動的に永久受容とする。

ウ：権限あるリスク所有者などが判断根拠を確認して受容し、必要な監視を継続する。

エ：残留リスクがあること自体を隠す。

答え・解説 正答：ウ

ア：判断根拠と履歴を残すことが重要です。

イ：責任と権限を明確にします。

ウ：基準以下でも、リスク受容は責任ある判断として記録し、環境変化に備えて監視します。

エ：意思決定者への適切な情報提供が必要です。

総合解説：基準以下でも、リスク受容は責任ある判断として記録し、環境変化に備えて監視します。 管理策を実施しても残るリスクが残留リスクです。受容可否を権限ある者が判断し、リスクの大きさ、期限、資源などを踏まえて優先順位を付け、実施項目・資源・責任者・完了予定時期・評価方法を対応計画に落とし込みます。

対象：2026年度 / 基準日 2026-09-05

0056 リスクマネジメント > 残留リスク・優先順位・リスク対応計画 ｜ 難易度：標準

対応待ちのリスクが多数ある。優先順位を決める方法として最も適切なものはどれか。

ア：発見された順だけで固定する。

イ：担当者の好みだけで決める。

ウ：全リスクを同時に最高優先度にする。

エ：リスクレベル、受容基準、被害の重大性、対応期限、対策に必要な資源などを踏まえて決める。

答え・解説 正答：エ

ア：重大なリスクが後回しになる可能性があります。

イ：一貫したリスク基準が必要です。

ウ：資源配分上の優先順位になりません。

エ：優先順位は単純な発見順ではなく、リスクと実行条件を総合して決めます。

総合解説：優先順位は単純な発見順ではなく、リスクと実行条件を総合して決めます。 管理策を実施しても残るリスクが残留リスクです。受容可否を権限ある者が判断し、リスクの大きさ、期限、資源などを踏まえて優先順位を付け、実施項目・資源・責任者・完了予定時期・評価方法を対応計画に落とし込みます。

対象：2026年度 / 基準日 2026-09-05

0057 リスクマネジメント > 残留リスク・優先順位・リスク対応計画 ｜ 難易度：標準

重大リスクの対策が予定日までに完了できないことが判明した。最も適切な対応はどれか。

ア：遅延による残留リスクを再評価し、責任者・リスク所有者へ報告して暫定策や期限変更の承認を得る。

イ：進捗表だけ完了に書き換える。

ウ：担当者だけで無期限延期を決める。

エ：監視を停止して問題を見えなくする。

答え・解説 正答：ア

ア：計画遅延はリスク状態の変化として扱い、隠さず再評価とエスカレーションを行います。

イ：実態と記録が不一致になりリスクが残ります。

ウ：重大リスクでは責任ある承認が必要です。

エ：リスク低減にはなりません。

総合解説：計画遅延はリスク状態の変化として扱い、隠さず再評価とエスカレーションを行います。 管理策を実施しても残るリスクが残留リスクです。受容可否を権限ある者が判断し、リスクの大きさ、期限、資源などを踏まえて優先順位を付け、実施項目・資源・責任者・完了予定時期・評価方法を対応計画に落とし込みます。

対象：2026年度 / 基準日 2026-09-05

0058 リスクマネジメント > 残留リスク・優先順位・リスク対応計画 ｜ 難易度：標準

リスク対応計画を「完了」とする前に確認すべき事項として最も適切なものはどれか。

ア：製品を購入した時点で効果確認を省略する。

イ：対策が実施された事実だけでなく、想定したリスク低減効果が得られ、残留リスクが許容可能かを確認する。

ウ：担当者が忙しければ残留リスクを評価しない。

エ：計画書を削除すれば完了とみなす。

答え・解説 正答：イ

ア：導入しても設定不備や運用不足があり得ます。

イ：作業完了とリスク低減効果は別です。計画の評価方法に従い、残留リスクを確認して終了判断します。

ウ：受容可否の判断ができません。

エ：実施結果を確認する必要があります。

総合解説：作業完了とリスク低減効果は別です。計画の評価方法に従い、残留リスクを確認して終了判断します。 管理策を実施しても残るリスクが残留リスクです。受容可否を権限ある者が判断し、リスクの大きさ、期限、資源などを踏まえて優先順位を付け、実施項目・資源・責任者・完了予定時期・評価方法を対応計画に落とし込みます。

対象：2026年度 / 基準日 2026-09-05

0059 リスクマネジメント > 残留リスク・優先順位・リスク対応計画 ｜ 難易度：応用

予算と人員が限られ、全リスク対策を同時に実施できない。最も適切な計画の立て方はどれか。

ア：全て無期限保留にする。

イ：低リスクだけ先に全予算を使う。

ウ：高リスク項目を優先しつつ、短期の暫定策と中長期の恒久策を分け、責任者・期限・必要資源を明確にする。

エ：期限も責任者も設定しない。

答え・解説 正答：ウ

ア：重大リスクへの対応責任を果たせません。

イ：優先順位がリスクに基づいていません。

ウ：資源制約がある場合でも、重大リスクを放置せず、優先順位と段階的な対応計画を設計します。

エ：実行可能な計画になりません。

総合解説：資源制約がある場合でも、重大リスクを放置せず、優先順位と段階的な対応計画を設計します。 管理策を実施しても残るリスクが残留リスクです。受容可否を権限ある者が判断し、リスクの大きさ、期限、資源などを踏まえて優先順位を付け、実施項目・資源・責任者・完了予定時期・評価方法を対応計画に落とし込みます。

対象：2026年度 / 基準日 2026-09-05

0060 リスクマネジメント > 残留リスク・優先順位・リスク対応計画 ｜ 難易度：応用

新サービスの開始前に残留リスクが受容基準をわずかに上回っているが、事業上の開始期限も重要である。最も適切な対応はどれか。

ア：現場担当者が記録を残さず独断で開始する。

イ：受容基準をその場だけ書き換えて問題を消す。

ウ：リスク情報を経営層に知らせない。

エ：リスク所有者と意思決定者に残留リスクと選択肢を提示し、追加管理策、条件付き開始、延期などを正式に判断する。

答え・解説 正答：エ

ア：責任ある受容判断になりません。

イ：基準変更にも正当な根拠と承認が必要です。

ウ：適切な意思決定を妨げます。

エ：リスク基準を無視して現場だけで開始するのではなく、残留リスクを透明化し、権限ある意思決定者が対応を選択します。

総合解説：リスク基準を無視して現場だけで開始するのではなく、残留リスクを透明化し、権限ある意思決定者が対応を選択します。 管理策を実施しても残るリスクが残留リスクです。受容可否を権限ある者が判断し、リスクの大きさ、期限、資源などを踏まえて優先順位を付け、実施項目・資源・責任者・完了予定時期・評価方法を対応計画に落とし込みます。

対象：2026年度 / 基準日 2026-09-05

0061 ISMS・ガバナンス > 方針・目的・適用範囲・管理策 ｜ 難易度：基礎

ISMSの適用範囲を定める目的として最も適切なものはどれか。

ア：どの組織、業務、情報、システム、拠点などをISMSの対象として管理するかを明確にする。

イ：ISMS対象を毎日無作為に変えるため。

ウ：対象外との依存関係を全て無視するため。

エ：管理策を一切実施しない範囲を作るため。

答え・解説 正答：ア

ア：適用範囲を明確にすることで、ISMSの対象と境界、関係する責任を一貫して管理できます。

イ：適用範囲は組織の状況に基づき明確に定めます。

ウ：境界外との依存・インタフェースも考慮が必要です。

エ：適用範囲は管理責任を明確にするものです。

総合解説：適用範囲を明確にすることで、ISMSの対象と境界、関係する責任を一貫して管理できます。ISMSでは、組織の状況と利害関係者を踏まえて適用範囲を定め、方針と目的を整合させ、リスクに応じた管理策を計画・運用・評価・改善します。管理策の導入自体ではなく、有効性を確認することが重要です。

対象：2026年度 / 基準日 2026-09-05

0062 ISMS・ガバナンス > 方針・目的・適用範囲・管理策 ｜ 難易度：基礎

情報セキュリティ方針の役割として最も適切なものはどれか。

ア：全てのFWルールのIPアドレスを記載することだけを目的とする。

イ：組織としての情報セキュリティに関する方向性と基本的なコミットメントを示す。

ウ：担当者ごとに異なる方針を秘密裏に持つ。

エ：リスク評価を禁止する。

答え・解説 正答：イ

ア：具体的な設定値は下位手順・設定管理で扱うのが一般的です。

イ：方針は、個別設定値の羅列ではなく、組織の方向性と管理の基本原則を示す上位方針です。

ウ：組織として一貫した方針が必要です。

エ：ISMSではリスクに基づく管理が重要です。

総合解説：方針は、個別設定値の羅列ではなく、組織の方向性と管理の基本原則を示す上位方針です。ISMSでは、組織の状況と利害関係者を踏まえて適用範囲を定め、方針と目的を整合させ、リスクに応じた管理策を計画・運用・評価・改善します。管理策の導入自体ではなく、有効性を確認することが重要です。

対象：2026年度 / 基準日 2026-09-05

0063 ISMS・ガバナンス > 方針・目的・適用範囲・管理策 ｜ 難易度：基礎

情報セキュリティ目的の設定として最も適切なものはどれか。

ア：方針と無関係な目標を設定する。

イ：「何となく安全にする」だけで評価方法を持たない。

ウ：方針と整合し、達成状況を評価できるよう具体的な指標や期限を必要に応じて定める。

エ：目的は一度決めたら事業変化があっても見直さない。

答え・解説 正答：ウ

ア：方針との整合が必要です。

イ：達成状況を評価しにくくなります。

ウ：目的は方針を実行可能な目標へ落とし込み、進捗や有効性を評価できる形にすることが重要です。

エ：状況変化に応じて見直す必要があります。

総合解説：目的は方針を実行可能な目標へ落とし込み、進捗や有効性を評価できる形にすることが重要です。 ISMSでは、組織の状況と利害関係者を踏まえて適用範囲を定め、方針と目的を整合させ、リスクに応じた管理策を計画・運用・評価・改善します。管理策の導入自体ではなく、有効性を確認することが重要です。

対象：2026年度 / 基準日 2026-09-05

0064 ISMS・ガバナンス > 方針・目的・適用範囲・管理策 ｜ 難易度：標準

ISMSの対象を本社業務だけとしたいが、本社の認証基盤は対象外のデータセンターに全面依存している。最も適切な考え方はどれか。

ア：範囲外なので認証基盤のリスクは存在しないとする。

イ：データセンターの存在を文書から削除する。

ウ：範囲を狭くすれば全てのリスクが自動的に消える。

エ：適用範囲の境界とデータセンターとの依存関係・責任分担を明確にし、必要な管理を確保する。

答え・解説 正答：エ

ア：依存している以上、対象業務へ影響します。

イ：実態は変わりません。

ウ：境界設定とリスク低減は同義ではありません。

エ：適用範囲外とのインタフェースや依存関係を無視すると、対象範囲のリスクを適切に管理できません。

総合解説：適用範囲外とのインタフェースや依存関係を無視すると、対象範囲のリスクを適切に管理できません。 ISMSでは、組織の状況と利害関係者を踏まえて適用範囲を定め、方針と目的を整合させ、リスクに応じた管理策を計画・運用・評価・改善します。管理策の導入自体ではなく、有効性を確認することが重要です。

対象：2026年度 / 基準日 2026-09-05

0065 ISMS・ガバナンス > 方針・目的・適用範囲・管理策 ｜ 難易度：標準

ISMSで情報セキュリティ管理策を選択する際の考え方として最も適切なものはどれか。

ア：リスクアセスメントとリスク対応の結果を踏まえ、必要な管理策を選択・設計する。

イ：他社が導入した管理策を理由なく全て同じにする。

ウ：リスク評価を行わず製品価格だけで決める。

エ：管理策の有効性は一切確認しない。

答え・解説 正答：ア

ア：管理策は規格名を機械的にコピーするのではなく、組織のリスクと要求事項に基づいて選択します。

イ：組織ごとのリスク・状況が異なります。

ウ：リスク低減との対応関係が必要です。

エ：運用後の評価が必要です。

総合解説：管理策は規格名を機械的にコピーするのではなく、組織のリスクと要求事項に基づいて選択します。 ISMSでは、組織の状況と利害関係者を踏まえて適用範囲を定め、方針と目的を整合させ、リスクに応じた管理策を計画・運用・評価・改善します。管理策の導入自体ではなく、有効性を確認することが重要です。

対象：2026年度 / 基準日 2026-09-05

0066 ISMS・ガバナンス > 方針・目的・適用範囲・管理策 ｜ 難易度：標準

「情報セキュリティ方針」「情報セキュリティ対策基準」「具体的な操作手順」の関係として最も適切なものはどれか。

ア：具体的手順が上位方針と矛盾しても問題ない。

イ：上位方針で基本的方向を示し、対策基準や手順へ具体化して、矛盾なく運用する。

ウ：方針だけあれば手順は常に不要である。

エ：手順は個人ごとに秘密にし、組織として共有しない。

答え・解説 正答：イ

ア：文書体系には整合性が必要です。

イ：上位方針と下位規程・手順を整合させることで、経営方針を現場の具体的な管理へ落とし込みます。

ウ：実際の運用には必要な手順・ルールが求められます。

エ：一貫した運用が困難です。

総合解説：上位方針と下位規程・手順を整合させることで、経営方針を現場の具体的な管理へ落とし込みます。 ISMSでは、組織の状況と利害関係者を踏まえて適用範囲を定め、方針と目的を整合させ、リスクに応じた管理策を計画・運用・評価・改善します。管理策の導入自体ではなく、有効性を確認することが重要です。

