Q001 5-1 情報セキュリティリスク管理 / 資産・脅威・脆弱性の特定

情報セキュリティリスクアセスメントの対象となる「情報資産」の捉え方として最も適切なものはどれか。
ア．データだけでなく、それを処理・保管・伝送するシステム、サービス、端末、媒体、重要な業務プロセスや依存関係も対象として把握する。
イ．購入価格が高いハードウェアだけを情報資産とする。
ウ．社内で所有する機器だけを対象とし、クラウドサービスは除外する。
エ．機密情報だけを対象とし、可用性が重要な公開サービスは除外する。

正答・4肢解説・総合解説

正答：ア．データだけでなく、それを処理・保管・伝送するシステム、サービス、端末、媒体、重要な業務プロセスや依存関係も対象として把握する。
ア：リスクは情報そのものだけでなく、情報を扱う仕組みや業務の依存関係を通じて発生するため、広い視点で資産を把握する。
イ：資産価値は購入価格だけで決まらず、情報やサービスの重要性も含まれる。
ウ：外部サービスでも組織の情報や業務を支えるならリスク評価対象になる。
エ：公開情報でも停止による事業影響が大きければ重要資産になり得る。
総合解説：資産特定では、機密性・完全性・可用性への影響と、業務がどの資産・外部サービスへ依存するかを合わせて確認する。

Q002 5-1 情報セキュリティリスク管理 / 資産・脅威・脆弱性の特定

「脅威」と「脆弱性」の組合せとして最も適切なものはどれか。
ア．脅威は必ず既知CVEを意味し、脆弱性は攻撃者本人を意味する。
イ．脅威は損害を引き起こす可能性のある原因・事象、脆弱性はその脅威に悪用され得る弱点である。
ウ．脅威と脆弱性は常に同じ意味で、区別する必要はない。
エ．脆弱性は損害額そのものを表し、脅威は復旧時間を表す。

正答・4肢解説・総合解説

正答：イ．脅威は損害を引き起こす可能性のある原因・事象、脆弱性はその脅威に悪用され得る弱点である。
ア：CVEは脆弱性識別子であり、攻撃者は脅威源になり得る。
イ：脅威と脆弱性は別概念であり、脅威が脆弱性を利用して資産へ影響を与えるという関係で捉える。
ウ：リスク分析では原因側と弱点側を区別することが重要である。
エ：損害額や復旧時間は影響評価に関する尺度である。
総合解説：例えば「攻撃者による不正アクセス」が脅威事象で、「管理画面が弱いパスワードだけで保護されている」が脆弱性になり得る。

Q003 5-1 情報セキュリティリスク管理 / 資産・脅威・脆弱性の特定

リスクシナリオで「犯罪者集団」と「盗んだ認証情報を使った不正ログイン」を区別する説明として最も適切なものはどれか。
ア．犯罪者集団は脆弱性、不正ログインは資産である。
イ．犯罪者集団は影響、不正ログインは管理策である。
ウ．犯罪者集団は脅威源、盗んだ認証情報を使った不正ログインは脅威事象として整理できる。
エ．両方とも残留リスクだけを表す。

正答・4肢解説・総合解説

正答：ウ．犯罪者集団は脅威源、盗んだ認証情報を使った不正ログインは脅威事象として整理できる。
ア：攻撃者は脅威源であり、不正ログインは資産ではない。
イ：影響は損失の結果、管理策はリスクを修正する対策である。
ウ：誰・何が原因となるかという脅威源と、実際に起こり得る行為・出来事である脅威事象を分けると分析が具体化する。
エ：残留リスクは対策後にも残るリスクであり、脅威源・事象とは異なる。
総合解説：脅威源、脅威事象、脆弱性、影響を分解して記録すると、対策すべき箇所と根拠が明確になる。

Q004 5-1 情報セキュリティリスク管理 / 資産・脅威・脆弱性の特定

情報資産の「資産所有者」に期待される役割として最も適切なものはどれか。
ア．資産に関する全ての技術作業を一人で実施しなければならない。
イ．資産がクラウドに移行した時点で責任を全てクラウド事業者へ移す。
ウ．資産価値を購入価格だけで決める。
エ．資産の業務上の重要性や取扱要件を明確にし、適切な保護・利用・見直しに責任を持つ。

正答・4肢解説・総合解説

正答：エ．資産の業務上の重要性や取扱要件を明確にし、適切な保護・利用・見直しに責任を持つ。
ア：責任を持つことと、全作業を本人だけで実施することは別である。
イ：外部委託後も組織側にリスク管理責任や確認事項が残る。
ウ：業務影響、法的要件、情報の機微性なども考慮する。
エ：資産所有者は必ずしも機器の物理的所有者ではなく、業務上の価値や保護要件を判断する責任主体として扱う。
総合解説：資産台帳には名称だけでなく、所有者、分類、利用目的、保管場所、依存関係などを関連付けるとリスク評価に使いやすい。

Q005 5-1 情報セキュリティリスク管理 / 資産・脅威・脆弱性の特定

CVSSスコアが高い脆弱性が見つかった。組織のリスク評価として最も適切な対応はどれか。
ア．技術的深刻度を参考にしつつ、対象資産の重要度、実際の露出状況、悪用可能性、既存対策、想定影響も確認する。
イ．CVSSが高ければ、利用していない機能でも必ず全社最優先とする。
ウ．CVSSが低ければ重要サーバでも無条件に放置する。
エ．CVSSをそのまま金額損失として扱う。

正答・4肢解説・総合解説

正答：ア．技術的深刻度を参考にしつつ、対象資産の重要度、実際の露出状況、悪用可能性、既存対策、想定影響も確認する。
ア：一般的な脆弱性深刻度は有用だが、組織固有のリスクは環境・資産価値・露出・既存管理策で変わる。
イ：利用状況や到達可能性を無視すると優先順位を誤ることがある。
ウ：業務文脈や攻撃連鎖によって実リスクが高まる場合がある。
エ：CVSSは損害額を表す尺度ではない。
総合解説：脆弱性情報はリスク評価の入力であり、最終的な対応優先度は組織の利用環境や影響と結び付けて決める。

Q006 5-1 情報セキュリティリスク管理 / 資産・脅威・脆弱性の特定

二つのサーバA・Bは同じ機種である。Aは停止しても代替可能だが、Bは決済処理を担い1時間停止すると重大な売上損失が生じる。資産評価として最も適切なものはどれか。
ア．同機種なのでAとBの重要度は必ず同じにする。
イ．機器価格が同じでも、業務影響を踏まえてBの可用性に関する重要度を高く評価する。
ウ．Bは公開サービスでないため重要度をゼロにする。
エ．Bの重要度はCPU使用率だけで決める。

正答・4肢解説・総合解説

正答：イ．機器価格が同じでも、業務影響を踏まえてBの可用性に関する重要度を高く評価する。
ア：同じ技術資産でも利用目的と業務影響が異なれば重要度は変わる。
イ：情報資産の価値は取得価格だけでなく、停止・改ざん・漏えいが事業へ与える影響で評価する必要がある。
ウ：非公開でも業務停止の影響が大きければ重要である。
エ：性能指標だけでは事業上の影響を表せない。
総合解説：資産重要度はCIAそれぞれの観点で評価すると、必要な管理策や復旧優先度へつなげやすい。

Q007 5-1 情報セキュリティリスク管理 / 資産・脅威・脆弱性の特定

自社サービスの認証を外部IdPへ全面依存している。資産・依存関係の特定として最も適切なものはどれか。
ア．自社資産ではないのでリスク評価から完全に除外する。
イ．契約済みであれば停止や侵害は発生しないものとして扱う。
ウ．IdPを重要な外部依存サービスとして台帳・構成図に含め、停止や侵害が自社サービスへ与える影響を評価する。
エ．IdPの存在を利用部門に知らせず、台帳にも記載しない。

正答・4肢解説・総合解説

正答：ウ．IdPを重要な外部依存サービスとして台帳・構成図に含め、停止や侵害が自社サービスへ与える影響を評価する。
ア：外部依存の障害や侵害は自社業務へ直接影響し得る。
イ：契約はリスクをゼロにするものではない。
ウ：自社が所有していなくても、業務継続や認証に不可欠な外部サービスは重要な依存関係である。
エ：依存関係が不明だと障害時の影響評価や代替策の検討が難しい。
総合解説：クラウド・SaaS・外部認証などの依存関係を可視化し、障害・侵害・契約終了など複数のシナリオを評価する。

Q008 5-1 情報セキュリティリスク管理 / 資産・脅威・脆弱性の特定

営業部門が会社未承認のファイル共有SaaSへ顧客資料を保存していることが分かった。最初のリスク管理として最も適切なものはどれか。
ア．存在を記録せず、利用者だけを口頭注意して終える。
イ．未承認SaaSは必ず安全なので、そのまま利用を拡大する。
ウ．顧客資料を公開リンクへ変更して管理を容易にする。
エ．利用実態、保存データ、共有範囲、認証・ログ・契約条件を把握し、資産台帳とリスク評価へ反映する。

正答・4肢解説・総合解説

正答：エ．利用実態、保存データ、共有範囲、認証・ログ・契約条件を把握し、資産台帳とリスク評価へ反映する。
ア：データ移行や再発防止、影響範囲の把握ができない。
イ：安全性や契約条件を評価していない。
ウ：機密性をさらに損なう可能性がある。
エ：未承認利用を見つけたら、実態把握と影響評価を行い、禁止・移行・正式承認などの対応を決める必要がある。
総合解説：シャドーITは「見えていない資産・データフロー」を生み、アクセス制御や退職者対応、ログ管理などの統制を弱める。

Q009 5-1 情報セキュリティリスク管理 / 資産・脅威・脆弱性の特定

顧客データが「社内DB→ETL→分析SaaS→委託先レポート」という経路で処理される。リスク特定を改善する方法として最も適切なものはどれか。
ア．各処理点と境界で、データの種類、保存場所、転送経路、権限、委託先、暗号化、ログ、保持・削除を可視化して評価する。
イ．最終出力のレポートだけを資産として扱い、中間処理を無視する。
ウ．社内DBが暗号化されていれば、外部SaaS以降の評価は不要とする。
エ．委託先が関与した時点で自社のデータフロー管理を終了する。

正答・4肢解説・総合解説

正答：ア．各処理点と境界で、データの種類、保存場所、転送経路、権限、委託先、暗号化、ログ、保持・削除を可視化して評価する。
ア：データの所在だけでなく移動と処理の流れを追うことで、境界をまたぐ漏えい・改ざん・誤送信・保管超過などを特定しやすい。
イ：中間処理や転送経路にも重要なリスクが存在する。
ウ：暗号化は一つの管理策であり、外部処理のリスクを消さない。
エ：委託後も自社の情報資産として管理・確認が必要になる。
総合解説：データフロー図は資産・信頼境界・外部依存を結び付け、脅威シナリオを具体化する基礎資料になる。

Q010 5-1 情報セキュリティリスク管理 / 資産・脅威・脆弱性の特定

古いストレージ装置を廃棄する際のリスク特定として最も適切なものはどれか。
ア．電源を切ればデータは自動的に消えるので確認不要である。
イ．装置内に残るデータや暗号鍵、バックアップ、資産台帳上の状態を確認し、媒体特性に応じた消去・破壊と記録を行う。
ウ．資産台帳から先に削除し、現物の処理は追跡しない。
エ．ラベルだけ剥がせばデータ保護は完了する。

正答・4肢解説・総合解説

正答：イ．装置内に残るデータや暗号鍵、バックアップ、資産台帳上の状態を確認し、媒体特性に応じた消去・破壊と記録を行う。
ア：不揮発性媒体では電源断後もデータが残る。
イ：資産のリスク管理は導入・利用中だけでなく、移管・返却・廃棄まで含むライフサイクル全体で行う。
ウ：未処理資産を見失い、漏えいにつながる。
エ：物理ラベルの除去だけでは記録データは消えない。
総合解説：廃棄・返却では、データ残存、媒体処理、第三者への引渡し、証跡を一体で管理する。

Q011 5-1 情報セキュリティリスク管理 / 資産・脅威・脆弱性の特定

リスク登録簿に「クラウドは危険：高」とだけ記載され、担当者ごとに解釈が異なる。改善として最も適切なものはどれか。
ア．「危険」という語を大文字にするだけで十分である。
イ．リスク名を担当者の氏名だけに置き換える。
ウ．対象資産、脅威事象、脆弱性・前提、想定影響、可能性、既存対策、責任者、対応期限を結び付けて記録する。
エ．評価根拠を残さず、毎回その場の印象で高・中・低を付ける。