対象：2026年度 / 基準日 2026-09-05

0067 ISMS・ガバナンス > 方針・目的・適用範囲・管理策 ｜ 難易度：標準

「重大インシデントの初動連絡を30分以内に行う」という目的を設定したが、半年間ほぼ達成できていない。最も適切な対応はどれか。

ア：測定結果を削除して達成したことにする。

イ：目的を廃止し、以後測定しない。

ウ：未達原因とプロセスの有効性を分析し、資源・手順・教育・目的値の妥当性を見直して改善する。

エ：未達の原因を調べず担当者個人だけを罰する。

答え・解説 正答：ウ

ア：事実を隠しても改善されません。

イ：リスクと事業要件に基づき適切に見直すべきです。

ウ：目的は設定するだけでなく、測定・評価し、未達なら原因と対策を検討してISMSの改善につなげます。

エ：プロセスや資源等の原因分析が必要です。

総合解説：目的は設定するだけでなく、測定・評価し、未達なら原因と対策を検討してISMSの改善につなげます。 ISMSでは、組織の状況と利害関係者を踏まえて適用範囲を定め、方針と目的を整合させ、リスクに応じた管理策を計画・運用・評価・改善します。管理策の導入自体ではなく、有効性を確認することが重要です。

対象：2026年度 / 基準日 2026-09-05

0068 ISMS・ガバナンス > 方針・目的・適用範囲・管理策 ｜ 難易度：標準

管理策の「有効性」を確認する例として最も適切なものはどれか。

ア：製品を購入した領収書だけ確認する。

イ：設定内容を確認せず、名称だけで安全と判断する。

ウ：評価結果が悪ければ測定をやめる。

エ：導入した多要素認証により、不正ログインの発生や認証突破リスクが期待どおり低減しているかを指標で確認する。

答え・解説 正答：エ

ア：導入・運用の効果までは分かりません。

イ：実装・運用の実態を確認する必要があります。

ウ：改善につなげるべきです。

エ：管理策の導入有無だけでなく、意図したリスク低減効果が得られているかを評価することが重要です。

総合解説：管理策の導入有無だけでなく、意図したリスク低減効果が得られているかを評価することが重要です。 ISMSでは、組織の状況と利害関係者を踏まえて適用範囲を定め、方針と目的を整合させ、リスクに応じた管理策を計画・運用・評価・改善します。管理策の導入自体ではなく、有効性を確認することが重要です。

対象：2026年度 / 基準日 2026-09-05

0069 ISMS・ガバナンス > 方針・目的・適用範囲・管理策 ｜ 難易度：応用

ISMS適用範囲に新しい海外拠点を追加することになった。最も適切な対応はどれか。

ア：拠点の業務・情報資産・法的要求・脅威・既存管理策を確認し、リスクアセスメント、目的、管理策、文書を必要に応じて更新する。

イ：拠点名だけ追記し、現地リスクは確認しない。

ウ：旧拠点の管理策を条件確認なしでそのままコピーする。

エ：新拠点は範囲内でも資産台帳に登録しない。

答え・解説 正答：ア

ア：適用範囲変更は単なる文書修正ではなく、リスクと管理策、運用体制全体への影響を評価する必要があります。

イ：実態に応じたリスク評価が必要です。

ウ：環境・法令・脅威が異なる可能性があります。

エ：管理対象の把握が必要です。

総合解説：適用範囲変更は単なる文書修正ではなく、リスクと管理策、運用体制全体への影響を評価する必要があります。 ISMSでは、組織の状況と利害関係者を踏まえて適用範囲を定め、方針と目的を整合させ、リスクに応じた管理策を計画・運用・評価・改善します。管理策の導入自体ではなく、有効性を確認することが重要です。

対象：2026年度 / 基準日 2026-09-05

0070 ISMS・ガバナンス > 方針・目的・適用範囲・管理策 ｜ 難易度：応用

会社方針が「顧客情報の漏えい防止を最優先」としている一方、部門目標にも管理策にも顧客情報保護が反映されていない。最も適切な改善はどれか。

ア：方針だけ掲示して実務は変更しない。

イ：方針に対応するリスクと目的を明確にし、必要な管理策と評価指標へ落とし込んで整合性を持たせる。

ウ：顧客情報のリスクを台帳から削除する。

エ：目的と管理策は方針と無関係に決める。

答え・解説 正答：イ

ア：方針が運用へ反映されません。

イ：ISMSでは方針、リスク、目的、管理策、評価を連鎖させ、経営の意図が実務に反映されるようにします。

ウ：リスクを隠すだけです。

エ：整合性が必要です。

総合解説：ISMSでは方針、リスク、目的、管理策、評価を連鎖させ、経営の意図が実務に反映されるようにします。 ISMSでは、組織の状況と利害関係者を踏まえて適用範囲を定め、方針と目的を整合させ、リスクに応じた管理策を計画・運用・評価・改善します。管理策の導入自体ではなく、有効性を確認することが重要です。

対象：2026年度 / 基準日 2026-09-05

0071 ISMS・ガバナンス > JIS Q 27001・27002・27014 ｜ 難易度：基礎

ISMSを確立・実施・維持し、継続的に改善するための要求事項を定めるJIS Q 27001について、最も適切な説明はどれか。

ア：暗号アルゴリズムAESの仕様だけを定める規格。

イ：情報セキュリティガバナンスの概念だけを扱う規格。

ウ：情報セキュリティマネジメントシステム（ISMS）の要求事項を定める規格。

エ：管理策の実施手引だけを示し認証要求事項を持たない規格。

答え・解説 正答：ウ

ア：AESは別の暗号標準です。

イ：それはJIS Q 27014の主な役割です。

ウ：JIS Q 27001:2023は、ISMSの確立、実施、維持、継続的改善などに関する要求事項を規定します。

エ：それはJIS Q 27002の位置付けに近いです。

総合解説：JIS Q 27001:2023は、ISMSの確立、実施、維持、継続的改善などに関する要求事項を規定します。 JIS Q 27001はISMSの要求事項、JIS Q 27002は情報セキュリティ管理策の実施指針、JIS Q 27014は情報セキュリティガバナンスのガイダンスという役割を区別して理解します。

対象：2026年度 / 基準日 2026-09-05

0072 ISMS・ガバナンス > JIS Q 27001・27002・27014 ｜ 難易度：基礎

アクセス制御や人的・物理的・技術的対策などを扱うJIS Q 27002について、最も適切な説明はどれか。

ア：ISMS認証の要求事項そのものを定める唯一の規格。

イ：情報セキュリティガバナンスだけを対象とする規格。

ウ：会計監査の手続だけを定める規格。

エ：一般的な情報セキュリティ管理策群と、それらを実施するための手引を示す規格。

答え・解説 正答：エ

ア：要求事項の中心はJIS Q 27001です。

イ：それはJIS Q 27014です。

ウ：情報セキュリティ管理策の規格です。

エ：JIS Q 27002:2024は、情報セキュリティ管理策を選択・実施する際の実践的な指針として利用されます。

総合解説：JIS Q 27002:2024は、情報セキュリティ管理策を選択・実施する際の実践的な指針として利用されます。 JIS Q 27001はISMSの要求事項、JIS Q 27002は情報セキュリティ管理策の実施指針、JIS Q 27014は情報セキュリティガバナンスのガイダンスという役割を区別して理解します。

対象：2026年度 / 基準日 2026-09-05

0073 ISMS・ガバナンス > JIS Q 27001・27002・27014 ｜ 難易度：基礎

経営層による情報セキュリティの評価・指示・監視などに関係するJIS Q 27014について、最も適切な説明はどれか。

ア：組織における情報セキュリティガバナンスの概念や原則に基づくガイダンスを示す規格。

イ：無線LAN暗号化方式を規定する規格。

ウ：ISMSの認証要求事項だけを定める規格。

エ：情報セキュリティ管理策の詳細実施手引を主目的とする規格。

答え・解説 正答：ア

ア：JIS Q 27014:2015は、情報セキュリティガバナンスについての概念及び原則に基づくガイダンスを示します。

イ：無線LAN技術規格ではありません。

ウ：それはJIS Q 27001です。

エ：それはJIS Q 27002の役割です。

総合解説：JIS Q 27014:2015は、情報セキュリティガバナンスについての概念及び原則に基づくガイダンスを示します。 JIS Q 27001はISMSの要求事項、JIS Q 27002は情報セキュリティ管理策の実施指針、JIS Q 27014は情報セキュリティガバナンスのガイダンスという役割を区別して理解します。

対象：2026年度 / 基準日 2026-09-05

0074 ISMS・ガバナンス > JIS Q 27001・27002・27014 ｜ 難易度：標準

JIS Q 27001とJIS Q 27002の関係として最も適切なものはどれか。

ア：両者は全く同じ内容で名称だけが異なる。

イ：27001はISMSの要求事項を示し、27002は情報セキュリティ管理策の実施に関するガイダンスを提供する。

ウ：27002が認証要求事項で、27001は参考資料にすぎない。

エ：27001は物理管理だけ、27002は暗号だけを扱う。

答え・解説 正答：イ

ア：役割が異なります。

イ：要求事項と管理策ガイダンスという役割の違いを理解することが重要です。

ウ：逆です。27001が要求事項です。

エ：どちらもより広い範囲を扱います。

総合解説：要求事項と管理策ガイダンスという役割の違いを理解することが重要です。 JIS Q 27001はISMSの要求事項、JIS Q 27002は情報セキュリティ管理策の実施指針、JIS Q 27014は情報セキュリティガバナンスのガイダンスという役割を区別して理解します。

対象：2026年度 / 基準日 2026-09-05

0075 ISMS・ガバナンス > JIS Q 27001・27002・27014 ｜ 難易度：標準

ISMS認証との関係で最も適切な説明はどれか。

ア：JIS Q 27002だけを購入すれば自動的に認証される。

イ：JIS Q 27014だけがISMS認証の要求事項である。

ウ：組織のISMSがJIS Q 27001の要求事項に適合しているかが認証審査の基準となる。

エ：認証はリスクアセスメントを行わなくても取得できることを意味する。

答え・解説 正答：ウ

ア：認証にはISMSの適合性審査が必要です。

イ：27014はガバナンスのガイダンスです。

ウ：JIS Q 27001はISMSの要求事項規格であり、認証の基準として用いられます。JIS Q 27002は管理策の実施ガイダンスです。

エ：27001ではリスクに基づく管理が重要です。

総合解説：JIS Q 27001はISMSの要求事項規格であり、認証の基準として用いられます。JIS Q 27002は管理策の実施ガイダンスです。 JIS Q 27001はISMSの要求事項、JIS Q 27002は情報セキュリティ管理策の実施指針、JIS Q 27014は情報セキュリティガバナンスのガイダンスという役割を区別して理解します。

対象：2026年度 / 基準日 2026-09-05

0076 ISMS・ガバナンス > JIS Q 27001・27002・27014 ｜ 難易度：標準

情報セキュリティガバナンスの視点として最も適切なものはどれか。

ア：OSのパッチ適用作業だけをガバナンスと呼ぶ。

イ：経営層は情報セキュリティに関与しない。

ウ：インシデントが起きたときだけ方針を考える。

エ：経営層が情報セキュリティを組織目的と整合させ、評価・指示・監視を通じて統治する。

答え・解説 正答：エ

ア：個別技術運用はガバナンスの一部を支えますが同義ではありません。

イ：ガバナンスでは経営の関与が重要です。

ウ：継続的な統治が必要です。

エ：情報セキュリティガバナンスは、技術部門だけの運用ではなく、経営レベルで方向性と監督を行う枠組みです。

総合解説：情報セキュリティガバナンスは、技術部門だけの運用ではなく、経営レベルで方向性と監督を行う枠組みです。 JIS Q 27001はISMSの要求事項、JIS Q 27002は情報セキュリティ管理策の実施指針、JIS Q 27014は情報セキュリティガバナンスのガイダンスという役割を区別して理解します。

対象：2026年度 / 基準日 2026-09-05

0077 ISMS・ガバナンス > JIS Q 27001・27002・27014 ｜ 難易度：標準

組織がISMSを構築中で、具体的なアクセス制御、人的対策、物理対策などの管理策を設計する参考を探している。最も適切な規格はどれか。

ア：JIS Q 27002。

イ：JIS Q 27014だけ。

ウ：JIS Q 27001だけを管理策の詳細手引として使う。

エ：ISO 14001。

答え・解説 正答：ア

ア：JIS Q 27002は一般的な情報セキュリティ管理策群と実施の手引を示すため、具体的な管理策設計の参考に適しています。

イ：ガバナンスのガイダンスが主目的です。

ウ：27001は要求事項の規格で、詳細ガイダンスは27002が適しています。

エ：環境マネジメントシステムの規格であり、本目的とは異なります。

総合解説：JIS Q 27002は一般的な情報セキュリティ管理策群と実施の手引を示すため、具体的な管理策設計の参考に適しています。 JIS Q 27001はISMSの要求事項、JIS Q 27002は情報セキュリティ管理策の実施指針、JIS Q 27014は情報セキュリティガバナンスのガイダンスという役割を区別して理解します。

対象：2026年度 / 基準日 2026-09-05

0078 ISMS・ガバナンス > JIS Q 27001・27002・27014 ｜ 難易度：標準

2026年9月5日時点のJIS Q 27001とJIS Q 27002について、最も適切な説明はどれか。

ア：JIS Q 27001は2014年版だけが有効であり、2023年版はまだ発行されていない。

イ：JIS Q 27001:2023とJIS Q 27002:2024はいずれも有効で、前者はISO/IEC 27001:2022、後者はISO/IEC 27002:2022に対応する。

ウ：JIS Q 27002はISMS認証の要求事項規格であり、JIS Q 27001は管理策の実施ガイダンスを定める。

エ：JIS Q 27001とJIS Q 27002は、国内規格として必ず同じ年に発行されなければ相互に参照できない。

答え・解説 正答：イ

ア：JIS Q 27001:2023が有効であり、2014年版だけが現行という説明は誤りです。

イ：日本規格協会の現行情報では、JIS Q 27001:2023とJIS Q 27002:2024が有効です。規格番号の年と対応国際規格の年が同じとは限りません。

ウ：役割が逆です。JIS Q 27001はISMSの要求事項、JIS Q 27002は管理策の実施ガイダンスです。

エ：JIS化の時期により発行年は異なり得るため、同一年であることは相互参照の条件ではありません。

総合解説：日本規格協会の現行情報では、JIS Q 27001:2023とJIS Q 27002:2024が有効です。規格番号の年と対応国際規格の年が同じとは限りません。 JIS Q 27001はISMSの要求事項、JIS Q 27002は情報セキュリティ管理策の実施指針、JIS Q 27014は情報セキュリティガバナンスのガイダンスという役割を区別して理解します。

対象：2026年度 / 基準日 2026-09-05

0079 ISMS・ガバナンス > JIS Q 27001・27002・27014 ｜ 難易度：応用

2026年9月5日時点の情報セキュリティガバナンス規格について、最も適切な説明はどれか。

ア：JIS Q 27014:2015は2025年に自動的にJIS Q 27014:2025へ改番された。

イ：ISO/IEC 27014:2020とJIS Q 27014:2015は発行年も内容版も必ず同一である。

ウ：JIS Q 27014:2015は2025年に確認され有効で、対応国際規格はISO/IEC 27014:2013である一方、ISOではISO/IEC 27014:2020が発行されている。

エ：JIS Q 27014は既に廃止されている。

答え・解説 正答：ウ

ア：確認では規格番号の西暦年は変更されません。

イ：対応版が異なります。

ウ：JIS Q 27014:2015は現行JISとして有効ですが、国際規格側には後続版ISO/IEC 27014:2020があります。JISとISOの版を混同しないことが重要です。

エ：2026-09-05時点で有効です。

総合解説：JIS Q 27014:2015は現行JISとして有効ですが、国際規格側には後続版ISO/IEC 27014:2020があります。JISとISOの版を混同しないことが重要です。 JIS Q 27001はISMSの要求事項、JIS Q 27002は情報セキュリティ管理策の実施指針、JIS Q 27014は情報セキュリティガバナンスのガイダンスという役割を区別して理解します。

対象：2026年度 / 基準日 2026-09-05

0080 ISMS・ガバナンス > JIS Q 27001・27002・27014 ｜ 難易度：応用

経営層はガバナンス指針、ISMS担当は要求事項、現場は管理策の実施ガイダンスを参照したい。最も適切な対応関係はどれか。

ア：経営層には管理策ガイダンスのJIS Q 27002、ISMS要求事項にはガバナンス規格JIS Q 27014、現場管理策にはJIS Q 27001を割り当てる。

イ：三つの目的を全て情報セキュリティガバナンスのJIS Q 27014だけで代替し、ISMS要求事項や管理策ガイダンスを別途参照しない。

ウ：三つの目的を全て管理策ガイダンスのJIS Q 27002だけで代替し、ISMS要求事項規格やガバナンス指針を別途参照しない。

エ：経営層：JIS Q 27014、ISMS要求事項：JIS Q 27001、管理策ガイダンス：JIS Q 27002。

答え・解説 正答：エ

ア：各規格の役割が入れ替わっています。JIS Q 27014はガバナンス、JIS Q 27001はISMS要求事項、JIS Q 27002は管理策ガイダンスです。

イ：JIS Q 27014はガバナンスのガイダンスであり、ISMS要求事項や管理策ガイダンスの役割を単独で代替しません。

ウ：JIS Q 27002は管理策の実施ガイダンスであり、ISMS要求事項とガバナンスの役割を単独では満たしません。

エ：三つの規格は競合ではなく、ガバナンス、マネジメントシステム要求事項、管理策実施ガイダンスという異なる層を補完します。

総合解説：三つの規格は競合ではなく、ガバナンス、マネジメントシステム要求事項、管理策実施ガイダンスという異なる層を補完します。 JIS Q 27001はISMSの要求事項、JIS Q 27002は情報セキュリティ管理策の実施指針、JIS Q 27014は情報セキュリティガバナンスのガイダンスという役割を区別して理解します。

対象：2026年度 / 基準日 2026-09-05

0081 ISMS・ガバナンス > 内部監査・マネジメントレビュー・継続的改善 ｜ 難易度：基礎

ISMSの内部監査の主な目的として最も適切なものはどれか。

ア：ISMSが定めた要求事項に適合し、有効に実施・維持されているかを客観的に確認する。

イ：監査対象部門の全責任を監査員へ移す。

ウ：監査で発見した問題を隠す。

エ：認証機関の外部審査だけを内部監査と呼ぶ。

答え・解説 正答：ア

ア：内部監査は、ISMSの適合性と運用状況を確認し、改善につなげるためのパフォーマンス評価活動です。

イ：運用責任は対象部門に残ります。

ウ：客観的に報告する必要があります。

エ：内部監査と外部審査は別です。

総合解説：内部監査は、ISMSの適合性と運用状況を確認し、改善につなげるためのパフォーマンス評価活動です。 内部監査はISMSが定めた要求事項に適合し有効に実施・維持されているかを客観的に確認し、マネジメントレビューはトップマネジメントがISMSの適切性・妥当性・有効性を評価します。不適合には原因を踏まえた是正処置と効果確認を行い、継続的改善につなげます。

対象：2026年度 / 基準日 2026-09-05

0082 ISMS・ガバナンス > 内部監査・マネジメントレビュー・継続的改善 ｜ 難易度：基礎

ISMSのマネジメントレビューの説明として最も適切なものはどれか。

ア：一般利用者が毎日パスワードを変更すること。

イ：トップマネジメントがISMSの適切性、妥当性、有効性などを評価し、必要な変更や改善を判断する。

ウ：監査員がシステム設定を直接修正すること。

エ：製品購入だけを決める会議。

答え・解説 正答：イ

ア：マネジメントレビューではありません。

イ：マネジメントレビューは、経営層がISMSの状態を評価し、方向性・資源・改善の意思決定を行う機会です。

ウ：レビューは経営上の評価・意思決定です。

エ：ISMS全体の適切性・有効性を扱います。

総合解説：マネジメントレビューは、経営層がISMSの状態を評価し、方向性・資源・改善の意思決定を行う機会です。 内部監査はISMSが定めた要求事項に適合し有効に実施・維持されているかを客観的に確認し、マネジメントレビューはトップマネジメントがISMSの適切性・妥当性・有効性を評価します。不適合には原因を踏まえた是正処置と効果確認を行い、継続的改善につなげます。

対象：2026年度 / 基準日 2026-09-05

0083 ISMS・ガバナンス > 内部監査・マネジメントレビュー・継続的改善 ｜ 難易度：基礎

ISMSにおける継続的改善として最も適切なものはどれか。

ア：規程を一度作成したら永久に変更しない。

イ：問題を発見しても記録しない。

ウ：監査、測定、インシデント、レビューなどから得た情報を基に、ISMSの適切性・妥当性・有効性を継続して向上させる。

エ：インシデントのたびに原因確認なしで同じ対策を繰り返す。

答え・解説 正答：ウ

ア：環境やリスクの変化に対応できません。

イ：改善機会を失います。

ウ：継続的改善は一度の大規模改修だけを意味せず、評価結果を使って管理の有効性を継続的に高める活動です。

エ：原因に基づく改善が必要です。

総合解説：継続的改善は一度の大規模改修だけを意味せず、評価結果を使って管理の有効性を継続的に高める活動です。 内部監査はISMSが定めた要求事項に適合し有効に実施・維持されているかを客観的に確認し、マネジメントレビューはトップマネジメントがISMSの適切性・妥当性・有効性を評価します。不適合には原因を踏まえた是正処置と効果確認を行い、継続的改善につなげます。

対象：2026年度 / 基準日 2026-09-05

0084 ISMS・ガバナンス > 内部監査・マネジメントレビュー・継続的改善 ｜ 難易度：標準

内部監査の客観性を高める方法として最も適切なものはどれか。

ア：監査対象部門の責任者が自分の業務を無条件で合格とする。

イ：証拠を確認せず印象だけで判断する。

ウ：不適合を出さないことを監査目標にする。

エ：可能な範囲で、監査員が自分自身の担当業務を直接監査することを避け、監査基準と証拠に基づいて評価する。

答え・解説 正答：エ

ア：自己監査では客観性が損なわれます。

イ：客観的証拠に基づく必要があります。

ウ：監査目的は問題の隠蔽ではありません。

エ：監査の信頼性には、監査員の客観性と公正な証拠評価が重要です。

総合解説：監査の信頼性には、監査員の客観性と公正な証拠評価が重要です。 内部監査はISMSが定めた要求事項に適合し有効に実施・維持されているかを客観的に確認し、マネジメントレビューはトップマネジメントがISMSの適切性・妥当性・有効性を評価します。不適合には原因を踏まえた是正処置と効果確認を行い、継続的改善につなげます。

対象：2026年度 / 基準日 2026-09-05

0085 ISMS・ガバナンス > 内部監査・マネジメントレビュー・継続的改善 ｜ 難易度：標準

内部監査で「退職者アカウントの削除遅延」が繰り返し見つかった。最も適切な是正処置はどれか。

ア：個別アカウントを削除するだけでなく、原因を分析し、人事連携や期限・責任・確認手順を改善して再発防止を図る。

イ：今回のアカウントだけ削除し、原因は調べない。

ウ：監査報告書から指摘を削除する。

エ：退職者アカウントを全て永久保持するルールに変える。

答え・解説 正答：ア

ア：不適合への是正処置では、表面的な修正だけでなく原因を取り除き、再発しない仕組みに改善します。

イ：同じ不適合が再発する可能性があります。

ウ：問題自体は残ります。

エ：セキュリティリスクを増やします。

総合解説：不適合への是正処置では、表面的な修正だけでなく原因を取り除き、再発しない仕組みに改善します。 内部監査はISMSが定めた要求事項に適合し有効に実施・維持されているかを客観的に確認し、マネジメントレビューはトップマネジメントがISMSの適切性・妥当性・有効性を評価します。不適合には原因を踏まえた是正処置と効果確認を行い、継続的改善につなげます。

対象：2026年度 / 基準日 2026-09-05

0086 ISMS・ガバナンス > 内部監査・マネジメントレビュー・継続的改善 ｜ 難易度：標準

マネジメントレビューで確認すべき情報として最も適切なものはどれか。

ア：社内食堂のメニューだけ。

イ：監査結果、目的の達成状況、リスクや環境の変化、是正処置の状況など、ISMSの有効性判断に必要な情報。

ウ：監査結果を意図的に除外する。

エ：成功事例だけを集め、問題情報は報告しない。

答え・解説 正答：イ

ア：ISMS有効性判断との関連がありません。

イ：経営層は一つの指標だけでなく、監査・測定・リスク・改善状況を総合してISMSをレビューします。

ウ：重要な評価情報を欠きます。

エ：偏った情報では適切な判断ができません。

総合解説：経営層は一つの指標だけでなく、監査・測定・リスク・改善状況を総合してISMSをレビューします。 内部監査はISMSが定めた要求事項に適合し有効に実施・維持されているかを客観的に確認し、マネジメントレビューはトップマネジメントがISMSの適切性・妥当性・有効性を評価します。不適合には原因を踏まえた是正処置と効果確認を行い、継続的改善につなげます。

対象：2026年度 / 基準日 2026-09-05

0087 ISMS・ガバナンス > 内部監査・マネジメントレビュー・継続的改善 ｜ 難易度：標準

内部監査の頻度・範囲を決める考え方として最も適切なものはどれか。

ア：過去に重大不適合があった領域ほど監査しない。

イ：監査範囲は担当者の気分だけで決める。

ウ：重要なプロセス、過去の不適合、変更、リスクなどを考慮して監査プログラムを計画する。

エ：システム変更が多い領域も一切見直さない。

答え・解説 正答：ウ

ア：重点確認が必要になり得ます。

イ：客観的な基準が必要です。

ウ：すべてを機械的に同じ頻度で監査するより、重要性や過去結果、変更を踏まえた監査計画が有効です。

エ：変更に伴うリスクを考慮すべきです。

総合解説：すべてを機械的に同じ頻度で監査するより、重要性や過去結果、変更を踏まえた監査計画が有効です。 内部監査はISMSが定めた要求事項に適合し有効に実施・維持されているかを客観的に確認し、マネジメントレビューはトップマネジメントがISMSの適切性・妥当性・有効性を評価します。不適合には原因を踏まえた是正処置と効果確認を行い、継続的改善につなげます。

対象：2026年度 / 基準日 2026-09-05

0088 ISMS・ガバナンス > 内部監査・マネジメントレビュー・継続的改善 ｜ 難易度：標準

是正処置を実施した後に行うべき確認として最も適切なものはどれか。

ア：処置記録を作った時点で効果確認を省略する。

イ：再発していても完了扱いのままにする。

ウ：担当者の口頭報告だけで証拠を確認しない。

エ：処置が実施されたかだけでなく、原因が除去され、同様の不適合が再発しにくくなったかを確認する。

答え・解説 正答：エ

ア：実際の効果が分かりません。

イ：追加改善が必要です。

ウ：客観的な確認が望まれます。

エ：是正処置は「作業実施」で終わらず、有効性確認まで行って改善を閉じます。

総合解説：是正処置は「作業実施」で終わらず、有効性確認まで行って改善を閉じます。 内部監査はISMSが定めた要求事項に適合し有効に実施・維持されているかを客観的に確認し、マネジメントレビューはトップマネジメントがISMSの適切性・妥当性・有効性を評価します。不適合には原因を踏まえた是正処置と効果確認を行い、継続的改善につなげます。