正答・4肢解説・総合解説

正答：ウ．対象資産、脅威事象、脆弱性・前提、想定影響、可能性、既存対策、責任者、対応期限を結び付けて記録する。
ア：表現を強調しても評価根拠や対応内容は明確にならない。
イ：誰が担当するかだけではリスク内容を表せない。
ウ：リスク記述を具体的なシナリオにし、評価根拠と対応責任を追跡可能にすることで、再評価や監査に耐えやすくなる。
エ：一貫性や再現性がなく、比較・見直しが難しい。
総合解説：良いリスク登録簿は「何が・どの条件で・どう影響するか」と「誰が・いつまでに・どう扱うか」を追跡できる。

Q012 5-1 情報セキュリティリスク管理 / 資産・脅威・脆弱性の特定

インターネット公開された管理画面で初期パスワードが残り、顧客DBの管理権限を取得できる。最も適切なリスク記述はどれか。
ア．「パスワードがあるので安全」という記述。
イ．「管理画面の色が見づらい」という記述だけ。
ウ．「顧客DBは重要」という記述だけ。
エ．外部攻撃者が初期パスワードを悪用して管理画面へ侵入し、顧客DBを閲覧・改ざんすることで情報漏えいや業務影響が生じるリスク。

正答・4肢解説・総合解説

正答：エ．外部攻撃者が初期パスワードを悪用して管理画面へ侵入し、顧客DBを閲覧・改ざんすることで情報漏えいや業務影響が生じるリスク。
ア：初期パスワードが残ること自体が弱点になり得る。
イ：セキュリティリスクの主要因と影響を表していない。
ウ：資産重要度だけで、脅威・脆弱性・事象が記述されていない。
エ：資産、脅威源・事象、脆弱性、影響を一つのシナリオとして結び付けると、対策と優先順位を検討しやすい。
総合解説：リスク分析では抽象語だけでなく、攻撃・障害がどの弱点を通じてどの資産へ影響するかを記述する。

Q013 5-1 情報セキュリティリスク管理 / 定量・定性リスク評価

定性的なリスク評価の説明として最も適切なものはどれか。
ア．可能性と影響を「高・中・低」などの尺度で評価し、定義した基準に基づいて優先順位を付ける方法である。
イ．全てのリスクを必ず円単位の期待損失額で表す方法である。
ウ．評価者の直感だけで基準を一切定めない方法である。
エ．脆弱性スキャンの件数だけでリスクを決める方法である。

正答・4肢解説・総合解説

正答：ア．可能性と影響を「高・中・低」などの尺度で評価し、定義した基準に基づいて優先順位を付ける方法である。
ア：定性評価は詳細な金額データが不足していても実施しやすいが、尺度と判定基準を明確にして一貫性を確保する必要がある。
イ：これは定量評価の代表的な考え方に近い。
ウ：定性評価でも尺度・基準・根拠が必要である。
エ：件数だけでは資産価値や影響、可能性を評価できない。
総合解説：定性評価では「高」の意味を具体化し、異なる部門・時期でも比較可能な基準を持つことが重要である。

Q014 5-1 情報セキュリティリスク管理 / 定量・定性リスク評価

ある情報資産の価値を1,000万円、1回の事故で失う割合を30%、事故の年間発生率を0.2回と見積もった。単純なALE（年間期待損失）はいくらか。
ア．300万円（SLE＝1,000万円×30%までを計算した値）
イ．60万円（1,000万円×30%×0.2）
ウ．200万円（1,000万円×0.2だけを計算した値）
エ．30万円（30%をそのまま30万円と誤解した値）

正答・4肢解説・総合解説

正答：イ．60万円（1,000万円×30%×0.2）
ア：300万円は1回当たり期待損失SLEであり、年間発生率0.2を掛ける前の値である。
イ：SLEは1,000万円×30%=300万円、ALEは300万円×0.2=60万円である。
ウ：200万円は資産価値に年間発生率だけを掛け、1回の事故で失う割合を反映していない。
エ：30%は割合であり、それだけで30万円という金額にはならない。
総合解説：ALEのような単純モデルは意思決定の一材料だが、入力値の不確実性や低頻度・巨大損失を過小評価しないよう補足分析が必要である。

Q015 5-1 情報セキュリティリスク管理 / 定量・定性リスク評価

資産価値2,000万円、1回の事故で失う割合25%と見積もる。単純なSLE（1回当たり期待損失額）はいくらか。
ア．50万円（25%を2.5%として扱った値）
イ．1,500万円（残存価値75%を損失額と取り違えた値）
ウ．500万円（2,000万円×25%）
エ．2,000万円（資産価値をそのまま損失額とした値）

正答・4肢解説・総合解説

正答：ウ．500万円（2,000万円×25%）
ア：25%を2.5%と誤って扱うと50万円になるが、与えられた損失割合は25%である。
イ：1,500万円は2,000万円の75%で、事故後に残る価値側を損失額と取り違えた値である。
ウ：SLEは資産価値×1回の事故で失う割合なので、2,000万円×25%=500万円である。
エ：資産価値全額を失う条件ではなく、損失割合25%が与えられているため2,000万円ではない。
総合解説：定量評価は数式自体より、資産価値・損失割合・発生頻度の根拠を説明できることが重要である。

Q016 5-1 情報セキュリティリスク管理 / 定量・定性リスク評価

「新規事業では一定のサイバーリスクを取るが、顧客データ漏えいにつながる残留リスクは定めた水準を超えてはならない」という説明に最も近い考え方はどれか。
ア．リスク選好とは全てのリスクをゼロにする義務である。
イ．リスク許容度は脆弱性の件数だけで決める。
ウ．両者はバックアップの保存期間を表す同じ用語である。
エ．経営として受け入れるリスクの方向性・量を示すリスク選好と、具体的な逸脱限界であるリスク許容度を使い分ける。

正答・4肢解説・総合解説

正答：エ．経営として受け入れるリスクの方向性・量を示すリスク選好と、具体的な逸脱限界であるリスク許容度を使い分ける。
ア：事業活動ではリスクを完全にゼロにできない場合が多い。
イ：許容度は事業目標・影響・法的要件等と関連して定める。
ウ：リスク方針・限界に関する概念であり、保持期間そのものではない。
エ：上位の方針と具体的な限界を結び付けることで、現場の判断を経営のリスク方針に整合させやすい。
総合解説：リスク評価結果は、組織が定めた基準・選好・許容度と比較して、対応やエスカレーションへつなげる。

Q017 5-1 情報セキュリティリスク管理 / 定量・定性リスク評価

新しい脅威で発生頻度の実績データがほとんどない。リスク評価として最も適切なものはどれか。
ア．複数の情報源や専門家判断を用い、前提・推定幅・不確実性を明示した上でシナリオ別に評価する。
イ．根拠がなくても小数点以下5桁まで発生確率を固定する。
ウ．実績がないためリスクはゼロと評価する。
エ．最も悲観的な値だけを必ず事実として採用する。

正答・4肢解説・総合解説

正答：ア．複数の情報源や専門家判断を用い、前提・推定幅・不確実性を明示した上でシナリオ別に評価する。
ア：不確実な数値を精密な一点推定のように扱わず、前提と幅を残すことで意思決定者が限界を理解できる。
イ：見かけ上の精密さが不確実性を隠す。
ウ：未観測は発生不能を意味しない。
エ：保守的評価はあり得るが、前提や幅を示さず事実扱いするのは不適切である。
総合解説：リスク評価では不確実性そのものを情報として扱い、追加情報の取得や感度分析の必要性を判断する。

Q018 5-1 情報セキュリティリスク管理 / 定量・定性リスク評価

固有リスク（inherent risk）と残留リスク（residual risk）を比較する説明として最も適切なものはどれか。
ア．固有リスクは保険で補償された額、残留リスクは保険料である。
イ．固有リスクは対象の管理策を考慮する前のリスク、残留リスクは管理策を適用した後にも残るリスクとして整理する。
ウ．残留リスクは必ずゼロでなければならない。
エ．固有リスクは過去の事故、残留リスクは将来の事故だけを意味する。

正答・4肢解説・総合解説

正答：イ．固有リスクは対象の管理策を考慮する前のリスク、残留リスクは管理策を適用した後にも残るリスクとして整理する。
ア：保険の金額概念ではない。
イ：両者を比較すると、管理策がどの程度リスクを低減したか、なお追加対応や受容が必要かを評価できる。
ウ：実務では対策後にも一定のリスクが残ることがある。
エ：時間軸による区別ではない。
総合解説：管理策導入後は「導入したから安全」とせず、残留リスクを再評価して受容基準と比較する。

Q019 5-1 情報セキュリティリスク管理 / 定量・定性リスク評価

複数の重要システムが同一クラウドリージョン、同一IdP、同一管理者アカウントへ依存している。リスク評価で特に確認すべきことはどれか。
ア．各システムの画面色が同じかだけを確認する。
イ．システム数が多いほど自動的にリスクが分散するものとみなす。
ウ．一つの障害や侵害が複数システムへ同時波及する集中・共通原因リスク。
エ．クラウドを使う限り可用性リスクは存在しないとみなす。

正答・4肢解説・総合解説

正答：ウ．一つの障害や侵害が複数システムへ同時波及する集中・共通原因リスク。
ア：共通原因リスクとは無関係である。
イ：依存先が共通なら、むしろ集中リスクが高まる場合がある。
ウ：個別システムごとの評価だけでは、共通依存による同時障害や横断侵害を過小評価することがある。
エ：クラウドにも障害・設定ミス・資格情報侵害等のリスクがある。
総合解説：リスク集約では、単純な個別リスクの足し算だけでなく、相関・集中・連鎖を確認する。

Q020 5-1 情報セキュリティリスク管理 / 定量・定性リスク評価

年平均の期待損失は小さいが、発生すれば会社存続に影響する極端なサイバー事故がある。評価として最も適切なものはどれか。
ア．期待損失が小さければ影響の上限を無視して必ず受容する。
イ．最大影響だけを見て発生可能性は一切考えない。
ウ．過去に起きていないので将来も発生しないとする。
エ．期待値だけでなく最大想定影響、事業継続、法的・信用上の影響、リスク許容度も合わせて評価する。

正答・4肢解説・総合解説

正答：エ．期待値だけでなく最大想定影響、事業継続、法的・信用上の影響、リスク許容度も合わせて評価する。
ア：極端損失が組織の許容範囲を超える可能性を見落とす。
イ：リスクは影響と可能性を含めて評価する必要がある。
ウ：過去未発生は将来の不発生を保証しない。
エ：低頻度・高影響のリスクは平均値だけでは重要性を表しにくく、尾部リスクや耐性の観点が必要である。
総合解説：定量指標は意思決定を支える道具であり、単一指標で全てを表現できるとは限らない。

Q021 5-1 情報セキュリティリスク管理 / 定量・定性リスク評価

ある脆弱性の悪用可能性を評価する。最も妥当な進め方はどれか。
ア．攻撃コードの公開状況、インターネット露出、攻撃者能力、認証要否、既存防御、実際の観測情報などを組み合わせて評価する。
イ．脆弱性名の文字数だけで発生確率を決める。
ウ．ベンダが重大と呼んだら必ず100%悪用されるとする。
エ．攻撃コードが未公開なら可能性を必ずゼロにする。

正答・4肢解説・総合解説

正答：ア．攻撃コードの公開状況、インターネット露出、攻撃者能力、認証要否、既存防御、実際の観測情報などを組み合わせて評価する。
ア：可能性は一つの指標だけでなく、脅威源の能力・意図、脆弱性の悪用条件、環境の露出等から判断する。
イ：リスクの根拠にならない。
ウ：重大度と実環境での発生可能性は同一ではない。
エ：非公開の攻撃手法や将来の公開、他の悪用経路もあり得る。
総合解説：評価根拠を記録すると、脅威状況や構成が変わった際に再評価しやすくなる。

Q022 5-1 情報セキュリティリスク管理 / 定量・定性リスク評価

二つのリスクがどちらもリスクマトリクスで「高」になった。次の優先順位付けとして最も適切なものはどれか。
ア．同じ「高」なら必ず同時刻に同じ対策を行う。
イ．影響対象、法的・契約上の義務、対策期限、攻撃の切迫性、復旧困難性など追加の判断材料で比較する。
ウ．登録順が早い方だけを永遠に優先する。
エ．同じランクになった時点で評価を中止し、対応者を決めない。

正答・4肢解説・総合解説

正答：イ．影響対象、法的・契約上の義務、対策期限、攻撃の切迫性、復旧困難性など追加の判断材料で比較する。
ア：資源制約や期限、影響の性質を考慮できない。
イ：粗い定性ランクが同じでも、経営上の優先度まで同一とは限らないため、補助基準で順位を細分化する。
ウ：登録順はリスク重要度の根拠ではない。
エ：実務上の意思決定につながらない。
総合解説：リスクマトリクスは簡便だが粒度に限界がある。タイブレーク基準や経営判断を明示して運用する。

Q023 5-1 情報セキュリティリスク管理 / リスク対応・残留リスク・サイバー保険

情報セキュリティリスクへの代表的な対応の説明として最も適切なものはどれか。
ア．全てのリスクは必ず受容し、管理策を導入してはならない。
イ．全てのリスクは事業を停止して回避しなければならない。
ウ．回避、低減、移転・共有、受容などから、組織の基準や費用対効果に応じて選択する。
エ．保険に加入すればリスクは完全に消滅する。

正答・4肢解説・総合解説

正答：ウ．回避、低減、移転・共有、受容などから、組織の基準や費用対効果に応じて選択する。
ア：リスク水準に応じて対応を選択する必要がある。
イ：過剰対応となり、事業目的と整合しない。
ウ：リスク対応は一律に「対策を追加する」だけではなく、事業や契約も含めた複数の選択肢から決める。
エ：保険は財務影響の一部を移転し得るが、事故発生や非財務影響は残る。
総合解説：対応後は残留リスクを再評価し、受容基準を超える場合は追加対応や経営判断へエスカレーションする。

Q024 5-1 情報セキュリティリスク管理 / リスク対応・残留リスク・サイバー保険

MFAを導入してアカウント乗っ取りリスクを低減した。次に行うべきリスク管理として最も適切なものはどれか。
ア．MFAを導入した時点でリスクをゼロとして登録簿から削除する。
イ．リスク評価を二度と見直さない。
ウ．MFA導入によりログ取得は不要になる。
エ．MFA回避手法や復旧手続、端末侵害などを含めて残留リスクを再評価し、受容可能か判断する。

正答・4肢解説・総合解説

正答：エ．MFA回避手法や復旧手続、端末侵害などを含めて残留リスクを再評価し、受容可能か判断する。
ア：MFAでもフィッシングやセッション窃取などのリスクが残り得る。
イ：脅威やシステム変更でリスクは変化する。
ウ：認証後の異常検知や調査にはログが引き続き重要である。
エ：管理策には限界があり、導入後にも残るシナリオを確認する必要がある。
総合解説：残留リスクの受容は、対策の存在ではなく対策後の実際のリスク水準と基準の比較で判断する。

Q025 5-1 情報セキュリティリスク管理 / リスク対応・残留リスク・サイバー保険

重要顧客データに関する残留リスクが許容基準に近い。受容手続として最も適切なものはどれか。
ア．権限を持つリスクオーナーが、評価根拠・残留影響・代替策・期限を確認して明示的に承認する。
イ．最初に気付いた担当者が口頭で「問題なし」と言えば完了する。
ウ．受容したリスクは将来の見直し対象から永久に除外する。
エ．受容理由を記録しない方が監査上望ましい。

正答・4肢解説・総合解説

正答：ア．権限を持つリスクオーナーが、評価根拠・残留影響・代替策・期限を確認して明示的に承認する。
ア：リスク受容は担当者の黙認ではなく、権限ある責任者による情報に基づく意思決定として残す。
イ：権限・根拠・証跡が不十分である。
ウ：状況変化に応じて再評価が必要である。
エ：後から判断根拠を検証できなくなる。
総合解説：受容には所有者、承認権限、期限、再評価条件を設定し、リスクの放置と区別する。

Q026 5-1 情報セキュリティリスク管理 / リスク対応・残留リスク・サイバー保険

サイバー保険をリスク管理に用いる際の説明として最も適切なものはどれか。
ア．加入すればパッチ適用やバックアップは不要になる。
イ．事故時の賠償責任や対応費用、事業中断損失など契約で定めた財務影響の一部を移転する手段であり、予防対策の代替ではない。
ウ．保険契約は全てのサイバー事故を無制限に補償する。
エ．保険は脆弱性を自動的に修正する技術である。

正答・4肢解説・総合解説

正答：イ．事故時の賠償責任や対応費用、事業中断損失など契約で定めた財務影響の一部を移転する手段であり、予防対策の代替ではない。
ア：技術・運用対策は引き続き必要である。
イ：サイバー保険はリスクファイナンスの手段であり、事故そのものや信用低下など全ての影響を消すものではない。
ウ：補償範囲、限度額、免責等は契約条件に依存する。
エ：保険は財務的なリスク移転手段であり、技術管理策ではない。
総合解説：保険を検討する際は、自社の損失シナリオと補償範囲・限度額・免責・必要なセキュリティ条件を照合する。

Q027 5-1 情報セキュリティリスク管理 / リスク対応・残留リスク・サイバー保険

サイバー保険への加入を検討している。最も適切な評価方法はどれか。
ア．保険料が安ければ補償内容は確認しなくてよい。
イ．契約書を読まず、広告の見出しだけで全損失が補償されると判断する。
ウ．想定事故ごとの損失を整理し、補償対象、支払限度額、自己負担、免責、通知条件などを確認して残留する財務リスクを評価する。
エ．自己負担額や限度額はリスク計算に影響しない。

正答・4肢解説・総合解説

正答：ウ．想定事故ごとの損失を整理し、補償対象、支払限度額、自己負担、免責、通知条件などを確認して残留する財務リスクを評価する。
ア：安さだけでは必要な損失が補償されるか判断できない。
イ：実際の補償は契約条件に従う。
ウ：「加入しているか」だけではなく、どの損失がどこまで補償されるかを具体的に確認する必要がある。
エ：組織が負担する残留損失を左右する。
総合解説：サイバー保険は財務的リスクの一部を移転するため、契約条件をリスクシナリオへ対応付けて評価する。

Q028 5-1 情報セキュリティリスク管理 / リスク対応・残留リスク・サイバー保険

個人情報漏えいに伴う費用の一部が保険で補償される見込みである。リスク受容判断として最も適切なものはどれか。
ア．保険で一部費用が出れば、漏えいの影響はゼロとみなす。
イ．保険会社があるため、組織はインシデント対応を実施しなくてよい。
ウ．保険加入後はリスク登録簿を削除する。
エ．補償対象外の信用低下、顧客離反、業務停止、法令・契約上の責任なども含め、総合的な残留リスクを評価する。

正答・4肢解説・総合解説

正答：エ．補償対象外の信用低下、顧客離反、業務停止、法令・契約上の責任なども含め、総合的な残留リスクを評価する。
ア：信用・業務・法的影響などが残り得る。
イ：組織自身の対応・報告・復旧責任がなくなるわけではない。
ウ：リスクは引き続き管理・見直し対象である。
エ：財務補償だけでは組織に生じる全ての影響を移転できないため、非財務的影響も受容判断に含める。
総合解説：リスク移転は「リスクの消滅」ではない。移転できない影響と自己負担部分を明確にする。

Q029 5-1 情報セキュリティリスク管理 / リスク対応・残留リスク・サイバー保険

「脆弱性を改善する」とだけ書かれたリスク対応計画を実行可能にするため、追加すべき情報として最も適切なものはどれか。
ア．具体的な対策、責任者、期限、必要資源、完了条件、残留リスク評価、進捗確認方法。
イ．担当者名だけを書き、何をするかは記録しない。
ウ．期限を設定せず、いつか対応することだけ決める。
エ．対策実施後は効果確認を行わない。

正答・4肢解説・総合解説

正答：ア．具体的な対策、責任者、期限、必要資源、完了条件、残留リスク評価、進捗確認方法。
ア：対応計画は実行・追跡・完了判定ができる粒度で記述し、対策後のリスク評価まで含める。
イ：実施内容と完了条件が不明で進捗を管理できない。
ウ：高リスク項目が長期放置される可能性がある。
エ：管理策が期待どおりリスクを下げたか判断できない。
総合解説：対応計画をリスク登録簿と連携し、進捗・例外・再評価を継続的に追跡する。

Q030 5-1 情報セキュリティリスク管理 / リスク対応・残留リスク・サイバー保険

対策後も残留リスクが組織の許容度を超えているが、現場予算では追加対策できない。最も適切な対応はどれか。
ア．予算がないので登録簿から削除する。
イ．リスクオーナーや経営層へ根拠と選択肢をエスカレーションし、追加投資、事業変更、移転、例外受容などを正式に判断してもらう。
ウ．担当者が無断で許容度を変更して受容扱いにする。
エ．残留リスクを固有リスクより低く見せるため数値だけ変更する。

正答・4肢解説・総合解説

正答：イ．リスクオーナーや経営層へ根拠と選択肢をエスカレーションし、追加投資、事業変更、移転、例外受容などを正式に判断してもらう。
ア：リスク自体は残っており、可視性を失う。
イ：現場で解消できない重要リスクは、権限と資源を持つ層へ上げて意思決定する。
ウ：組織のリスク基準を現場判断で改変してはならない。
エ：評価の信頼性を損なう。
総合解説：ガバナンスでは、リスクの大きさに応じた意思決定権限とエスカレーション経路を定めておく。

Q031 5-2 ISMS・規程・監査 / ISMS・管理策

複数部門が個別にセキュリティ対策を行っているが、全社としてリスクの優先順位や責任が統一されていない。この組織がISMSを導入する意義として最も適切なものはどれか。
ア．ファイアウォール製品そのものを指す。
イ．情報システム部門だけの障害復旧手順を指す。
ウ．組織が情報セキュリティリスクを体系的に管理し、方針・目標・管理策を運用して継続的に改善する仕組みである。
エ．一度認証を取得すれば、その後の見直しが不要になる制度である。

正答・4肢解説・総合解説

正答：ウ．組織が情報セキュリティリスクを体系的に管理し、方針・目標・管理策を運用して継続的に改善する仕組みである。
ア：ISMSは単一の技術製品ではない。
イ：適用範囲は組織のリスクと定めたISMS範囲に基づき、マネジメント要素を含む。
ウ：ISMSは特定製品の導入ではなく、組織的なマネジメントの仕組みとして情報セキュリティを維持・改善する。
エ：継続的な運用・監視・改善が必要である。
総合解説：ISMSでは、組織の状況、リーダーシップ、計画、支援、運用、評価、改善を通じてリスクを管理する。

Q032 5-2 ISMS・規程・監査 / ISMS・管理策

ISMSの適用範囲を定める際の考え方として最も適切なものはどれか。
ア．認証取得が容易になるよう、重要な外部依存は記載せずに除外する。
イ．組織図の部署名だけを書き、対象システムや拠点は一切確認しない。
ウ．一度定めた適用範囲は組織再編後も変更してはならない。
エ．組織の業務、拠点、システム、外部サービス、インタフェースや依存関係を考慮し、境界と適用対象を明確にする。

正答・4肢解説・総合解説

正答：エ．組織の業務、拠点、システム、外部サービス、インタフェースや依存関係を考慮し、境界と適用対象を明確にする。
ア：依存関係を隠すと実際のリスクを適切に管理できない。
イ：実際の業務・情報・技術境界を把握できない。
ウ：事業や組織の変化に応じて妥当性を見直す必要がある。
エ：範囲の境界だけでなく、範囲外との依存関係を把握しないと重要なリスクが抜け落ちる。
総合解説：適用範囲は、何をISMSで管理するかを定める基礎であり、事業変化やクラウド移行などに応じて再確認する。

Q033 5-2 ISMS・規程・監査 / ISMS・管理策

ISMSを運用する組織が、顧客契約で特定のログ保持要件を求められている。最も適切な対応はどれか。
ア．顧客を利害関係者として要求を把握し、適用される要求として関連する規程・管理策へ反映する。
イ．ISMSは社内規程だけを扱うので顧客契約は無視する。
ウ．契約要件と社内ルールが異なれば、常に弱い方を採用する。
エ．要求の存在を担当者だけが知っていれば文書化は不要である。

正答・4肢解説・総合解説

正答：ア．顧客を利害関係者として要求を把握し、適用される要求として関連する規程・管理策へ反映する。
ア：ISMSでは法令だけでなく、契約や顧客などの関連要求も把握し、管理の前提にする。
イ：契約上の要求も情報セキュリティ管理に影響し得る。
ウ：適用される要求を満たす必要があり、弱い基準へ下げる根拠にはならない。
エ：組織として一貫して実施・評価できる形にする必要がある。
総合解説：利害関係者の要求を把握し、法令・契約・事業上の要件とISMSの管理策を対応付ける。