対象：2026年度 / 基準日 2026-09-05

0089 ISMS・ガバナンス > 内部監査・マネジメントレビュー・継続的改善 ｜ 難易度：応用

ISMSの改善サイクルとして最も適切な流れはどれか。

ア：内部監査や測定で課題を把握し、マネジメントレビューで意思決定し、是正・改善を実施して効果を再評価する。

イ：監査で課題を見つけたら報告せず終了する。

ウ：レビューで決定しても実施状況を追跡しない。

エ：改善後は二度と測定しない。

答え・解説 正答：ア

ア：監査、レビュー、改善は独立したイベントではなく、評価結果を意思決定と改善へ循環させる仕組みとして機能します。

イ：改善につながりません。

ウ：意思決定が実行されません。

エ：効果確認と継続的改善ができません。

総合解説：監査、レビュー、改善は独立したイベントではなく、評価結果を意思決定と改善へ循環させる仕組みとして機能します。 内部監査はISMSが定めた要求事項に適合し有効に実施・維持されているかを客観的に確認し、マネジメントレビューはトップマネジメントがISMSの適切性・妥当性・有効性を評価します。不適合には原因を踏まえた是正処置と効果確認を行い、継続的改善につなげます。

対象：2026年度 / 基準日 2026-09-05

0090 ISMS・ガバナンス > 内部監査・マネジメントレビュー・継続的改善 ｜ 難易度：応用

内部監査で複数部門の教育不足が指摘され、インシデント件数も増加している。一方、教育予算は削減予定である。マネジメントレビューで最も適切な対応はどれか。

ア：予算計画を優先し、リスク情報を議題から外す。

イ：監査所見とインシデント傾向、リスクを根拠に教育の有効性と必要資源を再評価し、改善方針と資源配分を決定する。

ウ：指摘を隠して教育を全面廃止する。

エ：インシデント件数が増えても原因分析をしない。

答え・解説 正答：イ

ア：ISMSの有効性判断に必要な情報を無視しています。

イ：マネジメントレビューは、監査・実績・リスクを経営判断へつなげ、必要な資源や改善方針を決める場です。

ウ：リスクを増やす可能性があります。

エ：改善の根拠が得られません。

総合解説：マネジメントレビューは、監査・実績・リスクを経営判断へつなげ、必要な資源や改善方針を決める場です。 内部監査はISMSが定めた要求事項に適合し有効に実施・維持されているかを客観的に確認し、マネジメントレビューはトップマネジメントがISMSの適切性・妥当性・有効性を評価します。不適合には原因を踏まえた是正処置と効果確認を行い、継続的改善につなげます。

対象：2026年度 / 基準日 2026-09-05

0091 組織・人的管理 > CISO・CSIRT・SOC等の役割と体制 ｜ 難易度：基礎

CISOの役割として最も適切なものはどれか。

ア：経営上のリスクとして情報セキュリティを捉え、組織全体の方針や体制を統括する。

イ：日々の全端末ログを自ら常時監視する。

ウ：全てのインシデントの技術解析を単独で実施する。

エ：監査対象部門の業務を代行して監査証拠を作成する。

答え・解説 正答：ア

ア：CISOは最高情報セキュリティ責任者として、経営層と連携しながらセキュリティ方針・体制・リスク対応を統括する役割を担います。

イ：常時監視はSOCなどの運用機能が担うことがあり、CISOの中心的役割は経営・統括です。

ウ：技術解析はCSIRTやSOC、専門部門等と分担します。

エ：監査の独立性・客観性を損なう行為であり、CISOの役割でもありません。

総合解説：CISOは最高情報セキュリティ責任者として、経営層と連携しながらセキュリティ方針・体制・リスク対応を統括する役割を担います。 経営責任者の役割と、監視・分析を担う実務機能を混同しないことがポイントです。

対象：2026年度 / 基準日 2026-09-05

0092 組織・人的管理 > CISO・CSIRT・SOC等の役割と体制 ｜ 難易度：基礎

CSIRTの説明として最も適切なものはどれか。

ア：経営計画の策定だけを専門に行う組織である。

イ：情報セキュリティインシデントへの対応を組織的に調整し、関係部門と連携して処理する体制である。

ウ：施設の入退室警備だけを担当する組織である。

エ：会計監査だけを担当する独立監査部門である。

答え・解説 正答：イ

ア：経営計画だけを扱う組織ではありません。

イ：CSIRTはインシデント対応の連絡受付、調整、分析、対応支援などを担う組織・機能です。

ウ：物理警備に限定された組織ではありません。

エ：CSIRTの中心はインシデント対応であり、会計監査部門ではありません。

総合解説：CSIRTはインシデント対応の連絡受付、調整、分析、対応支援などを担う組織・機能です。 CSIRTは単なる技術チーム名ではなく、インシデント対応を組織横断で調整する機能として捉えます。

対象：2026年度 / 基準日 2026-09-05

0093 組織・人的管理 > CISO・CSIRT・SOC等の役割と体制 ｜ 難易度：基礎

SOCの機能として最も適切なものはどれか。

ア：情報セキュリティ方針を最終承認する。

イ：人事評価と給与計算を担当する。

ウ：ログやセキュリティ機器の情報を継続的に監視・分析し、脅威や異常の検知につなげる。

エ：契約書の法的有効性だけを審査する。

答え・解説 正答：ウ

ア：最終承認は経営層等のガバナンス上の役割であり、SOCの中心機能ではありません。

イ：SOCの役割とは無関係です。

ウ：SOCはセキュリティ監視・分析を中心に、異常の検知や初期分析、必要に応じたエスカレーションを行います。

エ：法務部門の役割に近く、SOCの中心機能ではありません。

総合解説：SOCはセキュリティ監視・分析を中心に、異常の検知や初期分析、必要に応じたエスカレーションを行います。 SOCは主に平常時からの監視・検知・分析を担い、必要に応じて対応組織へつなぎます。

対象：2026年度 / 基準日 2026-09-05

0094 組織・人的管理 > CISO・CSIRT・SOC等の役割と体制 ｜ 難易度：標準

複数部門がセキュリティ対策に関与する企業で、責任の押し付け合いが発生している。最も適切な改善策はどれか。

ア：問題が起きるたびに担当者をその場で決める。

イ：全ての判断をSOC担当者一人に集中させる。

ウ：担当部署を非公開にして攻撃者に知られないようにする。

エ：各関係者の役割・責任・権限・報告経路を明文化し、既存のガバナンスや内部統制との整合を取る。

答え・解説 正答：エ

ア：場当たり的な割当ては責任の空白や重複を防げません。

イ：権限集中は単一障害点や過大な負担を生み、経営判断との連携も欠けます。

ウ：組織内部で役割や報告経路を明確にすることが重要です。

エ：IPAは、サイバーセキュリティリスク管理体制では関係者の役割と責任を明確化し、組織のガバナンス等との整合を取ることを求めています。

総合解説：IPAは、サイバーセキュリティリスク管理体制では関係者の役割と責任を明確化し、組織のガバナンス等との整合を取ることを求めています。 体制設計では、誰が決めるか、誰が実行するか、誰へ報告するかを曖昧にしないことが重要です。

対象：2026年度 / 基準日 2026-09-05

0095 組織・人的管理 > CISO・CSIRT・SOC等の役割と体制 ｜ 難易度：標準

SOCが重要サーバへの不審な通信を検知した。次の対応として最も適切なものはどれか。

ア：定められた基準で事象を評価し、インシデントの可能性が高ければCSIRTなど対応体制へ速やかにエスカレーションする。

イ：監視担当者が証拠を消去してアラートを閉じる。

ウ：翌月の定例会まで報告を保留する。

エ：利用者全員に未確認情報を一斉公開する。

答え・解説 正答：ア

ア：監視・検知を担うSOCと、インシデント対応を調整するCSIRTは、定めた基準と連絡経路で連携することが重要です。

イ：証拠や記録の消去は分析・対応を妨げます。

ウ：重大な可能性がある事象は迅速なエスカレーションが必要です。

エ：事実確認や情報公開手順を経ずに広報するのは不適切です。

総合解説：監視・検知を担うSOCと、インシデント対応を調整するCSIRTは、定めた基準と連絡経路で連携することが重要です。 検知から対応への引継ぎ条件を事前に定めることで、見逃しと対応遅延を抑えられます。

対象：2026年度 / 基準日 2026-09-05

0096 組織・人的管理 > CISO・CSIRT・SOC等の役割と体制 ｜ 難易度：標準

セキュリティ部門が重大リスクを把握したとき、経営判断につなげるための対応として最も適切なものはどれか。

ア：技術部門内だけで共有し、経営層には知らせない。

イ：事業影響や残留リスクを整理し、定められた経路でCISOや経営層へ報告する。

ウ：発生確率がゼロでない限り全サービスを停止する。

エ：報告書には脆弱性名だけを書き、影響を示さない。

答え・解説 正答：イ

ア：重大リスクを経営判断から切り離すのは不適切です。

イ：セキュリティは経営リスクでもあるため、技術情報だけでなく事業影響とリスクを整理して意思決定者へ報告することが重要です。

ウ：リスクの大きさや事業影響を評価せず一律停止するのは合理的ではありません。

エ：経営判断には事業影響・優先度・必要な対応などの情報が必要です。

総合解説：セキュリティは経営リスクでもあるため、技術情報だけでなく事業影響とリスクを整理して意思決定者へ報告することが重要です。 経営報告では技術的重大度だけでなく、事業停止・顧客影響・法的影響なども整理します。

対象：2026年度 / 基準日 2026-09-05

0097 組織・人的管理 > CISO・CSIRT・SOC等の役割と体制 ｜ 難易度：標準

IT部門だけでセキュリティを運営しているが、個人情報・契約・人事に関する判断が滞っている。最も適切な体制改善はどれか。

ア：IT部門が法務判断や人事処分まで単独で決定する。

イ：関係部門にはインシデント後だけ知らせる。

ウ：法務、人事、事業部門など必要な関係部門を含む横断体制を設け、CISO等の責任者の下で連携する。

エ：体制図を作らず口頭合意だけで運用する。

答え・解説 正答：ウ

ア：専門性・権限の範囲を超えるため不適切です。

イ：平常時から役割を定め、予防・対応の両面で連携する必要があります。

ウ：セキュリティリスクはITだけで完結しません。法務・人事・業務部門などの役割を明確にし、横断的に連携する体制が有効です。

エ：担当変更や緊急時に混乱しやすく、役割・責任は明確化すべきです。

総合解説：セキュリティリスクはITだけで完結しません。法務・人事・業務部門などの役割を明確にし、横断的に連携する体制が有効です。 セキュリティはIT、法務、人事、事業継続などにまたがるため、組織横断の連携が必要です。

対象：2026年度 / 基準日 2026-09-05

0098 組織・人的管理 > CISO・CSIRT・SOC等の役割と体制 ｜ 難易度：標準

24時間監視を外部SOCへ委託する場合の考え方として最も適切なものはどれか。

ア：委託した時点で自組織のセキュリティ責任は全て消滅する。

イ：外部SOCからの連絡は月1回だけに限定する。

ウ：自組織側には連絡窓口を置かない。

エ：監視業務を委託しても、自組織のリスク管理責任がなくなるわけではなく、役割・連絡・判断基準を明確にする。

答え・解説 正答：エ

ア：委託は責任そのものの全面移転を意味しません。

イ：重大インシデントでは即時連絡など、リスクに応じた条件が必要です。

ウ：委託先と連携する窓口や意思決定者が必要です。

エ：外部サービスを利用しても、委託元には自組織のリスクを管理する責任が残ります。監視範囲、通知条件、エスカレーション先などの明確化が必要です。

総合解説：外部サービスを利用しても、委託元には自組織のリスクを管理する責任が残ります。監視範囲、通知条件、エスカレーション先などの明確化が必要です。 外部SOCは監視能力を補完しますが、リスク受容や事業上の意思決定は委託元側に残ります。

対象：2026年度 / 基準日 2026-09-05

0099 組織・人的管理 > CISO・CSIRT・SOC等の役割と体制 ｜ 難易度：応用

セキュリティ管理者が「アクセス権の申請、承認、設定、監査」を一人で全て実施している。最も適切な改善はどれか。

ア：重要な承認・設定・監査を適切に分離し、相互牽制が働くよう役割を設計する。

イ：担当者の権限をさらに増やして処理を速くする。

ウ：監査ログを本人だけが削除できるようにする。

エ：申請手続を廃止して口頭依頼だけにする。

答え・解説 正答：ア

ア：重要操作を一人に集中すると誤りや不正を発見しにくくなります。職務分掌と独立した確認によって統制を強化します。

イ：権限集中を強めるため統制上のリスクが増します。

ウ：証跡の改変・消去リスクを高めます。

エ：承認記録が残らず、統制が弱くなります。

総合解説：重要操作を一人に集中すると誤りや不正を発見しにくくなります。職務分掌と独立した確認によって統制を強化します。 職務分掌は不正防止だけでなく、誤操作の早期発見や監査可能性の確保にも役立ちます。

対象：2026年度 / 基準日 2026-09-05

0100 組織・人的管理 > CISO・CSIRT・SOC等の役割と体制 ｜ 難易度：応用

インシデント対応体制の実効性を高める施策として最も適切なものはどれか。

ア：インシデント発生後に初めて責任者を選ぶ。

イ：平常時に連絡網、役割、判断基準を整備し、演習や訓練で機能するか確認する。

ウ：連絡網は機密なので担当者にも共有しない。

エ：訓練は実際の事故ではないため実施しない。

答え・解説 正答：イ

ア：初動が遅れ、判断の混乱を招きます。

イ：緊急時に初めて役割を決めるのではなく、平常時から体制・連絡・エスカレーションを整え、訓練で改善することが重要です。

ウ：必要な関係者が利用できなければ緊急時に機能しません。

エ：訓練は手順・役割の不備を発見するために有効です。

総合解説：緊急時に初めて役割を決めるのではなく、平常時から体制・連絡・エスカレーションを整え、訓練で改善することが重要です。 体制は文書化するだけでなく、訓練によって連絡網や意思決定が実際に機能するか検証します。

対象：2026年度 / 基準日 2026-09-05

0101 組織・人的管理 > 教育・訓練・情報セキュリティ意識向上 ｜ 難易度：基礎

情報セキュリティ教育・訓練の主な目的として最も適切なものはどれか。

ア：受講記録だけを作り、行動変容は確認しない。

イ：全従業員に同じ専門技術だけを暗記させる。

ウ：方針・手順・脅威と影響を理解させ、安全な行動を実践できる状態にする。

エ：事故が起きた人だけに教育し、他の従業員には実施しない。

答え・解説 正答：ウ

ア：形式的な受講だけでなく、理解・行動につなげることが目的です。

イ：職務やリスクに応じた内容が必要です。

ウ：IPAシラバスでは、ポリシー、職務上の方針・手順、セキュリティ課題と影響を理解するための教育・訓練が求められています。

エ：予防と意識向上のため組織的な教育が必要です。

総合解説：IPAシラバスでは、ポリシー、職務上の方針・手順、セキュリティ課題と影響を理解するための教育・訓練が求められています。 教育の成果は、知識を知っていることではなく、必要な場面で安全な行動を選べることに現れます。

対象：2026年度 / 基準日 2026-09-05

0102 組織・人的管理 > 教育・訓練・情報セキュリティ意識向上 ｜ 難易度：基礎

情報セキュリティ教育計画として最も適切なものはどれか。

ア：全員に同じ内容を一度だけ実施すれば十分とする。

イ：新入社員は業務経験がないので教育対象から外す。

ウ：教育内容は担当者の好みだけで決める。

エ：対象者の職務やリスクに応じて内容・時期・方法を定め、必要に応じて役割別教育を行う。

答え・解説 正答：エ

ア：脅威や職務は変化するため、継続的かつ対象別の教育が必要です。

イ：入社時はルールを理解させる重要なタイミングです。

ウ：方針・リスク・職務上の必要性に基づくべきです。

エ：全員共通の基礎教育に加え、管理者や特権利用者など職務固有のリスクに応じた教育を組み合わせるのが適切です。

総合解説：全員共通の基礎教育に加え、管理者や特権利用者など職務固有のリスクに応じた教育を組み合わせるのが適切です。 教育対象と内容は、一般利用者・管理者・経営層など役割ごとのリスク差を踏まえて設計します。

対象：2026年度 / 基準日 2026-09-05

0103 組織・人的管理 > 教育・訓練・情報セキュリティ意識向上 ｜ 難易度：基礎

情報セキュリティにおけるリカレント教育の考え方として最も適切なものはどれか。

ア：重要なルールやコンプライアンス事項を繰り返し伝え、意識と行動の定着を図る。

イ：一度受講した従業員には二度と教育しない。

ウ：毎回内容を完全に無関係なものへ変更する。

エ：教育履歴を残さないことを原則とする。

答え・解説 正答：ア

ア：IPAシラバスは、コンプライアンス意識の定着を目指して繰り返し伝達するリカレント教育を挙げています。

イ：継続的な定着という考え方に反します。

ウ：重要事項を継続して理解・実践させることが目的です。

エ：実施状況や成果を評価するには記録も有用です。

総合解説：IPAシラバスは、コンプライアンス意識の定着を目指して繰り返し伝達するリカレント教育を挙げています。 繰り返し教育は、法令・規程・脅威の変化を反映しながら重要行動を定着させるために行います。

対象：2026年度 / 基準日 2026-09-05

0104 組織・人的管理 > 教育・訓練・情報セキュリティ意識向上 ｜ 難易度：標準

標的型メール訓練を実施したところ、模擬メールのリンクを開いた従業員がいた。最も適切な対応はどれか。

ア：対象者名を全社公開して見せしめにする。

イ：個人を責めるだけで終えず、報告手順や見分け方を再教育し、訓練結果を次回の改善に活用する。

ウ：結果を確認せず、毎回同じ訓練を繰り返す。

エ：一度失敗した従業員のメール利用を永久停止する。

答え・解説 正答：イ

ア：萎縮や報告回避を招き、改善につながりにくい対応です。

イ：訓練は失敗者を罰することが主目的ではなく、行動上の弱点を把握して教育・手順を改善するために行います。

ウ：成果評価と改善が欠けています。

エ：リスクに比例しない過剰対応であり、教育・改善の目的から外れます。

総合解説：訓練は失敗者を罰することが主目的ではなく、行動上の弱点を把握して教育・手順を改善するために行います。 訓練結果は、個人攻撃ではなく組織の弱点発見と手順改善に利用するのが基本です。

対象：2026年度 / 基準日 2026-09-05

0105 組織・人的管理 > 教育・訓練・情報セキュリティ意識向上 ｜ 難易度：標準

情報セキュリティ教育の有効性を評価する指標として、最も適切な組合せはどれか。

ア：受講者数だけを測定し、理解度は見ない。

イ：教育資料のページ数だけを測定する。

ウ：理解度テスト、訓練結果、インシデント報告行動などを組み合わせて確認する。

エ：講師の発言時間だけを測定する。

答え・解説 正答：ウ

ア：受講実績だけでは内容が身についたか分かりません。

イ：資料量は教育効果の直接的な指標ではありません。

ウ：受講率だけでなく、理解度や実際の行動が改善したかを複数指標で確認すると教育の有効性を評価しやすくなります。

エ：行動変容や理解度を示す指標ではありません。

総合解説：受講率だけでなく、理解度や実際の行動が改善したかを複数指標で確認すると教育の有効性を評価しやすくなります。 受講率が高くても安全行動が改善していなければ、教育の実効性は十分とはいえません。

対象：2026年度 / 基準日 2026-09-05

0106 組織・人的管理 > 教育・訓練・情報セキュリティ意識向上 ｜ 難易度：標準

情報セキュリティ規程を大幅改定し、USBメモリの利用ルールを変更した。最も適切な対応はどれか。

ア：規程を社内サイトに置くだけで周知は不要とする。

イ：旧ルールのまま運用し、事故が起きてから説明する。

ウ：IT部門だけに知らせ、USBを使う他部門には知らせない。

エ：改定内容と理由、具体的な操作・申請手順を対象者へ周知し、必要な教育を実施する。

答え・解説 正答：エ

ア：掲載だけでは対象者が変更を認識・理解したか確認できません。

イ：改定の意味がなく、予防的管理になりません。

ウ：利用者全体への必要な周知が不足します。

エ：規程変更は伝達するだけでなく、対象者が新しい行動を実践できるよう具体的な手順まで教育することが重要です。

総合解説：規程変更は伝達するだけでなく、対象者が新しい行動を実践できるよう具体的な手順まで教育することが重要です。 規程変更時は「何が変わったか」に加え、「現場で何をすべきか」まで伝える必要があります。

対象：2026年度 / 基準日 2026-09-05

0107 組織・人的管理 > 教育・訓練・情報セキュリティ意識向上 ｜ 難易度：標準

一般利用者とシステム管理者に同一の初級教育だけを実施している。改善策として最も適切なものはどれか。

ア：共通教育に加え、システム管理者には特権ID管理、ログ、変更手順など職務固有の教育を追加する。

イ：管理者は詳しいので教育対象から外す。

ウ：一般利用者にも管理者専用操作を全て実習させる。

エ：教育の代わりに管理者へ全権限を与える。

答え・解説 正答：ア

ア：特権を持つ役割は事故時の影響が大きいため、一般教育だけでなく職務別のリスク・手順に即した教育が必要です。

イ：知識があっても組織固有の手順や責任の教育が必要です。

ウ：必要以上の権限・知識を広げることは適切ではありません。

エ：権限付与は教育の代替ではありません。

総合解説：特権を持つ役割は事故時の影響が大きいため、一般教育だけでなく職務別のリスク・手順に即した教育が必要です。 特権利用者は影響範囲が大きいため、権限管理・変更管理・証跡管理を含む役割別教育が重要です。

対象：2026年度 / 基準日 2026-09-05

0108 組織・人的管理 > 教育・訓練・情報セキュリティ意識向上 ｜ 難易度：標準

従業員が不審メールを発見しても「誤報が怖い」と報告しないことが多い。最も適切な教育・訓練はどれか。

ア：誤報した従業員に罰則を科す。

イ：報告すべき兆候、連絡先、初動を具体的に示し、模擬事例で報告手順を練習する。

ウ：不審メールは各自で削除し、誰にも知らせない。

エ：報告先を毎月変更し、覚えにくくする。

答え・解説 正答：イ

ア：報告をさらに萎縮させるおそれがあります。

イ：報告の心理的・手続的ハードルを下げるには、何を・どこへ・どのように報告するかを具体化し、訓練することが有効です。

ウ：組織的な検知・対応につながりません。

エ：迅速な報告を妨げます。

総合解説：報告の心理的・手続的ハードルを下げるには、何を・どこへ・どのように報告するかを具体化し、訓練することが有効です。 早期報告を促すには、報告対象と窓口を明確にし、誤報を過度に恐れない文化を作ることも重要です。

対象：2026年度 / 基準日 2026-09-05

0109 組織・人的管理 > 教育・訓練・情報セキュリティ意識向上 ｜ 難易度：応用

毎年同じ標的型メール訓練を実施し、クリック率だけを評価している。より実効性を高める改善として最も適切なものはどれか。

ア：クリック率が下がるまで同じ文面だけを送る。

イ：結果が悪い部門の訓練を中止する。

ウ：最近の脅威や職務上のリスクを反映した複数シナリオを用い、報告率や初動の適切さも評価する。

エ：訓練結果を記録せず、感想だけで評価する。

答え・解説 正答：ウ

ア：学習が文面の暗記に偏り、別の攻撃へ一般化しにくくなります。

イ：弱点がある部門ほど改善の対象です。

ウ：実効的な訓練では、現実的な脅威を反映し、単なる失敗率だけでなく正しい報告・対応行動も評価します。

エ：継続的改善のため客観的な評価が必要です。

総合解説：実効的な訓練では、現実的な脅威を反映し、単なる失敗率だけでなく正しい報告・対応行動も評価します。 訓練は脅威の変化に合わせ、報告・初動・判断まで含めて評価すると実務性が高まります。

対象：2026年度 / 基準日 2026-09-05

0110 組織・人的管理 > 教育・訓練・情報セキュリティ意識向上 ｜ 難易度：応用

クラウド利用と在宅勤務が急増したが、教育内容は数年前のままである。最も適切な対応はどれか。

ア：過去に教育済みなので変更しない。

イ：クラウド利用者だけ自己責任とし、組織教育をやめる。

ウ：教育を技術用語の暗記だけに限定する。

エ：新しい業務形態で生じる認証、端末、情報共有等のリスクを再評価し、教育内容と訓練を更新する。

答え・解説 正答：エ

ア：環境変化で必要な知識・行動が変わります。

イ：組織の方針・手順を徹底する責任は残ります。

ウ：実務上の安全な行動や判断につながりません。

エ：業務・システム・脅威の変化に応じて教育内容も見直す必要があります。教育は固定的な年中行事ではなく、リスク管理の一部です。

総合解説：業務・システム・脅威の変化に応じて教育内容も見直す必要があります。教育は固定的な年中行事ではなく、リスク管理の一部です。 新しい働き方やサービス導入は新しいリスクを生むため、教育計画もリスクアセスメントと連動させます。

対象：2026年度 / 基準日 2026-09-05

0111 組織・人的管理 > 内部不正防止・コンプライアンス・自己点検 ｜ 難易度：基礎

不正のトライアングルを構成する三つの要素として適切なものはどれか。

ア：機会・動機（又はプレッシャー）・正当化

イ：機密性・完全性・可用性

ウ：識別・防御・復旧

エ：予防・検知・是正

答え・解説 正答：ア

ア：内部不正対策では、不正の機会、動機・プレッシャー、正当化という観点から要因を減らす考え方が用いられます。

イ：これは情報セキュリティの代表的な3特性です。

ウ：サイバーセキュリティ活動の一部を表す語であり、不正のトライアングルではありません。

エ：管理策の性質を表す分類であり、不正のトライアングルではありません。

総合解説：内部不正対策では、不正の機会、動機・プレッシャー、正当化という観点から要因を減らす考え方が用いられます。 内部不正は技術だけでなく心理・環境要因も関係するため、複数の観点から対策します。

対象：2026年度 / 基準日 2026-09-05

0112 組織・人的管理 > 内部不正防止・コンプライアンス・自己点検 ｜ 難易度：基礎

内部不正の「機会」を減らす対策として最も適切なものはどれか。

ア：全従業員に管理者権限を付与する。

イ：必要最小限の権限付与と職務分掌を行い、重要操作を記録・確認する。

ウ：重要操作のログを保存しない。

エ：退職予定者の権限を無期限に残す。

答え・解説 正答：イ

ア：不正や誤操作の機会を増やします。

イ：過大な権限や一人で完結できる業務は不正の機会を増やします。最小権限、職務分掌、ログ確認などが有効です。

ウ：検知・追跡可能性を低下させます。

エ：不要なアクセス機会を残します。

総合解説：過大な権限や一人で完結できる業務は不正の機会を増やします。最小権限、職務分掌、ログ確認などが有効です。 「機会」を減らす施策は、必要以上の権限や一人で完結できる重要処理を減らすことが中心です。

対象：2026年度 / 基準日 2026-09-05

0113 組織・人的管理 > 内部不正防止・コンプライアンス・自己点検 ｜ 難易度：基礎

情報セキュリティにおける自己点検の説明として最も適切なものはどれか。

ア：外部監査人だけが実施できる法定監査である。

イ：システムの性能測定だけを行う活動である。

ウ：部門などが自らルールの順守状況を確認し、問題点を把握して改善につなげる活動である。

エ：問題が見つかっても改善しないことを前提とする。

答え・解説 正答：ウ

ア：自己点検は外部監査に限定されません。

イ：順守状況や管理策の実施状況などを確認します。

ウ：自己点検は、現場が自ら統制やルールの順守状況を確認する活動です。内部監査とは目的や独立性の位置付けが異なります。

エ：問題把握と改善につなげることが重要です。

総合解説：自己点検は、現場が自ら統制やルールの順守状況を確認する活動です。内部監査とは目的や独立性の位置付けが異なります。 自己点検は日常的な統制確認に有効ですが、独立した監査による評価とは役割が異なります。