Q034 5-2 ISMS・規程・監査 / ISMS・管理策

ISMSにおけるトップマネジメントの役割として最も適切なものはどれか。
ア．脆弱性スキャンの全コマンドを経営者自身が実行する。
イ．情報セキュリティ方針や目標を事業の方向性と整合させ、必要な資源・役割を確保し、ISMSの有効性に責任を持つ。
ウ．セキュリティ目標を事業目標と無関係に設定する。
エ．資源不足があっても経営は関与せず現場に任せる。

正答・4肢解説・総合解説

正答：イ．情報セキュリティ方針や目標を事業の方向性と整合させ、必要な資源・役割を確保し、ISMSの有効性に責任を持つ。
ア：経営責任と個別技術作業の実施者は同一である必要はない。
イ：情報セキュリティをIT部門だけへ丸投げせず、経営上のリスク管理として方向付けと支援を行う。
ウ：ISMSは組織の事業・リスクと整合させる必要がある。
エ：必要な資源・優先順位の意思決定は経営の重要な役割である。
総合解説：トップマネジメントの関与は、リスク受容、資源配分、役割明確化、継続改善を実効的にする。

Q035 5-2 ISMS・規程・監査 / ISMS・管理策

各部門が異なる尺度でリスクを評価し、同じ事象でも「高」「低」がばらばらになっている。改善策として最も適切なものはどれか。
ア．各担当者の感覚を尊重し、尺度は一切定義しない。
イ．全てのリスクを同じ「中」に固定する。
ウ．可能性・影響・受容可否の基準を組織として定義し、評価者が同じ考え方で適用できるようにする。
エ．評価結果だけ保存し、評価基準や根拠は削除する。

正答・4肢解説・総合解説

正答：ウ．可能性・影響・受容可否の基準を組織として定義し、評価者が同じ考え方で適用できるようにする。
ア：評価結果の一貫性や説明可能性が低くなる。
イ：優先順位付けができなくなる。
ウ：リスク評価方法と基準を定めることで、部門間や時系列で結果を比較しやすくなる。
エ：再現性・監査可能性が失われる。
総合解説：リスク基準は固定不変ではなく、組織の状況やリスク選好の変化に応じて見直す。

Q036 5-2 ISMS・規程・監査 / ISMS・管理策

ISMSにおける適用宣言書（Statement of Applicability）の役割として最も適切なものはどれか。
ア．全ての管理策を理由なく同じ強度で実装した証明書である。
イ．監査員の個人履歴書をまとめる文書である。
ウ．リスク評価を実施しなくても管理策を自動選択する一覧である。
エ．必要と判断した管理策と、その採用・除外の理由や実施状況を整理し、リスク対応との関係を示す。

正答・4肢解説・総合解説

正答：エ．必要と判断した管理策と、その採用・除外の理由や実施状況を整理し、リスク対応との関係を示す。
ア：管理策は組織のリスクや要求に基づき選定され、適用の理由を明確にする。
イ：適用宣言書は管理策の適用性に関する文書である。
ウ：管理策選定はリスク対応や要求事項と整合させる必要がある。
エ：適用宣言書は管理策選択の結果を可視化し、なぜその管理策を採用・除外したかを追跡できるようにする。
総合解説：適用宣言書を形だけのチェックリストにせず、リスク評価・対応計画・実際の運用状況と整合させることが重要である。

Q037 5-2 ISMS・規程・監査 / ISMS・管理策

ISMSの管理策を選ぶ考え方として最も適切なものはどれか。
ア．リスク評価、法令・契約要求、業務要件を踏まえ、必要な管理策を選定し、十分性を確認する。
イ．他社が導入している管理策だけを理由なく全てコピーする。
ウ．コストがゼロの管理策だけを選ぶ。
エ．技術的管理策だけを選び、人的・組織的対策は除外する。

正答・4肢解説・総合解説

正答：ア．リスク評価、法令・契約要求、業務要件を踏まえ、必要な管理策を選定し、十分性を確認する。
ア：管理策は一覧から機械的に選ぶのではなく、組織が管理すべきリスクと要求に対応させる。
イ：自組織のリスク・事業・要求との適合性を確認できない。
ウ：重要リスクに必要な対策を外す可能性がある。
エ：リスクは技術だけでなく人・プロセス・物理面にも関係する。
総合解説：同じ管理策でも対象範囲や実装方法は組織によって異なるため、リスク低減効果を確認する。

Q038 5-2 ISMS・規程・監査 / ISMS・管理策

2026年9月5日時点で、日本のISMS要求事項に関するJIS Q 27001の扱いとして適切なものはどれか。
ア．JIS Q 27001:2014だけが現行で、2023年以降の改正はない。
イ．JIS Q 27001:2023に2025年の追補1が反映され、JIS Q 27001:2025として扱われている。
ウ．JIS Q 27001は2026年時点で廃止され、国内規格は存在しない。
エ．ISO/IEC 27001:2022とは無関係な独自規格である。

正答・4肢解説・総合解説

正答：イ．JIS Q 27001:2023に2025年の追補1が反映され、JIS Q 27001:2025として扱われている。
ア：2023年改正と2025年追補が存在する。
イ：ISMS-ACは2025年5月20日にJIS Q 27001:2025（ISO/IEC 27001:2022+Amd 1:2024対応）の発行を案内している。
ウ：有効なJISとして運用されている。
エ：JIS Q 27001はISO/IEC 27001との対応関係を持つ。
総合解説：規格・法令に関する問題は基準日を明確にし、版の変更を追跡する必要がある。

Q039 5-2 ISMS・規程・監査 / ISMS・管理策

「MFAを導入した」という実施記録はあるが、侵害件数や設定状況を確認していない。管理策評価として最も適切な改善はどれか。
ア．購入したライセンス数だけで有効性を断定する。
イ．一度設定すれば永遠に有効とみなし、変更後も確認しない。
ウ．導入有無だけでなく、適用率、例外、回避可能な経路、検知結果などを測定し、意図したリスク低減が得られているか確認する。
エ．失敗や例外のデータは評価を難しくするので削除する。

正答・4肢解説・総合解説

正答：ウ．導入有無だけでなく、適用率、例外、回避可能な経路、検知結果などを測定し、意図したリスク低減が得られているか確認する。
ア：未適用・設定不備・例外を把握できない。
イ：環境・脅威・設定変更で有効性は変わり得る。
ウ：管理策は「存在すること」と「有効に機能すること」を区別して評価する。
エ：問題点を把握できなくなる。
総合解説：有効性評価には、達成すべき成果、指標、測定方法、責任者、評価時期を明確にするとよい。

Q040 5-2 ISMS・規程・監査 / ISMS・管理策

「セキュリティを高める」という目標をISMSで管理しやすくする改善として最も適切なものはどれか。
ア．「できるだけ頑張る」とだけ追記する。
イ．期限も指標も設けず、達成したかは担当者の印象だけで決める。
ウ．目標は事業方針と無関係に設定する。
エ．対象、達成指標、期限、責任者、必要資源、評価方法を具体化し、進捗と結果を確認できるようにする。

正答・4肢解説・総合解説

正答：エ．対象、達成指標、期限、責任者、必要資源、評価方法を具体化し、進捗と結果を確認できるようにする。
ア：達成条件や責任が明確にならない。
イ：客観的評価が難しい。
ウ：ISMS目標は組織の方向性・リスクと整合させることが重要である。
エ：抽象目標だけでは達成判定ができないため、組織の方針・リスクに整合した測定可能な目標へ落とし込む。
総合解説：目標はKPIを増やすこと自体が目的ではなく、リスク低減や管理策有効性を確認できる内容にする。

Q041 5-2 ISMS・規程・監査 / ISMS・管理策

セキュリティ手順書が共有フォルダに複数版存在し、担当者ごとに異なる手順を使っている。最も適切な改善はどれか。
ア．承認済み最新版を識別できる版管理、変更履歴、承認、アクセス制御、旧版の誤使用防止を実施する。
イ．ファイル名を全て「最新版」にして内容は確認しない。
ウ．誰でも承認なしで規程を上書きできるようにする。
エ．旧版を現場に残し続け、どれを使うか利用者に任せる。

正答・4肢解説・総合解説

正答：ア．承認済み最新版を識別できる版管理、変更履歴、承認、アクセス制御、旧版の誤使用防止を実施する。
ア：文書化した情報は作成だけでなく、承認・配布・更新・保存・廃止まで管理する必要がある。
イ：複数の「最新版」が生まれ、版識別できない。
ウ：不適切な変更や責任不明を招く。
エ：誤った手順の実施につながる。
総合解説：文書管理は「証跡のため」だけでなく、現場が正しい要求・手順を利用するための統制でもある。

Q042 5-2 ISMS・規程・監査 / ISMS・管理策

主要システムをオンプレミスからクラウドへ移行する。ISMS上の対応として最も適切なものはどれか。
ア．クラウドは自動的に安全なのでリスク評価を省略する。
イ．資産・依存関係・責任分界・リスク・管理策・規程・監視方法などへの影響を評価し、必要な変更を計画して反映する。
ウ．移行後も旧オンプレミス前提の手順を必ず使い続ける。
エ．変更はIT部門だけの問題なのでISMSの範囲に影響しない。

正答・4肢解説・総合解説

正答：イ．資産・依存関係・責任分界・リスク・管理策・規程・監視方法などへの影響を評価し、必要な変更を計画して反映する。
ア：クラウドにも構成、ID、データ、委託先等のリスクがある。
イ：技術環境の大きな変更はリスク前提を変えるため、既存管理策がそのまま有効とは限らない。
ウ：実環境と手順が乖離する。
エ：業務・契約・監視・役割など組織的な影響がある。
総合解説：変更管理では、計画時点でセキュリティへの影響を評価し、実施後に管理策の有効性も確認する。

Q043 5-2 ISMS・規程・監査 / ISMS・管理策

サイバーリスク評価が情報システム部門内だけで完結し、経営会議の全社リスク一覧と連携していない。改善として最も適切なものはどれか。
ア．技術用語だけで報告し、事業影響は説明しない。
イ．全社リスク管理と重複するのでサイバーリスクを記録しない。
ウ．サイバーリスクを事業目標・財務・法務・レピュテーション等の影響へ結び付け、全社リスク管理の報告・意思決定へ統合する。
エ．IT部門の予算内で解決できないリスクは隠す。

正答・4肢解説・総合解説

正答：ウ．サイバーリスクを事業目標・財務・法務・レピュテーション等の影響へ結び付け、全社リスク管理の報告・意思決定へ統合する。
ア：経営が優先度や投資判断を行いにくい。
イ：重要な事業リスクが可視化されなくなる。
ウ：サイバーリスクはITだけで完結せず、組織の事業リスクとして経営判断の対象にする必要がある。
エ：経営層への適切なエスカレーションを妨げる。
総合解説：NIST CSF 2.0のGOVERNは、サイバーセキュリティを企業リスク管理や経営上の役割・方針と結び付けることを重視する。

Q044 5-2 ISMS・規程・監査 / ISMS・管理策

複数部門が独自の管理策を増やした結果、同じ承認を三重に行う一方、退職者アカウント削除には責任者がいない。最も適切な改善はどれか。
ア．全管理策をさらに一律で二倍にする。
イ．部門間の責任分界を曖昧なままにする。
ウ．管理策一覧を廃止し、個人の記憶だけで運用する。
エ．リスクと管理策の対応を横断的に整理し、重複・欠落・責任分界・例外を確認して統制体系を最適化する。

正答・4肢解説・総合解説

正答：エ．リスクと管理策の対応を横断的に整理し、重複・欠落・責任分界・例外を確認して統制体系を最適化する。
ア：重複を増やしても欠落は解消しない。
イ：誰も実施しない統制が生じやすい。
ウ：一貫性・監査可能性が失われる。
エ：管理策の数を増やすこと自体ではなく、重要リスクへ十分で効率的な統制が配置されていることが重要である。
総合解説：管理策の体系化では、リスク、目的、責任者、証跡、例外、関連統制を結び付けて見直す。

Q045 5-2 ISMS・規程・監査 / セキュリティ方針・諸規程

情報セキュリティ文書の階層の説明として最も適切なものはどれか。
ア．方針で組織の基本姿勢・方向性を示し、規程・基準で具体的な要求を定め、手順で実施方法を示す。
イ．手順が最上位で経営方針を決定し、方針は端末操作だけを記載する。
ウ．方針・規程・手順は全く同じ文書で、区別する意味はない。
エ．規程には要求を書かず、担当者の自由判断だけを記載する。

正答・4肢解説・総合解説

正答：ア．方針で組織の基本姿勢・方向性を示し、規程・基準で具体的な要求を定め、手順で実施方法を示す。
ア：文書ごとの役割を分けると、経営方針を現場の具体的行動へ落とし込みやすい。
イ：一般的な役割関係と逆である。
ウ：抽象度と目的を分けることで管理しやすくなる。
エ：統一的な遵守事項を示せない。
総合解説：名称は組織によって異なっても、上位方針から具体的な基準・手順へ整合する構造が重要である。

Q046 5-2 ISMS・規程・監査 / セキュリティ方針・諸規程

情報セキュリティ基本方針に含める内容として最も適切なものはどれか。
ア．全サーバのIPアドレスと管理者パスワード。
イ．経営としての情報セキュリティへの基本姿勢、目的、責任、遵守・継続改善の方向性。
ウ．特定OSの詳細なレジストリ設定だけ。
エ．毎日のヘルプデスク当番表だけ。

正答・4肢解説・総合解説

正答：イ．経営としての情報セキュリティへの基本姿勢、目的、責任、遵守・継続改善の方向性。
ア：基本方針へ秘密情報を記載するべきではない。
イ：基本方針は組織の方向性を示す上位文書であり、個々の製品設定値だけを並べる文書ではない。
ウ：詳細設定は下位の標準・手順に置く内容である。
エ：情報セキュリティの基本姿勢を示す内容ではない。
総合解説：基本方針を各種規程・標準・手順へ展開し、実際の管理策と一致させる。

Q047 5-2 ISMS・規程・監査 / セキュリティ方針・諸規程

テレワークが常態化したが、規程は「社外への端末持出し禁止」の古い前提のままで、実態と乖離している。最も適切な対応はどれか。
ア．規程を変えず、全員が違反している状態を黙認する。
イ．規程を廃止してテレワークを無条件に自由化する。
ウ．現行の業務実態とリスクを評価し、承認端末、接続方法、データ取扱い、物理的配慮、事故報告などを規程へ反映する。
エ．利用者ごとに口頭ルールを変え、記録しない。

正答・4肢解説・総合解説

正答：ウ．現行の業務実態とリスクを評価し、承認端末、接続方法、データ取扱い、物理的配慮、事故報告などを規程へ反映する。
ア：形骸化し、統制の信頼性を損なう。
イ：必要な管理策や責任がなくなる。
ウ：規程は現実の業務と整合し、守れる具体的な要求になって初めて統制として機能する。
エ：一貫性と説明可能性がない。
総合解説：働き方・技術・法令・脅威の変化は、規程見直しのトリガーになる。

Q048 5-2 ISMS・規程・監査 / セキュリティ方針・諸規程

業務上の理由で一時的に通常のUSB利用禁止規程を例外扱いにする必要がある。最も適切な運用はどれか。
ア．一度例外を認めた利用者は永久に全USBを自由利用できるようにする。
イ．例外は記録せず口頭だけにする。
ウ．代替策は不要で、例外時はリスクを考えない。
エ．業務理由、対象、期間、承認者、代替管理策を記録し、期限到来時に自動的または明示的に見直す。

正答・4肢解説・総合解説

正答：エ．業務理由、対象、期間、承認者、代替管理策を記録し、期限到来時に自動的または明示的に見直す。
ア：例外範囲が必要以上に拡大する。
イ：後で正当性や期限を確認できない。
ウ：例外による追加リスクを評価する必要がある。
エ：例外は無制限な規程無効化ではなく、限定的・期限付き・承認付きで残留リスクを管理する。
総合解説：例外台帳を持ち、期限・理由・補完策・承認権限を管理すると形骸化を防ぎやすい。

Q049 5-2 ISMS・規程・監査 / セキュリティ方針・諸規程

バックアップ規程では「7年保存」、個人データ削除手順では「目的達成後に不要データを速やかに削除」となり、対象データの扱いが衝突している。最も適切な対応はどれか。
ア．法令・契約・業務要件と対象データを確認し、優先関係と例外を整理して規程・手順を整合させる。
イ．担当者ごとに都合のよい方を選ばせる。
ウ．両方の規程をそのまま残し、衝突は存在しないことにする。
エ．保存年数を根拠なく最長の100年に変更する。

正答・4肢解説・総合解説

正答：ア．法令・契約・業務要件と対象データを確認し、優先関係と例外を整理して規程・手順を整合させる。
ア：規程間の矛盾を現場任せにせず、適用要件を確認して一貫したルールへ修正する。
イ：一貫性がなく、過剰保存や不適切削除が起こり得る。
ウ：実務で判断不能な状態が続く。
エ：データ最小化や保管コスト等を無視した過剰対応になり得る。
総合解説：上位方針、法令・契約要求、データ分類、業務目的を基準に、規程間の整合性を定期的に点検する。

Q050 5-2 ISMS・規程・監査 / セキュリティ方針・諸規程

情報セキュリティ規程を社内ポータルに掲載したが、従業員の多くが内容を知らない。最も適切な改善はどれか。
ア．閲覧されていなくても掲載した事実だけで遵守されたとみなす。
イ．対象者に必要な内容を教育・周知し、重要事項は理解確認や同意を行い、質問・改定通知の仕組みも用意する。
ウ．規程を秘密扱いにして従業員には見せない。
エ．違反時だけ初めて規程を知らせる。

正答・4肢解説・総合解説

正答：イ．対象者に必要な内容を教育・周知し、重要事項は理解確認や同意を行い、質問・改定通知の仕組みも用意する。
ア：認知・理解・行動を確認できない。
イ：規程は公開しただけでは実効性がなく、役割に応じて理解・実践できる状態にする必要がある。
ウ：遵守すべき要求を利用者が把握できない。
エ：予防的統制にならない。
総合解説：周知・教育・理解確認・改定通知を一体で運用し、対象者が必要な時に最新版へアクセスできるようにする。

Q051 5-2 ISMS・規程・監査 / セキュリティ方針・諸規程

顧客契約で監査ログを2年間保持することが求められているが、社内標準は1年間である。対象顧客システムの対応として最も適切なものはどれか。
ア．社内標準が1年なので契約要件は自動的に無効になる。
イ．顧客に知らせずログを半年で削除する。
ウ．適用される契約要件を確認し、対象範囲では少なくとも2年間保持できるよう社内ルール・設定を整合させる。
エ．2年保持を全社の全データへ無条件適用し、必要性は確認しない。

正答・4肢解説・総合解説

正答：ウ．適用される契約要件を確認し、対象範囲では少なくとも2年間保持できるよう社内ルール・設定を整合させる。
ア：契約上の義務を社内標準だけで無効化できない。
イ：契約要件を満たさない。
ウ：外部要求が社内標準より厳しい場合、対象範囲で要求を満たす仕組みが必要になる。
エ：対象と要件を整理せず過剰適用するのも適切ではない。
総合解説：法令・契約・規程の要求を対応表で管理すると、設定や監査証跡へ落とし込みやすい。

Q052 5-2 ISMS・規程・監査 / セキュリティ方針・諸規程

「強い暗号を使うこと」という技術標準だけでは担当者ごとに実装が異なる。改善として最も適切なものはどれか。
ア．「最新を使う」とだけ書き、何が最新かは管理しない。
イ．各担当者が好きな方式を選び、レビューしない。
ウ．禁止方式だけを無期限に増やし、移行手順は定めない。
エ．許可するプロトコル・暗号方式・鍵管理、禁止方式、例外手続、見直し条件などを具体的かつ検証可能に定める。

正答・4肢解説・総合解説

正答：エ．許可するプロトコル・暗号方式・鍵管理、禁止方式、例外手続、見直し条件などを具体的かつ検証可能に定める。
ア：時点や対象により解釈が分かれる。
イ：組織として安全水準を統一できない。
ウ：安全な移行を実現できず、現場で例外が常態化しやすい。
エ：技術標準は、実装者が一貫して適用でき、監査・自動チェックで適否を判定できる粒度が望ましい。
総合解説：技術標準は脅威や標準更新に応じて見直し、現行環境へ適用できる形で版管理する。

Q053 5-2 ISMS・規程・監査 / セキュリティ方針・諸規程

「特権操作は事前承認を得て実施する」という規程の遵守状況を監査可能にする仕組みとして最も適切なものはどれか。
ア．承認記録と、誰がいつどの特権操作を行ったかの監査ログを関連付けて保存する。
イ．管理者本人の記憶だけを証拠とする。
ウ．特権操作ログを取得せず、承認記録も削除する。
エ．承認は必要だが、誰が承認したかは記録しない。

正答・4肢解説・総合解説

正答：ア．承認記録と、誰がいつどの特権操作を行ったかの監査ログを関連付けて保存する。
ア：要求に対応する証跡を設計しておくと、実際に承認された操作だけが行われたか検証できる。
イ：客観的・再現可能な証跡になりにくい。
ウ：遵守を確認できない。
エ：権限ある承認か確認できない。
総合解説：規程を作る際は、遵守を示す記録や自動統制が何かまで設計すると実効性が高まる。

Q054 5-2 ISMS・規程・監査 / セキュリティ方針・諸規程

セキュリティ規程の見直し方法として最も適切なものはどれか。
ア．一度承認した規程は廃業まで変更しない。
イ．定期レビューに加え、重大インシデント、法令・契約変更、新技術導入、組織再編など重要な変化をトリガーに見直す。
ウ．毎日全規程を全面改訂する。
エ．インシデントが起きても規程の不備は検討しない。

正答・4肢解説・総合解説

正答：イ．定期レビューに加え、重大インシデント、法令・契約変更、新技術導入、組織再編など重要な変化をトリガーに見直す。
ア：環境・脅威・要求の変化に対応できない。
イ：固定周期だけでは変化への追随が遅れるため、イベント駆動の見直しも組み合わせる。
ウ：必要性に比べて運用負荷が過大で、変更管理も不安定になる。
エ：再発防止の機会を逃す。
総合解説：レビューでは改定要否だけでなく、現場の遵守状況や例外、監査結果も確認する。

Q055 5-2 ISMS・規程・監査 / 監査・是正・継続的改善

ISMS内部監査で、単に「規程どおり作業したか」だけでなく確認すべき観点として最も適切なものはどれか。
ア．売上高だけを確認する会計処理である。
イ．監査対象部門の責任者を処罰することだけが目的である。
ウ．定めた要求事項や組織のルールに適合し、ISMSが有効に実施・維持されているかを客観的に確認する。
エ．監査前に全ての証拠を削除して問題を見えなくする。

正答・4肢解説・総合解説

正答：ウ．定めた要求事項や組織のルールに適合し、ISMSが有効に実施・維持されているかを客観的に確認する。
ア：ISMS内部監査の目的ではない。
イ：不適合の把握と改善が主眼である。
ウ：内部監査は単なる犯人探しではなく、適合性と有効性を確認し、改善のための情報を提供する。
エ：客観的評価ができなくなる。
総合解説：監査結果は是正やマネジメントレビューへ入力し、ISMSの改善につなげる。

Q056 5-2 ISMS・規程・監査 / 監査・是正・継続的改善

内部監査員の割当てとして最も適切なものはどれか。
ア．自分の作業を自分だけで監査し、問題は必ずゼロと報告する。
イ．監査員は証拠を見ず、対象部門の説明だけをそのまま採用する。
ウ．監査結果は経営へ報告せず個人メモにする。
エ．監査の客観性を損なわないよう、可能な範囲で自分が直接設計・運用した統制を自分だけで監査しない体制にする。

正答・4肢解説・総合解説

正答：エ．監査の客観性を損なわないよう、可能な範囲で自分が直接設計・運用した統制を自分だけで監査しない体制にする。
ア：自己レビューだけでは客観性が不足しやすい。
イ：十分な監査証拠を得られない。
ウ：是正・改善の意思決定につながらない。
エ：内部監査でも、利害関係を管理して公平・客観的な評価を行えるようにする。
総合解説：監査員の力量、範囲、頻度、方法、報告経路を計画し、監査の独立性・客観性を確保する。

Q057 5-2 ISMS・規程・監査 / 監査・是正・継続的改善

退職者アカウントが規程どおり退職日に無効化されているか監査したい。最も有効な監査証拠の組合せはどれか。
ア．人事の退職記録、アカウント管理台帳、IdPや対象システムの無効化時刻ログを突合する。
イ．担当者に「いつもできている」と口頭で聞くだけ。
ウ．現役社員のパスワード一覧だけを見る。
エ．画面デザインのスクリーンショットだけを見る。