対象：2026年度 / 基準日 2026-09-05

0114 組織・人的管理 > 内部不正防止・コンプライアンス・自己点検 ｜ 難易度：標準

機密情報へアクセスできる従業員が退職する。最も適切な対応はどれか。

ア：退職後も問い合わせ対応のため権限を残す。

イ：貸与PCは本人の希望があればそのまま譲渡する。

ウ：退職者のアカウントを後任者が共有して使う。

エ：退職手続に合わせてアカウント・権限を無効化し、貸与物を回収し、必要な秘密保持義務を再確認する。

答え・解説 正答：エ

ア：不要な権限を残すと情報持出し等のリスクが高まります。

イ：データ消去・資産管理など必要な手続なしの譲渡は不適切です。

ウ：本人性・追跡可能性が失われます。

エ：退職・異動時には不要となるアクセス権を速やかに削除し、媒体・端末の回収や秘密保持の確認を行うことが内部不正防止につながります。

総合解説：退職・異動時には不要となるアクセス権を速やかに削除し、媒体・端末の回収や秘密保持の確認を行うことが内部不正防止につながります。 退職・異動はアクセス権を見直す代表的なトリガーであり、アカウントと貸与物を連動して管理します。

対象：2026年度 / 基準日 2026-09-05

0115 組織・人的管理 > 内部不正防止・コンプライアンス・自己点検 ｜ 難易度：標準

データベース管理者による大量データ抽出の内部不正を抑止・検知する施策として最も適切なものはどれか。

ア：特権操作を記録し、通常と異なる大量抽出などを独立した立場で定期的又は適時に確認する。

イ：管理者の操作は信頼してログ対象外にする。

ウ：全ログを管理者自身が自由に削除できるようにする。

エ：大量抽出を常に許可し、事後確認もしない。

答え・解説 正答：ア

ア：高権限者の操作も例外にせず記録・監視し、本人以外が確認できる仕組みにすることで抑止・検知を強化できます。

イ：特権者による不正・誤操作を検知できなくなります。

ウ：証跡の信頼性が損なわれます。

エ：異常な操作を見逃す可能性が高まります。

総合解説：高権限者の操作も例外にせず記録・監視し、本人以外が確認できる仕組みにすることで抑止・検知を強化できます。 高権限者も監視対象から除外せず、ログを本人だけで改変できないよう統制することが重要です。

対象：2026年度 / 基準日 2026-09-05

0116 組織・人的管理 > 内部不正防止・コンプライアンス・自己点検 ｜ 難易度：標準

新しい情報セキュリティ規程を制定した後の運用として最も適切なものはどれか。

ア：規程文書を保管するだけで利用者には知らせない。

イ：対象者へ内容を周知・教育し、定期的に順守状況を点検して必要な改善を行う。

ウ：一度周知したら変更があっても再教育しない。

エ：違反件数を隠して改善対象にしない。

答え・解説 正答：イ

ア：周知がなければ実効性を確保できません。

イ：規程は制定するだけでは機能しません。周知・教育、順守状況の評価、指摘への改善まで継続して運用します。

ウ：変更内容や継続的な意識定着には再周知が必要です。

エ：問題の把握・改善を妨げます。

総合解説：規程は制定するだけでは機能しません。周知・教育、順守状況の評価、指摘への改善まで継続して運用します。 コンプライアンスは規程の存在ではなく、周知・実施・点検・改善まで回して初めて機能します。

対象：2026年度 / 基準日 2026-09-05

0117 組織・人的管理 > 内部不正防止・コンプライアンス・自己点検 ｜ 難易度：標準

自己点検と内部監査の関係について最も適切なものはどれか。

ア：自己点検を行えば内部監査は必ず不要になる。

イ：内部監査では監査対象部門が結論を決める。

ウ：自己点検は現場自身の確認に有効であり、内部監査はより独立した立場から客観的に評価する役割を持つ。

エ：自己点検は監査指摘を隠すために行う。

答え・解説 正答：ウ

ア：独立した評価が必要な場面は残ります。

イ：監査の独立性・客観性を損ないます。

ウ：自己点検と内部監査は代替関係ではなく、異なる立場から統制の実効性を高める活動です。

エ：目的は順守状況の把握と改善です。

総合解説：自己点検と内部監査は代替関係ではなく、異なる立場から統制の実効性を高める活動です。自己点検と内部監査を組み合わせることで、現場の自律的改善と客観的評価の双方を得られます。

対象：2026年度 / 基準日 2026-09-05

0118 組織・人的管理 > 内部不正防止・コンプライアンス・自己点検 ｜ 難易度：標準

厳しすぎるファイル共有ルールのため、従業員が無断の個人クラウドを常用している。最も適切な対応はどれか。

ア：違反者を処分するだけでルールは一切見直さない。

イ：個人クラウド利用を正式手続なしに黙認する。

ウ：全ての共有業務を停止する。

エ：違反を是正するとともに業務上の必要性と現行ルールの妥当性を分析し、安全に利用できる代替手段や規程改定を検討する。

答え・解説 正答：エ

ア：根本原因が残り、違反が再発しやすくなります。

イ：シャドーITのリスクを固定化します。

ウ：事業要件とのバランスを欠く過剰対応です。

エ：IPAシラバスは、非現実的なルールに起因する違反の続出などを整理し、規程の妥当性を確認する継続的改善を求めています。

総合解説：IPAシラバスは、非現実的なルールに起因する違反の続出などを整理し、規程の妥当性を確認する継続的改善を求めています。 違反が頻発する場合は、利用者だけでなくルールや業務設計そのものに原因がないか確認します。

対象：2026年度 / 基準日 2026-09-05

0119 組織・人的管理 > 内部不正防止・コンプライアンス・自己点検 ｜ 難易度：応用

研究データの持出しによる内部不正リスクが高い部門で、最も実効性の高い対策の組合せはどれか。

ア：権限最小化、持出しルール、ログ監視、教育、相談・通報経路、退職時管理を組み合わせる。

イ：秘密保持誓約書だけに依存する。

ウ：USBメモリ禁止だけを実施し、クラウドやメールは無制限にする。

エ：全員を常時監視し、業務上必要なアクセスも禁止する。

答え・解説 正答：ア

ア：内部不正には単一の対策だけでなく、抑止・予防・検知・事後対応を組み合わせることが重要です。

イ：誓約書は抑止策の一つですが、技術的・運用的対策も必要です。

ウ：別経路の持出しリスクが残ります。

エ：過剰な対策は業務を阻害し、リスクに応じた統制になりません。

総合解説：内部不正には単一の対策だけでなく、抑止・予防・検知・事後対応を組み合わせることが重要です。 内部不正対策は、抑止・予防・検知・対応を組み合わせ、単一管理策への依存を避けます。

対象：2026年度 / 基準日 2026-09-05

0120 組織・人的管理 > 内部不正防止・コンプライアンス・自己点検 ｜ 難易度：応用

自己点検で複数部署に同じ規程違反が見つかった。最も適切な次の対応はどれか。

ア：各部署へ注意メールを一度送り、記録を残さない。

イ：違反の共通原因を分析し、責任者・期限・確認方法を含む改善計画を作成して実施状況を追跡する。

ウ：違反件数を減らすため次回から点検項目を削除する。

エ：改善期限を定めず、対応は各担当者の任意とする。

答え・解説 正答：イ

ア：原因分析や実施確認がなく、再発防止の実効性が低いです。

イ：複数部署で同じ違反が起きる場合、個人の注意不足だけでなく規程・教育・仕組みの問題を疑い、組織的な是正につなげる必要があります。

ウ：問題の可視化を避けるだけで改善になりません。

エ：責任と期限が曖昧で進捗管理できません。

総合解説：複数部署で同じ違反が起きる場合、個人の注意不足だけでなく規程・教育・仕組みの問題を疑い、組織的な是正につなげる必要があります。 同じ違反が横断的に見つかる場合は、個別是正だけでなく共通原因への組織的対策が必要です。

対象：2026年度 / 基準日 2026-09-05

0121 外部委託・クラウド管理 > 委託先の選定・事前評価・要求事項 ｜ 難易度：基礎

機密情報を扱う業務を外部委託する前に、最初に行うべきこととして最も適切なものはどれか。

ア：価格だけを比較し、契約後にセキュリティ条件を決める。

イ：委託先の知名度だけで安全と判断する。

ウ：委託する情報・業務・リスクを整理し、委託先に求める情報セキュリティ要求事項を明確にする。

エ：全てのリスクを委託先へ移転したことにする。

答え・解説 正答：ウ

ア：事前評価の基準がなくなり、必要な対策を契約に反映できません。

イ：知名度は要求事項への適合を保証しません。

ウ：委託先を評価するには、まず何を守るのか、どのような要求を満たす必要があるのかを明確にする必要があります。

エ：委託元の管理責任は残ります。

総合解説：委託先を評価するには、まず何を守るのか、どのような要求を満たす必要があるのかを明確にする必要があります。 委託前に守る対象と要求水準を決めておくことで、候補先を同じ基準で比較できます。

対象：2026年度 / 基準日 2026-09-05

0122 外部委託・クラウド管理 > 委託先の選定・事前評価・要求事項 ｜ 難易度：基礎

委託候補先のセキュリティ対策状況を事前確認する方法として最も適切なものはどれか。

ア：営業担当者の口頭説明だけで評価を終える。

イ：契約締結後まで確認を行わない。

ウ：セキュリティ事故歴が不明でも無条件で採用する。

エ：質問票だけでなく、必要に応じて規程、監査報告、認証範囲などの証跡を確認する。

答え・解説 正答：エ

ア：客観的な裏付けが不足します。

イ：事前に要求事項とのかい離を把握する必要があります。

ウ：リスクに関する情報を収集・評価すべきです。

エ：IPAの実践例でも、アンケートに加えて回答を裏付ける証跡を求め、総合的に評価する考え方が示されています。

総合解説：IPAの実践例でも、アンケートに加えて回答を裏付ける証跡を求め、総合的に評価する考え方が示されています。 質問票は入口であり、重要事項は証跡や第三者評価などで裏付けることが評価精度を高めます。

対象：2026年度 / 基準日 2026-09-05

0123 外部委託・クラウド管理 > 委託先の選定・事前評価・要求事項 ｜ 難易度：基礎

委託先がISMS認証を取得している場合の評価として最も適切なものはどれか。

ア：認証取得を有力な情報の一つとして確認しつつ、認証範囲や自社要求事項への適合も確認する。

イ：認証があれば自社の要求事項確認は一切不要である。

ウ：認証がなければ必ず委託不可である。

エ：認証書の有効期限や範囲は確認しなくてよい。

答え・解説 正答：ア

ア：認証は管理体制の評価材料になりますが、対象範囲が委託業務を含むか、自社固有の要求事項を満たすかは別途確認が必要です。

イ：認証範囲や契約固有要件との適合確認が必要です。

ウ：リスクや要求に応じた総合評価が必要で、一律に決まるものではありません。

エ：有効性や適用範囲の確認が重要です。

総合解説：認証は管理体制の評価材料になりますが、対象範囲が委託業務を含むか、自社固有の要求事項を満たすかは別途確認が必要です。 認証は有力な証拠ですが、認証範囲と自社が委託する業務範囲の一致を確認する必要があります。

対象：2026年度 / 基準日 2026-09-05

0124 外部委託・クラウド管理 > 委託先の選定・事前評価・要求事項 ｜ 難易度：標準

委託候補先の事前評価で、自社の要求するログ保存期間を満たしていないことが分かった。最も適切な対応はどれか。

ア：契約後に考えることにして、そのまま採用する。

イ：かい離によるリスクを評価し、是正方法・時期・費用負担などを契約担当者と委託先で調整してから判断する。

ウ：要求事項を黙って削除して評価を合わせる。

エ：委託先へ理由を伝えず即時排除する以外に方法はない。

答え・解説 正答：イ

ア：未解決の重要要件を放置することになります。

イ：IPAシラバスでは、要求事項と委託先の現状との差異を事前確認し、是正が必要なら対応方法・時期・費用を調整することを求めています。

ウ：リスク受容の判断なしに要求水準を下げるのは不適切です。

エ：是正可能性や代替管理策を含めて評価・調整できます。

総合解説：IPAシラバスでは、要求事項と委託先の現状との差異を事前確認し、是正が必要なら対応方法・時期・費用を調整することを求めています。 要求とのかい離は、重大度・代替策・是正期限を踏まえて、受容できるかを判断します。

対象：2026年度 / 基準日 2026-09-05

0125 外部委託・クラウド管理 > 委託先の選定・事前評価・要求事項 ｜ 難易度：標準

委託先が業務の一部を再委託する予定である。委託元の対応として最も適切なものはどれか。

ア：再委託先は直接契約していないので一切確認しない。

イ：再委託を認める代わりにセキュリティ要求を免除する。

ウ：再委託の条件、情報の取扱い、セキュリティ要求の継承、再委託先の管理方法を確認する。

エ：委託先名だけ分かれば管理方法は不要である。

答え・解説 正答：ウ

ア：サプライチェーン上のリスクを見落とします。

イ：要求水準を下げる合理的理由にはなりません。

ウ：委託先の先に再委託先がある場合も、情報がどこで扱われ、要求事項がどのように維持されるかを確認する必要があります。

エ：対策状況や責任範囲の把握が必要です。

総合解説：委託先の先に再委託先がある場合も、情報がどこで扱われ、要求事項がどのように維持されるかを確認する必要があります。 再委託では、要求事項がサプライチェーンの先まで維持される仕組みを確認することが重要です。