正答・4肢解説・総合解説

正答：ア．人事の退職記録、アカウント管理台帳、IdPや対象システムの無効化時刻ログを突合する。
ア：異なる独立した記録を突合することで、規程と実際の実施結果の一致を確認できる。
イ：客観的な実施証拠が不足する。
ウ：退職者無効化の事実を確認できない。
エ：アカウント無効化の実施時刻や対象を検証できない。
総合解説：監査証拠は監査目的に関連し、十分かつ信頼できるものを選び、必要に応じてサンプリングする。

Q058 5-2 ISMS・規程・監査 / 監査・是正・継続的改善

監査で「退職者アカウントが残存していた」という不適合が見つかった。是正処置として最も適切なものはどれか。
ア．該当1アカウントだけ削除し、なぜ残ったかは調べない。
イ．残存アカウントを停止するだけでなく、連携漏れの根本原因を分析し、人事イベントからIAMへ確実に反映するプロセスを改善する。
ウ．監査記録を削除して不適合がなかったことにする。
エ．退職者アカウントを全て現役扱いに変更する。

正答・4肢解説・総合解説

正答：イ．残存アカウントを停止するだけでなく、連携漏れの根本原因を分析し、人事イベントからIAMへ確実に反映するプロセスを改善する。
ア：応急的な修正にとどまり、同じ原因で再発し得る。
イ：目の前の不適合を修正する「修正」と、再発原因を除去する「是正処置」を区別する。
ウ：問題を隠してもリスクは残る。
エ：不正アクセスリスクを拡大する。
総合解説：是正処置では、原因、類似問題の有無、対策、責任者、期限、実施後の有効性確認まで追跡する。

Q059 5-2 ISMS・規程・監査 / 監査・是正・継続的改善

フィッシング訓練の問題を受け、追加教育を実施した。是正処置の有効性確認として最も適切なものはどれか。
ア．受講者数だけ確認し、行動変化は一切見ない。
イ．教育資料を作った時点で無条件にクローズする。
ウ．一定期間後に再訓練や関連指標を確認し、報告率・誤操作率などが意図した方向へ改善したか評価する。
エ．悪化していても成功扱いにする。

正答・4肢解説・総合解説

正答：ウ．一定期間後に再訓練や関連指標を確認し、報告率・誤操作率などが意図した方向へ改善したか評価する。
ア：実施量だけでは有効性を判断できない。
イ：対策効果が確認されていない。
ウ：「教育した」という実施記録だけでは、原因が改善されたかは分からない。
エ：評価結果を改善へ反映できない。
総合解説：是正処置は実施後の有効性を確認し、不十分なら追加対策や原因分析を行う。

Q060 5-2 ISMS・規程・監査 / 監査・是正・継続的改善

トップマネジメントがISMSを見直す際に確認すべき情報として最も適切なものはどれか。
ア．ロゴの色だけを毎回評価する。
イ．良い指標だけを選び、問題や未完了の是正は隠す。
ウ．監査・リスク評価・目標の情報は見ない。
エ．監査結果、目標達成状況、インシデントやリスクの変化、是正状況、利害関係者・事業環境の変化など。

正答・4肢解説・総合解説

正答：エ．監査結果、目標達成状況、インシデントやリスクの変化、是正状況、利害関係者・事業環境の変化など。
ア：ISMS有効性の主要情報ではない。
イ：経営判断を誤らせる。
ウ：改善や資源配分の根拠が不足する。
エ：マネジメントレビューではISMSの適切性・十分性・有効性を判断できる情報を総合的に確認する。
総合解説：レビュー結果は、改善、資源、方針・目標、リスク対応などの意思決定へつなげる。

Q061 5-2 ISMS・規程・監査 / 監査・是正・継続的改善

ISMSの継続的改善として最も適切なものはどれか。
ア．監査、インシデント、測定、脅威変化、利用者からのフィードバック等を基に、方針・プロセス・管理策を反復的に改善する。
イ．認証取得後は変更すると監査に不利なので何も改善しない。
ウ．失敗事例は公開せず記録も残さない。
エ．改善項目は優先順位を付けず全て同時に着手する。

正答・4肢解説・総合解説

正答：ア．監査、インシデント、測定、脅威変化、利用者からのフィードバック等を基に、方針・プロセス・管理策を反復的に改善する。
ア：改善は大規模な年1回改訂だけに限らず、運用から得た知見を継続的に反映する活動である。
イ：環境変化に追随できず、ISMSの有効性が低下する。
ウ：組織学習の機会を失う。
エ：資源が分散し、重要課題が進まない可能性がある。
総合解説：継続的改善では、リスクや効果に基づいて改善項目を優先し、実施後の効果まで確認する。

Q062 5-2 ISMS・規程・監査 / 監査・是正・継続的改善

監査で20件の指摘が出た。是正の優先順位付けとして最も適切なものはどれか。
ア．報告書のページ番号が小さい順だけで対応する。
イ．指摘が関連するリスクの重大度、悪用可能性、法令・契約影響、是正期限、代替策の有無などで優先順位を決める。
ウ．全指摘を同じ期限に設定し、重要度は見ない。
エ．技術的指摘だけ対応し、人的・規程上の指摘は無視する。

正答・4肢解説・総合解説

正答：イ．指摘が関連するリスクの重大度、悪用可能性、法令・契約影響、是正期限、代替策の有無などで優先順位を決める。
ア：リスク重要度と無関係である。
イ：件数や報告書の並び順だけでなく、リスクに基づいて限られた資源を配分する。
ウ：重大指摘への迅速な対応が遅れる可能性がある。
エ：組織的なリスクを残す。
総合解説：監査指摘の管理には、所有者、期限、リスク、根本原因、進捗、完了証拠を紐付けるとよい。

Q063 5-3 人的・組織的対策 / 内部不正防止

内部不正を防止する基本的な考え方として最も適切なものはどれか。
ア．監視カメラを1台設置すれば他の対策は不要である。
イ．全従業員へ無制限の管理者権限を与えて信頼を示す。
ウ．権限管理、ログ監視、ルール・教育、職場環境、退職時対応、事後対応など複数の対策を組み合わせる。
エ．内部者は信頼できるためログ取得を停止する。

正答・4肢解説・総合解説

正答：ウ．権限管理、ログ監視、ルール・教育、職場環境、退職時対応、事後対応など複数の対策を組み合わせる。
ア：一つの物理対策だけでは多様な内部不正シナリオを十分に抑止できない。
イ：過剰権限は不正・誤操作の影響を拡大する。
ウ：内部不正は正当な権限や業務知識が悪用される場合があるため、単一の技術対策だけに依存しない多層的な管理が必要である。
エ：内部者による不正や誤操作の検知・調査が困難になる。
総合解説：IPAの内部不正防止ガイドラインは、基本方針、資産管理、物理的・技術的管理、人的管理、職場環境、事後対策などを横断的に扱う。

Q064 5-3 人的・組織的対策 / 内部不正防止

退職予定者が重要情報へアクセスできる環境で、退職時の内部不正対策として最も適切なものはどれか。
ア．退職後も念のため全アカウントを1年間有効にする。
イ．会社貸与端末は本人の記念品として無条件に持ち帰らせる。
ウ．退職手続とアカウント管理を完全に分離し、通知もしない。
エ．業務上必要な範囲を再確認し、退職・異動のタイミングに合わせて権限を縮小・失効し、端末・媒体回収や秘密保持事項の再確認を行う。

正答・4肢解説・総合解説

正答：エ．業務上必要な範囲を再確認し、退職・異動のタイミングに合わせて権限を縮小・失効し、端末・媒体回収や秘密保持事項の再確認を行う。
ア：不要なアクセス経路を残し、悪用リスクを高める。
イ：組織資産やデータが管理外になる。
ウ：失効漏れが生じやすい。
エ：雇用の終了はアクセス権・資産・秘密情報の取扱いが変化する重要イベントであり、手続きを人事・IT・上司で連携させる。
総合解説：退職・契約終了時の権限失効を自動連携やチェックリストで確実にし、情報持出しの兆候も必要に応じ確認する。

Q065 5-3 人的・組織的対策 / 内部不正防止

内部不正対策として従業員の操作ログを監視する場合の運用として最も適切なものはどれか。
ア．監視目的・対象・利用方法を明確にし、必要性と相当性を検討した上で、プライバシーや人権に配慮し適切な権限管理と人による確認を行う。
イ．業務目的に関係なく私生活の全情報を無制限に収集する。
ウ．監視アルゴリズムが警告した従業員は、事実確認なしで必ず不正者と断定する。
エ．監視ログは誰でも閲覧できるよう公開する。

正答・4肢解説・総合解説

正答：ア．監視目的・対象・利用方法を明確にし、必要性と相当性を検討した上で、プライバシーや人権に配慮し適切な権限管理と人による確認を行う。
ア：監視は不正検知に有効だが、無制限・秘密裏の収集や自動判定だけに依存すると別のリスクを生む。
イ：目的を超えた過剰監視となり得る。
ウ：誤検知があり得るため、状況確認や適切な手続が必要である。
エ：監視データ自体に個人情報や機密情報が含まれ得る。
総合解説：IPAは内部不正対策の技術的管理を行う際、目的の明示や個人情報への配慮、機械的判断だけに依存しない運用の重要性を示している。

Q066 5-3 人的・組織的対策 / 内部不正防止

全営業担当者が全顧客の詳細データを閲覧・一括出力できる。内部不正リスクを下げる対策として最も適切なものはどれか。
ア．利便性を優先し、全社員に同じ管理者権限を与える。
イ．担当業務に必要な顧客範囲と操作に権限を限定し、一括出力など高リスク操作は追加承認や監視を適用する。
ウ．アクセスログを停止して従業員の不安をなくす。
エ．顧客データを公開URLで共有し、認証をなくす。

正答・4肢解説・総合解説

正答：イ．担当業務に必要な顧客範囲と操作に権限を限定し、一括出力など高リスク操作は追加承認や監視を適用する。
ア：過剰権限により影響範囲が広がる。
イ：正当な利用者であっても、必要以上の権限を持たせないことで不正・誤操作時の影響を抑える。
ウ：異常な閲覧や持出しを検知・調査できなくなる。
エ：機密性を大きく損なう。
総合解説：最小権限、職務に応じたアクセス制御、高リスク操作の追加統制を組み合わせる。

Q067 5-3 人的・組織的対策 / 内部不正防止

業務上USBメモリの利用が必要な部門がある。内部不正と情報漏えいを抑える運用として最も適切なものはどれか。
ア．私物USBを無記名で自由利用できるようにする。
イ．USBに保存した情報は会社管理外になるのでルール不要とする。
ウ．承認済み媒体に限定し、利用者・目的・期間を管理し、暗号化やマルウェア対策、持出し記録など必要な統制を適用する。
エ．暗号化鍵をUSB本体に平文のテキストで保存する。

正答・4肢解説・総合解説

正答：ウ．承認済み媒体に限定し、利用者・目的・期間を管理し、暗号化やマルウェア対策、持出し記録など必要な統制を適用する。
ア：媒体の追跡性や安全性を確保できない。
イ：会社情報である限り管理責任は残る。
ウ：業務要件がある場合、単純な全面禁止だけでなく、許可範囲と保護要件を明確にして管理する。
エ：紛失時に暗号化の保護効果が失われる。
総合解説：媒体制御は利用禁止・許可だけでなく、承認、記録、暗号化、返却・廃棄まで含めて設計する。

Q068 5-3 人的・組織的対策 / 内部不正防止

内部不正防止において職場環境への配慮が重要な理由として最も適切なものはどれか。
ア．良い職場環境があればアクセス制御は一切不要になる。
イ．不満を持つ従業員は必ず不正を行うと断定できる。
ウ．内部不正は技術的原因だけで発生し、職場環境は無関係である。
エ．不満や孤立、過度な負担などの要因が不正の動機・機会と結び付くことがあるため、相談・コミュニケーションや公正な運用も予防に寄与する。

正答・4肢解説・総合解説

正答：エ．不満や孤立、過度な負担などの要因が不正の動機・機会と結び付くことがあるため、相談・コミュニケーションや公正な運用も予防に寄与する。
ア：人的対策だけで技術的・組織的統制を代替できない。
イ：個人を一律に不正者とみなすのは不適切である。
ウ：IPAガイドラインは職場環境も対策観点として扱う。
エ：内部不正対策はアクセス制御だけでなく、組織文化や職場環境など人的・組織的要因も考慮する。
総合解説：内部不正の抑止では、機会を減らす統制と、早期相談・公正な人事・コミュニケーションなど組織面を組み合わせる。