対象：2026年度 / 基準日 2026-09-05

0126 外部委託・クラウド管理 > 委託先の選定・事前評価・要求事項 ｜ 難易度：標準

顧客情報を扱う委託先に対する要求事項として、インシデント対応の観点から最も適切なものはどれか。

ア：事故が起きても委託先の判断で報告しなくてよいとする。

イ：報告方法を定めず、事故発生後に協議する。

ウ：事故情報は契約終了まで一切共有しないとする。

エ：事故の報告条件、連絡先、報告期限、必要な初動・協力事項をあらかじめ定める。

答え・解説 正答：エ

ア：委託元が影響評価や対応を行えなくなります。

イ：初動が遅れるおそれがあります。

ウ：迅速な対応に反します。

エ：インシデント時の連絡や役割を契約前から具体化しておくことで、発生時の遅延や認識齟齬を減らせます。

総合解説：インシデント時の連絡や役割を契約前から具体化しておくことで、発生時の遅延や認識齟齬を減らせます。 事故報告条項は、何を事故とするか、いつまでに誰へ何を報告するかを具体化すると実効性が高まります。

対象：2026年度 / 基準日 2026-09-05

0127 外部委託・クラウド管理 > 委託先の選定・事前評価・要求事項 ｜ 難易度：標準

100社の取引先を一斉に同じ深さで評価することが困難である。最も適切な考え方はどれか。

ア：扱う情報の重要度、接続範囲、業務停止影響などでリスクを分類し、高リスクの委託先から重点評価する。

イ：会社規模だけで評価対象を決める。

ウ：全社を評価できないなら一社も評価しない。

エ：契約金額が低ければ機密情報を扱っても評価しない。

答え・解説 正答：ア

ア：委託先管理はリスクに応じて重点化することが合理的です。IPAの実践例でも、まずサイバーセキュリティリスクのある委託先を特定して対策状況を確認しています。

イ：規模だけでは自社への影響を判断できません。

ウ：高リスクから着手する考え方が有効です。

エ：情報・接続・事業影響などを含めて判断すべきです。

総合解説：委託先管理はリスクに応じて重点化することが合理的です。IPAの実践例でも、まずサイバーセキュリティリスクのある委託先を特定して対策状況を確認しています。 委託先の評価優先度は、契約金額ではなく自社の情報・接続・業務への影響を軸に決めます。

対象：2026年度 / 基準日 2026-09-05

0128 外部委託・クラウド管理 > 委託先の選定・事前評価・要求事項 ｜ 難易度：標準

委託先に「十分なセキュリティ対策をすること」とだけ要求している。改善として最も適切なものはどれか。

ア：「十分」の意味は委託先だけに任せる。

イ：アクセス制御、パッチ適用、ログ、バックアップ、事故報告など必要な管理策と確認方法を具体化する。

ウ：要求事項を口頭だけで伝え、記録しない。

エ：セキュリティ要求を価格交渉の後に全て削除する。

答え・解説 正答：イ

ア：委託元の要求水準との齟齬が生じやすくなります。

イ：抽象的な要求だけでは適合性を判断しにくいため、リスクに応じて具体的で検証可能な要求へ落とし込む必要があります。

ウ：契約・運用時の確認が困難になります。

エ：必要な管理策を失い、リスクが高まります。

総合解説：抽象的な要求だけでは適合性を判断しにくいため、リスクに応じて具体的で検証可能な要求へ落とし込む必要があります。 要求事項は実施有無を確認できる粒度まで具体化し、確認方法も同時に決めるのが実務的です。

対象：2026年度 / 基準日 2026-09-05

0129 外部委託・クラウド管理 > 委託先の選定・事前評価・要求事項 ｜ 難易度：応用

新しいSaaSを導入する際、IT部門だけでは利用規約・個人情報・契約条件の判断が難しい。最も適切な対応はどれか。

ア：IT部門が分からない条項は全て無視する。

イ：利用部門だけで導入し、セキュリティ部門には知らせない。

ウ：情報セキュリティ、法務、個人情報、業務部門など必要な関係者で評価し、要求事項への適合を確認する。

エ：ベンダーの広告内容だけで安全性を判断する。

答え・解説 正答：ウ

ア：契約上の重要リスクを見落とします。

イ：シャドーITや不適切な情報取扱いにつながります。

ウ：外部サービス選定では、技術だけでなく契約・法務・業務上の観点も関わるため、必要な部門を巻き込むことが重要です。

エ：客観的な要求適合確認が不足します。

総合解説：外部サービス選定では、技術だけでなく契約・法務・業務上の観点も関わるため、必要な部門を巻き込むことが重要です。 外部サービスの選定では技術評価だけでなく、法務・個人情報・業務継続などの観点を統合します。

対象：2026年度 / 基準日 2026-09-05

0130 外部委託・クラウド管理 > 委託先の選定・事前評価・要求事項 ｜ 難易度：応用

委託先の選定時には要件を満たしていたが、契約開始までにシステム構成が大きく変わった。最も適切な対応はどれか。

ア：選定時に合格していれば以後の確認は不要とする。

イ：変更内容を確認せず契約期間だけ延長する。

ウ：構成変更を理由に要求事項を全て撤回する。

エ：開始時にセキュリティが担保されていることを再確認し、重要な変更があればリスクと要求適合性を再評価する。

答え・解説 正答：エ

ア：環境変更でリスクや適合状況が変わる可能性があります。

イ：更新判断の根拠が不足します。

ウ：必要なセキュリティ水準を失います。

エ：IPAシラバスは委託開始時と更新時にもセキュリティが担保されていることの確認を求めています。選定時評価だけで固定しないことが重要です。

総合解説：IPAシラバスは委託開始時と更新時にもセキュリティが担保されていることの確認を求めています。選定時評価だけで固定しないことが重要です。 委託先の環境が大きく変わった場合、選定時の評価結果をそのまま使わず再評価します。

対象：2026年度 / 基準日 2026-09-05

0131 外部委託・クラウド管理 > 契約・NDA・SLA・責任共有モデル ｜ 難易度：基礎

外部委託契約に情報セキュリティ事項を盛り込む目的として最も適切なものはどれか。

ア：委託業務の範囲、情報の取扱い、役割・責任、事故時対応などを双方で明確にする。

イ：委託元の全責任を自動的に消滅させる。

ウ：委託先に自由な情報利用権を与える。

エ：セキュリティ事項を口頭合意だけにする。

答え・解説 正答：ア

ア：契約によって必要な管理策や責任分担を明確にし、実施状況を確認できる状態にすることが重要です。

イ：契約しても委託元の管理責任は残ります。

ウ：利用目的・範囲は必要に応じて制限すべきです。

エ：齟齬や確認困難を招きます。

総合解説：契約によって必要な管理策や責任分担を明確にし、実施状況を確認できる状態にすることが重要です。 契約はセキュリティ要求を双方の義務として明確にし、運用時の確認基準にもなります。

対象：2026年度 / 基準日 2026-09-05

0132 外部委託・クラウド管理 > 契約・NDA・SLA・責任共有モデル ｜ 難易度：基礎

NDA（秘密保持契約）の主な目的として最も適切なものはどれか。

ア：サービス稼働率を99.9%に保証する。

イ：開示された秘密情報の取扱い、利用目的、第三者提供等の条件を定め、秘密保持義務を明確にする。

ウ：全ての知的財産権を自動的に移転する。

エ：委託先の全従業員に管理者権限を与える。

答え・解説 正答：イ

ア：これはSLAなどで扱うサービスレベルの論点です。

イ：NDAは秘密情報の取扱いに関する義務を契約上明確にする手段です。可用性やサービス性能の保証そのものではありません。

ウ：NDAの主目的ではありません。

エ：秘密保持とは逆に情報アクセスのリスクを高めます。

総合解説：NDAは秘密情報の取扱いに関する義務を契約上明確にする手段です。可用性やサービス性能の保証そのものではありません。 NDAは秘密保持の範囲を定めるものであり、可用性や応答時間などは別の契約条件で扱います。

対象：2026年度 / 基準日 2026-09-05

0133 外部委託・クラウド管理 > 契約・NDA・SLA・責任共有モデル ｜ 難易度：基礎

SLAの説明として最も適切なものはどれか。

ア：秘密情報の定義だけを定める契約である。

イ：従業員の人事評価基準だけを定める文書である。

ウ：提供するサービスの水準について、可用性や応答時間など測定可能な目標を合意するものである。

エ：暗号アルゴリズムの国際標準を定める文書である。

答え・解説 正答：ウ

ア：これはNDAに近い内容です。

イ：SLAの対象ではありません。

ウ：IPAシラバスではSLAをサービスレベル合意書として扱い、サービス時間、応答時間、サービスレベル目標などを挙げています。

エ：SLAはサービスレベルに関する合意です。

総合解説：IPAシラバスではSLAをサービスレベル合意書として扱い、サービス時間、応答時間、サービスレベル目標などを挙げています。 SLAでは「何を、どの基準で、どの期間に測るか」を明確にすることが基本です。

対象：2026年度 / 基準日 2026-09-05

0134 外部委託・クラウド管理 > 契約・NDA・SLA・責任共有モデル ｜ 難易度：標準

クラウドサービスのSLA条項として、最も評価しやすいものはどれか。

ア：高品質なサービスを可能な限り提供する。

イ：障害時はなるべく早く連絡する。

ウ：利用者が満足するよう努力する。

エ：月間稼働率99.9%以上、重大障害の初回応答30分以内など測定方法を含む目標を定める。

答え・解説 正答：エ

ア：基準が曖昧で達成状況を客観的に評価しにくいです。

イ：「なるべく早く」では測定可能な基準になりません。

ウ：主観的で客観的なサービスレベル評価が困難です。

エ：SLAは達成状況を確認できるよう、対象・指標・基準・測定条件を明確にすることが重要です。

総合解説：SLAは達成状況を確認できるよう、対象・指標・基準・測定条件を明確にすることが重要です。 曖昧な表現では未達成を判定できないため、SLAは測定可能な数値や条件へ落とし込みます。

対象：2026年度 / 基準日 2026-09-05

0135 外部委託・クラウド管理 > 契約・NDA・SLA・責任共有モデル ｜ 難易度：標準

委託先で情報漏えいが発生した場合に備え、契約で最も明確にすべき事項はどれか。

ア：連絡期限、初動、証拠保全、原因調査への協力、顧客対応など双方の役割と責任を定める。

イ：事故対応は全て発生後に口頭で決める。

ウ：委託元は事故情報を受け取らない。

エ：委託先が報告しなくても違反にならないようにする。

答え・解説 正答：ア

ア：事故時の役割・連絡・協力事項を事前に定めることで、責任の空白や初動遅延を防ぎます。

イ：緊急時に混乱・遅延を招きます。

ウ：影響評価や必要な対応ができません。

エ：重要事故の把握を妨げます。

総合解説：事故時の役割・連絡・協力事項を事前に定めることで、責任の空白や初動遅延を防ぎます。事故対応条項には、通知だけでなく調査協力・証拠保全・復旧・対外対応まで含めると責任の空白を減らせます。

対象：2026年度 / 基準日 2026-09-05

0136 外部委託・クラウド管理 > 契約・NDA・SLA・責任共有モデル ｜ 難易度：標準

重要業務を委託する契約で、対策の実施状況を継続確認しやすくする条項として最も適切なものはどれか。

ア：委託先の自己申告は一切確認しないと定める。

イ：必要な報告、証跡提出、監査又は第三者評価結果の確認方法を定める。

ウ：契約期間中はセキュリティについて質問しないと定める。

エ：監査ログの廃棄を毎日義務付ける。

答え・解説 正答：イ

ア：実施状況の客観的確認ができません。

イ：契約後も要求事項の実施状況を確認できるよう、報告や検証方法をあらかじめ合意しておくことが有効です。

ウ：変化や不備を把握できません。

エ：必要な証跡が失われます。

総合解説：契約後も要求事項の実施状況を確認できるよう、報告や検証方法をあらかじめ合意しておくことが有効です。 継続確認の方法を契約で確保しておくと、委託先の対策状況を客観的に追跡しやすくなります。

対象：2026年度 / 基準日 2026-09-05

0137 外部委託・クラウド管理 > 契約・NDA・SLA・責任共有モデル ｜ 難易度：標準

クラウドの責任共有モデルについて最も適切な説明はどれか。

ア：クラウドでは利用者側のセキュリティ責任は常にゼロである。

イ：責任範囲は全てのクラウドサービスで同一である。

ウ：サービスモデルや契約に応じて事業者と利用者の責任範囲が分かれ、利用者側にもデータ・ID・設定等の責任が残る。

エ：責任共有モデルは料金分担だけを示す。

答え・解説 正答：ウ

ア：利用者はデータ、ID、アクセス管理等に関する責任を持ち続けます。

イ：サービスモデルや契約・機能によって異なります。

ウ：クラウド利用では「事業者が全て守る」のではなく、IaaS/PaaS/SaaSなどに応じて責任分担が変わります。

エ：セキュリティ管理の責任分担に関する考え方です。

総合解説：クラウド利用では「事業者が全て守る」のではなく、IaaS/PaaS/SaaSなどに応じて責任分担が変わります。 クラウドでは利用者が制御できる範囲ほど利用者責任が残る、と理解すると責任分担を整理しやすくなります。

対象：2026年度 / 基準日 2026-09-05

0138 外部委託・クラウド管理 > 契約・NDA・SLA・責任共有モデル ｜ 難易度：標準

IaaS上の仮想マシンを利用する企業で、一般に利用者側の責任となるものはどれか。

ア：データセンター建物の物理警備を利用者が直接実施する。

イ：クラウド事業者の物理サーバを利用者が交換する。

ウ：サービス利用者のID管理も必ず事業者だけが行う。

エ：仮想マシンのOSやアプリケーションの設定・更新、利用者アカウントやアクセス制御を適切に管理する。

答え・解説 正答：エ

ア：物理データセンターは通常クラウド事業者側の責任です。

イ：物理ホストは通常事業者側が管理します。

ウ：利用者組織は自組織のユーザー・アクセス管理を担います。

エ：IaaSでは物理基盤等をクラウド事業者が管理しても、ゲストOSやアプリケーション、ID・アクセス管理などは利用者側が担うのが一般的です。

総合解説：IaaSでは物理基盤等をクラウド事業者が管理しても、ゲストOSやアプリケーション、ID・アクセス管理などは利用者側が担うのが一般的です。 IaaSはオンプレミスより基盤管理が減りますが、ゲストOSやアプリの管理責任までなくなるわけではありません。