Q069 5-3 人的・組織的対策 / 内部不正防止

同僚による不審な情報持出しを見た従業員が報告しやすくする仕組みとして最も適切なものはどれか。
ア．報告・相談先と手順を明確にし、秘密保持や不利益取扱い防止に配慮しつつ、受領後の調査・エスカレーション方法を定める。
イ．報告者の氏名を必ず全社公開する。
ウ．通報は受け付けるが、内容は一切記録・調査しない。
エ．疑い段階の情報をSNSへ公開して世論で判断する。

正答・4肢解説・総合解説

正答：ア．報告・相談先と手順を明確にし、秘密保持や不利益取扱い防止に配慮しつつ、受領後の調査・エスカレーション方法を定める。
ア：従業員が懸念を早期に報告でき、組織が適切に扱う仕組みは内部不正の早期発見に役立つ。
イ：報告をためらわせ、報告者保護にも問題がある。
ウ：早期対応につながらない。
エ：機密性、名誉、証拠保全などに問題が生じる。
総合解説：通報制度は、受付、秘密保持、調査、証拠保全、関係者への連携をあらかじめ設計する。

Q070 5-3 人的・組織的対策 / 内部不正防止

重要設計情報の不正持出しを検知したい。監視対象として特に有用な組合せはどれか。
ア．社員食堂のメニューだけを記録する。
イ．重要ファイルへのアクセス、一括ダウンロード、外部媒体・クラウドへの転送、特権操作、認証イベントなどのログ。
ウ．ログ量を減らすためファイルアクセス記録を全て無効化する。
エ．監視対象者自身に監査ログの削除権限を無制限に与える。

正答・4肢解説・総合解説

正答：イ．重要ファイルへのアクセス、一括ダウンロード、外部媒体・クラウドへの転送、特権操作、認証イベントなどのログ。
ア：情報持出しとの関連性が低い。
イ：情報へのアクセスから持出し経路まで複数の証跡を相関すると、不自然な行動を検知しやすい。
ウ：重要情報への異常アクセスを追えなくなる。
エ：不正の隠蔽を可能にする。
総合解説：ログ監視では目的に必要なイベントを選定し、ログ自体の保護やアクセス制御も行う。

Q071 5-3 人的・組織的対策 / 内部不正防止

UEBAが「大量ファイル閲覧」を異常として検知した。内部不正対応として最も適切なものはどれか。
ア．アラートが出た時点で必ず懲戒処分を確定する。
イ．異常検知は誤検知があるため全て無視する。
ウ．本人の職務、業務予定、アクセス対象、端末、時間帯などを確認し、他の証跡と合わせて人が事実関係を評価する。
エ．検知対象の本人に監視ルールを自由に無効化させる。

正答・4肢解説・総合解説

正答：ウ．本人の職務、業務予定、アクセス対象、端末、時間帯などを確認し、他の証跡と合わせて人が事実関係を評価する。
ア：誤検知や正当業務の可能性があり、適切な調査が必要である。
イ：有用な兆候を見逃す。
ウ：行動分析は調査の手掛かりであり、アラートだけで不正を断定せず文脈を確認する。
エ：監視の有効性を損なう。
総合解説：内部不正監視では、個人情報・人権へ配慮しつつ、機械的な判定だけに依存せず適切な調査手続を設ける。

Q072 5-3 人的・組織的対策 / 内部不正防止

社員が経理部から営業部へ異動した後も、旧経理システムの承認権限が残っている。最も適切な対策はどれか。
ア．長く勤務するほど権限が増えるのは当然として放置する。
イ．異動者には新旧両部門の全権限を永久付与する。
ウ．権限台帳を削除して問題を見えなくする。
エ．異動を権限見直しのトリガーとし、新職務に不要な旧権限を速やかに削除する。

正答・4肢解説・総合解説

正答：エ．異動を権限見直しのトリガーとし、新職務に不要な旧権限を速やかに削除する。
ア：権限蓄積により不正・誤操作の影響が大きくなる。
イ：最小権限に反する。
ウ：残存権限の把握がさらに困難になる。
エ：入社・異動・退職などの人事イベントにアクセス権管理を連動させることで、権限の蓄積を防ぐ。
総合解説：定期棚卸しだけでなく、人事イベントを即時の権限変更トリガーにすることが重要である。

Q073 5-3 人的・組織的対策 / 内部不正防止

顧客情報システムで、通常は1件ずつ閲覧する業務なのに全件CSV出力機能が全利用者へ提供されている。最も適切な改善はどれか。
ア．全件出力を必要な役割に限定し、目的に応じて承認、件数制限、透かし・識別情報、ログ・アラートなどを適用する。
イ．全利用者に毎日全件出力させ、異常を通常化する。
ウ．全件出力のログだけを削除する。
エ．CSVをZIP化すればアクセス制御は不要になる。

正答・4肢解説・総合解説

正答：ア．全件出力を必要な役割に限定し、目的に応じて承認、件数制限、透かし・識別情報、ログ・アラートなどを適用する。
ア：高リスク機能は通常業務より強い統制を適用し、持出しの機会と検知不能性を減らす。
イ：不要なコピーが増え、漏えいリスクが高まる。
ウ：不正持出しを調査できなくなる。
エ：圧縮は認可や監視の代替にならない。
総合解説：内部不正対策では、重要情報への大量アクセス・出力を特権的操作として扱い、予防と検知を組み合わせる。

Q074 5-3 人的・組織的対策 / 内部不正防止

内部者による情報持出しが発生した後の対応として最も適切なものはどれか。
ア．関係ログを削除し、事件がなかったことにする。
イ．証拠を保全し、影響範囲と原因を調査し、必要な法務・人事対応を行い、権限・監視・規程・教育などの再発防止策へ反映する。
ウ．本人の処分だけ行い、同じ過剰権限を全員に残す。
エ．全社員を一律に不正者扱いして業務を永久停止する。

正答・4肢解説・総合解説

正答：イ．証拠を保全し、影響範囲と原因を調査し、必要な法務・人事対応を行い、権限・監視・規程・教育などの再発防止策へ反映する。
ア：原因・影響の調査や証拠保全ができない。
イ：事後対応では個別処分だけで終わらせず、なぜ不正が可能だったかを分析して統制改善につなげる。
ウ：構造的な原因が残り再発し得る。
エ：過剰かつ非現実的で、適切なリスク対応ではない。
総合解説：内部不正発生後は、技術・人的・組織的原因を横断的に確認し、再発防止と監視の改善へ反映する。

Q075 5-3 人的・組織的対策 / 教育・訓練・自己点検

情報セキュリティ教育・訓練の目的として最も適切なものはどれか。
ア．年1回動画を再生した記録だけを作れば目的達成である。
イ．教育はIT部門だけに行い、一般利用者には不要である。
ウ．必要な知識・技能を身に付け、日常業務で安全な行動を取れるようにし、組織のリスクを低減する。
エ．教育の目的はインシデントを隠す方法を教えることである。

正答・4肢解説・総合解説

正答：ウ．必要な知識・技能を身に付け、日常業務で安全な行動を取れるようにし、組織のリスクを低減する。
ア：受講記録だけでは理解・行動の定着を確認できない。
イ：一般利用者もフィッシングや情報取扱い等のリスクに関与する。
ウ：受講履歴を作ること自体ではなく、役割に応じた理解と行動変容につなげることが重要である。
エ：報告・予防・適切な対応を促すことが目的である。
総合解説：NIST SP 800-50 Rev.1は教育プログラムをライフサイクルで管理し、セキュリティ文化や行動変容、評価を重視している。

Q076 5-3 人的・組織的対策 / 教育・訓練・自己点検

全社員へ同じ一般教育だけを実施している。改善として最も適切なものはどれか。
ア．管理者も一般社員と同じ内容だけで十分とする。
イ．経営層には技術作業をしないためセキュリティ教育は不要とする。
ウ．教育内容は職務と無関係な雑学だけにする。
エ．全社員向け基礎教育に加え、開発者、管理者、経営層、人事など役割固有のリスクと責任に応じた教育を実施する。

正答・4肢解説・総合解説

正答：エ．全社員向け基礎教育に加え、開発者、管理者、経営層、人事など役割固有のリスクと責任に応じた教育を実施する。
ア：高権限操作や設定管理など役割固有の知識が必要である。
イ：リスク受容・資源配分・ガバナンスの役割がある。
ウ：業務で必要な行動につながらない。
エ：役割ごとに扱う情報・権限・意思決定が異なるため、必要な能力も異なる。
総合解説：役割別教育では、対象者が実際に行う業務・判断・権限に対応した学習目標を設定する。

Q077 5-3 人的・組織的対策 / 教育・訓練・自己点検

模擬フィッシング訓練でリンクをクリックした従業員がいた。最も適切なフォローはどれか。
ア．個人を公開して辱めるのではなく、なぜ見分けにくかったかを分析し、報告方法や確認ポイントを教育して組織全体の改善に生かす。
イ．クリック者の氏名を全社掲示し、恐怖で再発を防ぐ。
ウ．結果を一切分析せず、同じメールを毎日送る。
エ．クリック率を下げるためメール利用を全面禁止する。

正答・4肢解説・総合解説

正答：ア．個人を公開して辱めるのではなく、なぜ見分けにくかったかを分析し、報告方法や確認ポイントを教育して組織全体の改善に生かす。
ア：訓練は罰することより、実際の安全行動と報告習慣を高めることが目的である。
イ：心理的安全性を損ない、今後の報告をためらわせる可能性がある。
ウ：学習目標や改善につながらない。
エ：業務要件と釣り合わない過剰対応である。
総合解説：訓練結果は教材改善、対象者別教育、報告手順、技術対策の見直しへつなげる。

Q078 5-3 人的・組織的対策 / 教育・訓練・自己点検

セキュリティ教育のKPIとして、受講率だけでは不十分な理由はどれか。
ア．受講率は常にセキュリティ事故件数と完全一致するから。
イ．受講完了は実施状況を示すが、理解度や安全な行動、報告能力が改善したかまでは分からないため。
ウ．受講率は測定できない指標だから。
エ．教育では評価を行ってはならないから。

正答・4肢解説・総合解説

正答：イ．受講完了は実施状況を示すが、理解度や安全な行動、報告能力が改善したかまでは分からないため。
ア：そのような一対一の関係はない。
イ：教育プログラムは知識・行動・業務上の成果を複数の指標で評価する方が有効性を判断しやすい。
ウ：受講率は測定できるが、有効性を単独で十分に表さない。
エ：評価は継続改善の重要な入力である。
総合解説：理解度テスト、模擬演習、報告率、役割別パフォーマンスなど、目標に対応した指標を組み合わせる。

Q079 5-3 人的・組織的対策 / 教育・訓練・自己点検

各部門に情報セキュリティ自己点検を依頼する。実効性を高める方法として最も適切なものはどれか。
ア．評価を良く見せるため証拠がなくても全て○にするよう指示する。
イ．質問文を曖昧にし、担当者ごとに自由な意味で回答させる。
ウ．質問ごとに判断基準と確認する証拠例を示し、未実施・不明を正直に報告できるようにして改善計画へつなげる。
エ．未実施項目は報告書から削除する。

正答・4肢解説・総合解説

正答：ウ．質問ごとに判断基準と確認する証拠例を示し、未実施・不明を正直に報告できるようにして改善計画へつなげる。
ア：実態把握ができず、改善機会を失う。
イ：比較可能性と一貫性が低下する。
ウ：自己点検は全項目を「○」にすることが目的ではなく、現状と弱点を把握して改善するために行う。
エ：リスクを隠すことになる。
総合解説：IPAの中小企業向けガイドラインや内部不正ガイドラインには自己点検に使えるチェックの考え方が示されている。

Q080 5-3 人的・組織的対策 / 教育・訓練・自己点検

実インシデントで、従業員が不審メールを報告する連絡先を知らなかったため初動が遅れた。教育改善として最も適切なものはどれか。
ア．教育内容は毎年固定し、インシデント結果は反映しない。
イ．報告先をさらに秘密にする。
ウ．不審メールを見た利用者が独自に攻撃者へ返信するよう教育する。
エ．インシデントの教訓を教育へ反映し、報告先・報告内容・緊急時の行動を実践的な演習で確認する。

正答・4肢解説・総合解説

正答：エ．インシデントの教訓を教育へ反映し、報告先・報告内容・緊急時の行動を実践的な演習で確認する。
ア：同じ弱点が再発する可能性がある。
イ：従業員が迅速に連絡できなくなる。
ウ：被害拡大や証拠汚染につながり得る。
エ：実際に発生した失敗は教育プログラムの有効性を見直す重要な入力である。
総合解説：教育は組織・脅威・技術・インシデントの変化に応じて更新するライフサイクル型の活動である。