対象：2026年度 / 基準日 2026-09-05

0139 外部委託・クラウド管理 > 契約・NDA・SLA・責任共有モデル ｜ 難易度：応用

SaaSを導入した企業が「サービス事業者が安全対策をするので自社の設定は不要」と判断した。最も適切な評価はどれか。

ア：誤りであり、利用者アカウント、権限、MFA設定、データ取扱いなど自社に残る責任を管理する必要がある。

イ：正しく、SaaSでは利用者が行うセキュリティ管理は一切ない。

ウ：正しく、退職者アカウントも事業者が自動削除する義務が常にある。

エ：誤りだが、利用者がクラウド事業者のデータセンター警備を担当する必要がある。

答え・解説 正答：ア

ア：SaaSではインフラ等の多くを事業者が管理しますが、利用者のID・アクセス・データ・設定等まで無条件に委ねられるわけではありません。

イ：共有責任モデルに反します。

ウ：自組織のアカウントライフサイクル管理は利用者側の責任です。

エ：物理インフラは通常事業者側の責任です。

総合解説：SaaSではインフラ等の多くを事業者が管理しますが、利用者のID・アクセス・データ・設定等まで無条件に委ねられるわけではありません。 SaaSでもアカウント管理や権限設定を誤れば漏えいは起こり得るため、利用者側の設定管理が重要です。

対象：2026年度 / 基準日 2026-09-05

0140 外部委託・クラウド管理 > 契約・NDA・SLA・責任共有モデル ｜ 難易度：応用

契約では「再委託禁止」と定めているが、実際には委託先が一部作業を第三者へ再委託していることが判明した。最も適切な対応はどれか。

ア：実際に動いているので契約違反は無視する。

イ：齟齬の理由とリスクを確認し、契約担当者と連携して是正措置、必要な契約変更又は停止等を判断する。

ウ：契約書を事後的に無断で書き換える。

エ：再委託先の存在を記録せず、口頭で了承する。

答え・解説 正答：イ

ア：契約と実態の不一致を放置すると責任や管理の空白が生じます。

イ：IPAシラバスでは、委託業務の実施内容と契約内容に相違がある場合、理由・課題を明確にし、契約担当者と協力して是正することを求めています。

ウ：双方の合意や適切な手続が必要です。

エ：サプライチェーンの可視性・追跡可能性が失われます。

総合解説：IPAシラバスでは、委託業務の実施内容と契約内容に相違がある場合、理由・課題を明確にし、契約担当者と協力して是正することを求めています。 契約と実態がずれた場合は、黙認せず原因・影響・是正方法を整理して正式に解消します。

対象：2026年度 / 基準日 2026-09-05

0141 外部委託・クラウド管理 > 実施状況確認・更新・終了・データ回収／廃棄 ｜ 難易度：基礎

委託契約締結後のセキュリティ管理として最も適切なものはどれか。

ア：契約した時点で全ての確認を終了する。

イ：事故が発生するまで委託先と連絡を取らない。

ウ：契約上の要求事項が実施されているか、報告や証跡などを用いて継続的に確認する。

エ：確認結果は記録せず担当者の記憶だけに残す。

答え・解説 正答：ウ

ア：環境や運用は変化するため継続確認が必要です。

イ：問題の早期把握や予防ができません。

ウ：委託先管理は選定・契約で終わらず、契約期間中の実施状況を確認する必要があります。

エ：追跡・説明・更新判断に利用できません。

総合解説：委託先管理は選定・契約で終わらず、契約期間中の実施状況を確認する必要があります。 委託先管理は契約書の保管ではなく、要求事項が実際に守られているかを確認する活動です。

対象：2026年度 / 基準日 2026-09-05

0142 外部委託・クラウド管理 > 実施状況確認・更新・終了・データ回収／廃棄 ｜ 難易度：基礎

外部委託契約を更新する際の対応として最も適切なものはどれか。

ア：前回の審査に合格していれば永久に再評価不要とする。

イ：更新時は価格だけを確認する。

ウ：過去の事故情報を評価対象から除外する。

エ：事故履歴、対策状況、業務・システム変更などを確認し、現行要求事項を満たしているか再評価する。

答え・解説 正答：エ

ア：状況変化を反映できません。

イ：セキュリティ要件の継続適合を確認できません。

ウ：改善状況やリスク判断に有用な情報です。

エ：IPAシラバスは委託開始時と更新時に情報セキュリティが担保されていることの確認を求めています。

総合解説：IPAシラバスは委託開始時と更新時に情報セキュリティが担保されていることの確認を求めています。 更新は価格や期間だけでなく、事故・変更・対策状況を踏まえて継続可否を判断する機会です。

対象：2026年度 / 基準日 2026-09-05

0143 外部委託・クラウド管理 > 実施状況確認・更新・終了・データ回収／廃棄 ｜ 難易度：基礎

外部委託の終了時に最も重要な情報セキュリティ対応はどれか。

ア：委託先へ提供した資料・データの回収又は適切な廃棄を指示し、その実施結果を確認する。

イ：契約終了後も全データを無期限に保持させる。

ウ：終了時の確認を行わず口頭で「消した」と聞くだけにする。

エ：委託先アカウントを残して再利用に備える。

答え・解説 正答：ア

ア：IPAシラバスは、委託終了時に資料やデータの回収・廃棄を指示し、実施結果を確認して文書化・報告することを求めています。

イ：不要なデータ保持は漏えいリスクを残します。

ウ：実施結果の確認が不十分です。

エ：不要なアクセス経路を残します。

総合解説：IPAシラバスは、委託終了時に資料やデータの回収・廃棄を指示し、実施結果を確認して文書化・報告することを求めています。 委託終了は情報ライフサイクルの重要な管理点で、データとアクセス権を残さないことが基本です。

対象：2026年度 / 基準日 2026-09-05

0144 外部委託・クラウド管理 > 実施状況確認・更新・終了・データ回収／廃棄 ｜ 難易度：標準

委託先がデータセンター所在地と利用するクラウド基盤を変更した。最も適切な対応はどれか。

ア：契約期間中なので変更内容は確認しない。

イ：変更内容が自社の情報セキュリティ要求やリスクに与える影響を確認し、必要に応じて再評価・契約見直しを行う。

ウ：変更があれば必ず即時契約解除する。

エ：委託先が決めた変更は自社に影響しないとみなす。

答え・解説 正答：イ

ア：リスクの変化を見落とします。

イ：重要な運用・システム変更は、契約時の前提やリスクを変えるため、再評価の契機となります。

ウ：影響を評価した上で適切な対応を選ぶべきです。

エ：自社データやサービスに影響する可能性があります。

総合解説：重要な運用・システム変更は、契約時の前提やリスクを変えるため、再評価の契機となります。 構成・保管場所・再委託先など重要前提の変更は、リスク再評価のトリガーとして扱います。

対象：2026年度 / 基準日 2026-09-05

0145 外部委託・クラウド管理 > 実施状況確認・更新・終了・データ回収／廃棄 ｜ 難易度：標準

定期確認で委託先のパッチ適用が契約要件より遅れていることが分かった。最も適切な対応はどれか。

ア：指摘だけして完了確認はしない。

イ：違反を隠すため評価記録を削除する。

ウ：リスクと原因を確認し、是正内容・期限・責任者を合意して進捗と完了を確認する。

エ：要求事項を自動的に削除して適合扱いにする。

答え・解説 正答：ウ

ア：是正が実際に行われたか確認できません。

イ：ガバナンスと監査可能性を損ないます。

ウ：不適合を発見したら、是正の方法・時期を明確にし、実施結果までフォローする必要があります。

エ：リスク受容の判断なしに要求水準を下げるのは不適切です。

総合解説：不適合を発見したら、是正の方法・時期を明確にし、実施結果までフォローする必要があります。 是正管理では、指摘するだけでなく期限と完了条件を定め、実施結果まで確認します。

対象：2026年度 / 基準日 2026-09-05

0146 外部委託・クラウド管理 > 実施状況確認・更新・終了・データ回収／廃棄 ｜ 難易度：標準

委託先でセキュリティ事故が発生した後、サービス復旧だけが確認できた。委託元の追加対応として最も適切なものはどれか。

ア：復旧したので原因調査は不要とする。

イ：事故記録を破棄して評価から除外する。

ウ：委託元側の影響確認は行わない。

エ：原因、影響範囲、再発防止策、契約要求への適合状況を確認し、必要な改善を追跡する。

答え・解説 正答：エ

ア：同種事故の再発防止につながりません。

イ：更新やリスク評価の重要な情報を失います。

ウ：自社データや業務への影響評価が必要です。

エ：復旧だけで終えず、事故原因と再発防止、委託管理上の問題を確認して継続的改善につなげることが必要です。

総合解説：復旧だけで終えず、事故原因と再発防止、委託管理上の問題を確認して継続的改善につなげることが必要です。 委託先事故は、契約要求や監督方法そのものに改善余地がないかを見直す契機にもなります。

対象：2026年度 / 基準日 2026-09-05

0147 外部委託・クラウド管理 > 実施状況確認・更新・終了・データ回収／廃棄 ｜ 難易度：標準

保守委託契約が終了した。最も適切なアクセス管理はどれか。

ア：委託先に付与したVPN、特権ID、APIキーなど不要となったアクセス手段を速やかに無効化・回収する。

イ：将来再契約するかもしれないので全権限を残す。

ウ：アカウント名だけ変更し、同じ認証情報を使い続ける。

エ：VPNは停止するが共有管理者パスワードは変更しない。

答え・解説 正答：ア

ア：契約終了後にアクセス手段を残すと不正利用のリスクになります。権限・認証情報をライフサイクルに合わせて終了させます。

イ：不要な権限は残すべきではありません。

ウ：実質的にアクセス経路が残ります。

エ：他のアクセス経路や共有認証情報の見直しも必要です。

総合解説：契約終了後にアクセス手段を残すと不正利用のリスクになります。権限・認証情報をライフサイクルに合わせて終了させます。 契約終了時は、VPN・ID・APIキー・証明書など複数のアクセス経路を漏れなく無効化します。

対象：2026年度 / 基準日 2026-09-05

0148 外部委託・クラウド管理 > 実施状況確認・更新・終了・データ回収／廃棄 ｜ 難易度：標準

委託終了時、委託先から「データは削除済み」とメール連絡があった。高機密情報を扱っていた場合の対応として最も適切なものはどれか。

ア：メールがあれば内容確認は不要とする。

イ：契約や手順に従い、削除・廃棄の対象と方法、実施者、完了結果を確認できる記録や証跡を取得する。

ウ：委託先にバックアップを永久保存させる。

エ：削除結果を記録せず、担当者が覚えておく。

答え・解説 正答：イ

ア：対象漏れや不適切な削除方法を見落とす可能性があります。

イ：高重要度データでは、単なる口頭・メール申告だけでなく、合意した方法で廃棄が完了したことを確認できる証跡が重要です。

ウ：契約上必要でなければ不要な保持リスクとなります。

エ：監査・報告・説明のため文書化が必要です。

総合解説：高重要度データでは、単なる口頭・メール申告だけでなく、合意した方法で廃棄が完了したことを確認できる証跡が重要です。 高機密データの廃棄では、対象・方法・完了の証跡を残すことで説明可能性を確保します。

対象：2026年度 / 基準日 2026-09-05

0149 外部委託・クラウド管理 > 実施状況確認・更新・終了・データ回収／廃棄 ｜ 難易度：応用

委託先が再委託先にも自社データを渡していた。契約終了時の対応として最も適切なものはどれか。

ア：一次委託先のPCだけ削除すれば十分とする。

イ：再委託先のデータは委託元と無関係とみなす。

ウ：委託先だけでなく再委託先を含むデータ所在を確認し、契約上の要求に従って回収・廃棄と完了確認を行う。

エ：終了後のデータ所在は確認しない。

答え・解説 正答：ウ

ア：再委託先にコピーが残る可能性があります。

イ：自社情報であれば管理対象です。

ウ：データがサプライチェーン上に広がっている場合、一次委託先だけの削除では残存リスクがあります。要求事項を再委託先まで実効的に及ぼす必要があります。

エ：残存データによる漏えいリスクを把握できません。

総合解説：データがサプライチェーン上に広がっている場合、一次委託先だけの削除では残存リスクがあります。要求事項を再委託先まで実効的に及ぼす必要があります。 再委託先を含むデータ所在を把握していないと、契約終了後もコピーが残るリスクがあります。

対象：2026年度 / 基準日 2026-09-05

0150 外部委託・クラウド管理 > 実施状況確認・更新・終了・データ回収／廃棄 ｜ 難易度：応用

重要業務の委託終了処理を完了した。最終確認として最も適切なものはどれか。

ア：担当者が口頭で「完了」と言えば記録は不要とする。

イ：完了記録には成功した項目だけを残し、未完了を除外する。

ウ：契約終了後は一切の確認や報告を禁止する。

エ：データ回収・廃棄、アカウント停止、貸与物回収などの結果を文書化し、必要な責任者へ報告する。

答え・解説 正答：エ

ア：後から検証・説明できません。

イ：残課題を隠すことになり、リスク管理できません。

ウ：終了管理の証跡・説明責任を損ないます。

エ：IPAシラバスでは、資料やデータの回収又は廃棄の状況を文書に取りまとめ、上位者に報告できることを要求しています。

総合解説：IPAシラバスでは、資料やデータの回収又は廃棄の状況を文書に取りまとめ、上位者に報告できることを要求しています。 終了処理の記録は、未完了事項の把握、監査対応、将来の委託先選定にも利用できる重要な証跡です。

対象：2026年度 / 基準日 2026-09-05