Q081 5-3 人的・組織的対策 / 教育・訓練・自己点検

新入社員へ重要システムのアクセス権を付与する際の教育運用として最も適切なものはどれか。
ア．アクセス付与前または利用開始時までに必要なセキュリティルール・報告手順を教育し、役割に応じて追加訓練を行う。
イ．半年間自由利用させてから初めてルールを説明する。
ウ．入社時教育は不要で、違反した人だけに後から説明する。
エ．新入社員には最初から全システムの管理者権限を付与する。

正答・4肢解説・総合解説

正答：ア．アクセス付与前または利用開始時までに必要なセキュリティルール・報告手順を教育し、役割に応じて追加訓練を行う。
ア：必要な知識を持たないまま高リスク資産へアクセスさせる期間を作らないことが重要である。
イ：教育前に不適切な操作が起きる可能性がある。
ウ：予防的な統制にならない。
エ：職務に必要な最小権限の原則に反する。
総合解説：入社・異動などのライフサイクルイベントに、教育とアクセス権付与を連携させる。

Q082 5-3 人的・組織的対策 / 教育・訓練・自己点検

経営層向けサイバーセキュリティ教育として最も適切な内容はどれか。
ア．一般社員と同じパスワード変更手順だけを繰り返す。
イ．主要なサイバーリスク、法令・契約上の責任、リスク受容、資源配分、重大インシデント時の意思決定や報告体制。
ウ．サイバーリスクはIT部門だけのため経営層教育は不要とする。
エ．全ての脆弱性のソースコード修正方法だけを必須とする。

正答・4肢解説・総合解説

正答：イ．主要なサイバーリスク、法令・契約上の責任、リスク受容、資源配分、重大インシデント時の意思決定や報告体制。
ア：経営固有の意思決定責任を十分に扱わない。
イ：経営層には技術詳細だけでなく、ガバナンスと事業継続に関する判断能力が求められる。
ウ：経営判断・資源配分・リスク受容に関与する。
エ：経営層の主要責務と合わない。
総合解説：役割別教育は、対象者が担う意思決定と責任に合わせる。

Q083 5-3 人的・組織的対策 / 教育・訓練・自己点検

自己点検と内部監査の関係として最も適切なものはどれか。
ア．自己点検があれば内部監査は必ず禁止される。
イ．内部監査は日々の自己点検結果を一切参照してはならない。
ウ．自己点検は現場が日常的に自ら確認する手段、内部監査はより独立・客観的な視点で要求への適合性や有効性を確認する手段で、相互補完する。
エ．自己点検は問題を隠すために行う。

正答・4肢解説・総合解説

正答：ウ．自己点検は現場が日常的に自ら確認する手段、内部監査はより独立・客観的な視点で要求への適合性や有効性を確認する手段で、相互補完する。
ア：両者は目的・独立性が異なり併用できる。
イ：監査計画やサンプリングの参考にできる。
ウ：自己点検は頻繁に実施しやすい一方、自己評価バイアスがあるため、独立した監査で補完する価値がある。
エ：現状把握と改善のために行う。
総合解説：複数の保証活動を役割分担し、重複を減らしながら重要リスクの見落としを防ぐ。

Q084 5-3 人的・組織的対策 / 教育・訓練・自己点検

生成AIサービスの業務利用を新たに許可する。教育プログラムの対応として最も適切なものはどれか。
ア．従来教育に生成AIの記載がなくても永遠に変更しない。
イ．利用者に全て自己判断させ、組織ルールは示さない。
ウ．生成AIへ機密情報を入力することを推奨し、データ取扱いは説明しない。
エ．入力してよい情報、承認済みサービス、出力の検証、著作権・機密情報、インシデント報告など組織の利用ルールに沿った教育を追加する。

正答・4肢解説・総合解説

正答：エ．入力してよい情報、承認済みサービス、出力の検証、著作権・機密情報、インシデント報告など組織の利用ルールに沿った教育を追加する。
ア：実際の利用リスクを扱えない。
イ：一貫した情報取扱いができない。
ウ：情報漏えい等のリスクを高める。
エ：新しい技術や業務変更で新たなリスクと行動要件が生じたら、教育内容も更新する。
総合解説：教育プログラムは組織・技術・脅威の変化を反映して継続的に更新する。

Q085 5-3 人的・組織的対策 / 職務分離・最小権限・人的管理

職務分離（separation of duties）の主な目的として最も適切なものはどれか。
ア．重要な処理を一人だけで完結できないよう役割を分け、権限悪用や誤りが単独で重大結果につながるリスクを減らす。
イ．全ての業務を一人の管理者へ集中して効率を最大化する。
ウ．職務分離とは全社員に同じ権限を与えることである。
エ．職務分離はバックアップ媒体を二つ作ることだけを意味する。

正答・4肢解説・総合解説

正答：ア．重要な処理を一人だけで完結できないよう役割を分け、権限悪用や誤りが単独で重大結果につながるリスクを減らす。
ア：申請・承認・実行・監査などを適切に分離することで、不正に共謀が必要になるなど抑止力を高められる。
イ：単独で不正・誤操作を完結できるリスクが高まる。
ウ：役割を分けて権限を区別する考え方と逆である。
エ：可用性対策ではなく権限・職責の分離に関する管理策である。
総合解説：NIST SP 800-53のAC-5は、悪意ある権限利用のリスクを低減するために分離すべき職務を特定し、アクセス権限へ反映する考え方を示す。

Q086 5-3 人的・組織的対策 / 職務分離・最小権限・人的管理

高額送金システムの権限設計として最も適切なものはどれか。
ア．一人の担当者に登録・承認・監査ログ削除の全権限を与える。
イ．送金データ登録者と承認者を分離し、必要に応じて実行・監査も別の役割として権限を制御する。
ウ．全社員が同じ送金管理者アカウントを共有する。
エ．承認機能を廃止し、送金額に関係なく自動実行する。

正答・4肢解説・総合解説

正答：イ．送金データ登録者と承認者を分離し、必要に応じて実行・監査も別の役割として権限を制御する。
ア：不正を単独で実行・隠蔽できる。
イ：重要取引を一人で作成・承認できないようにすることで、不正や誤りを発見・抑止しやすくなる。
ウ：個人識別と責任追跡ができない。
エ：高額取引への統制が弱くなる。
総合解説：職務分離は業務プロセスとシステム権限の両方へ反映し、共有アカウントなどで実質的に迂回されないようにする。

Q087 5-3 人的・組織的対策 / 職務分離・最小権限・人的管理

最小権限の原則として最も適切なものはどれか。
ア．在籍期間が長いほど自動的に全管理者権限を付与する。
イ．一度付与した権限は異動後も削除しない。
ウ．利用者・プロセスには、担当業務を遂行するために必要な最小限の権限だけを与える。
エ．最小権限とはパスワードを短くすることである。

正答・4肢解説・総合解説

正答：ウ．利用者・プロセスには、担当業務を遂行するために必要な最小限の権限だけを与える。
ア：職務上の必要性と無関係な権限付与である。
イ：権限が蓄積して最小権限から逸脱する。
ウ：不要な権限を減らすことで、アカウント侵害、内部不正、誤操作時の影響範囲を小さくできる。
エ：アクセス権限の範囲に関する原則であり、パスワード長とは別である。
総合解説：最小権限は初回付与だけでなく、異動・退職・業務変更・定期棚卸しで継続的に維持する。

Q088 5-3 人的・組織的対策 / 職務分離・最小権限・人的管理

外部ベンダの保守担当者に本番管理者権限が月1回、2時間だけ必要である。最も適切な権限管理はどれか。
ア．1年間有効な共有rootパスワードをメールで送る。
イ．作業終了後も次回のため権限を残す。
ウ．作業ログを取得しない。
エ．作業申請・承認後に必要時間だけ特権を付与し、終了時に失効させ、操作ログを記録・確認する。

正答・4肢解説・総合解説

正答：エ．作業申請・承認後に必要時間だけ特権を付与し、終了時に失効させ、操作ログを記録・確認する。
ア：常設・共有・平文送信の特権資格情報はリスクが高い。
イ：不要な期間の特権が残る。
ウ：問題発生時の追跡や責任確認ができない。
エ：常設特権を避け、JIT的な時間限定アクセスと監査証跡を組み合わせると、不要な攻撃面を減らせる。
総合解説：特権アクセスは、本人識別、承認、最小権限、期限、記録、レビューを通常権限より厳格に管理する。

Q089 5-3 人的・組織的対策 / 職務分離・最小権限・人的管理

重要システム担当者に対する人的セキュリティ対策の考え方として最も適切なものはどれか。
ア．職務のリスクと適用される法令・社内ルールに応じて、採用・配属・秘密保持・教育・異動・退職などの管理を適切に設計する。
イ．全職種で業務と無関係な私生活情報を無制限に調査する。
ウ．入社時だけ確認し、異動・退職時の管理は行わない。
エ．秘密保持義務は口頭だけで、重要情報の扱いを一切説明しない。

正答・4肢解説・総合解説

正答：ア．職務のリスクと適用される法令・社内ルールに応じて、採用・配属・秘密保持・教育・異動・退職などの管理を適切に設計する。
ア：人的管理は一律の過剰監視ではなく、職務の重要性と合法性・相当性を踏まえたライフサイクル管理として行う。
イ：必要性・相当性を欠く過剰な取扱いになり得る。
ウ：権限・責任の変化に対応できない。
エ：本人が義務や取扱要件を理解できない。
総合解説：人的セキュリティは、雇用前・雇用中・異動・退職後までの責任やアクセスを一貫して管理する。

Q090 5-3 人的・組織的対策 / 職務分離・最小権限・人的管理

小規模組織で人員が少なく、完全な職務分離が難しい。代替・補完策として最も適切なものはどれか。
ア．職務分離できないので全ての統制を廃止する。
イ．独立した事後レビュー、詳細ログ、上位者承認、定期ローテーションなどで単独不正を検知・抑止する。
ウ．同じ担当者に監査ログ削除権限まで追加する。
エ．管理者アカウントを全員で共有する。

正答・4肢解説・総合解説

正答：イ．独立した事後レビュー、詳細ログ、上位者承認、定期ローテーションなどで単独不正を検知・抑止する。
ア：リスクが残るため代替策を検討すべきである。
イ：人員制約があっても、権限集中によるリスクを認識し、補完統制で低減することができる。
ウ：不正の隠蔽が容易になる。
エ：個人の操作追跡が困難になる。
総合解説：組織規模に応じて実行可能な補完策を選び、残留リスクを明示して承認する。

Q091 5-3 人的・組織的対策 / 職務分離・最小権限・人的管理

システム管理者がメール閲覧やWeb閲覧も常にドメイン管理者アカウントで行っている。改善として最も適切なものはどれか。
ア．管理者アカウントを全社員へ配布して利用を分散する。
イ．特権アカウントのパスワードをブラウザへ平文保存する。
ウ．日常業務用の標準権限アカウントと管理作業用の特権アカウントを分離し、特権利用を必要時に限定する。
エ．管理者操作のログを停止して利便性を上げる。

正答・4肢解説・総合解説

正答：ウ．日常業務用の標準権限アカウントと管理作業用の特権アカウントを分離し、特権利用を必要時に限定する。
ア：高権限の利用範囲が拡大する。
イ：資格情報漏えいリスクが高い。
ウ：高権限アカウントを日常利用から分離すると、フィッシングやブラウザ侵害時の影響を抑えやすい。
エ：不正・誤操作の追跡が難しくなる。
総合解説：特権アカウントは用途分離、強固な認証、利用監視、定期的な権限確認を組み合わせる。

Q092 5-3 人的・組織的対策 / 職務分離・最小権限・人的管理

契約社員の契約終了情報が人事システムには登録されたが、複数SaaSのアカウントが数週間残存する問題が繰り返されている。最も適切な改善はどれか。
ア．各SaaS担当者が気付いた時だけ手作業で削除し、期限は設けない。
イ．契約終了者のアカウントを共有アカウントへ変更して残す。
ウ．人事情報とIT権限は無関係として連携を禁止する。
エ．人事・契約情報を権限管理の信頼できるトリガーとして連携し、対象アカウントの特定、期限、失効結果、例外を自動または統制された手順で確認する。

正答・4肢解説・総合解説

正答：エ．人事・契約情報を権限管理の信頼できるトリガーとして連携し、対象アカウントの特定、期限、失効結果、例外を自動または統制された手順で確認する。
ア：削除漏れや遅延が繰り返されやすい。
イ：誰が利用しているか追跡できず、不要アクセスも残る。
ウ：退職・契約終了に伴う失効を確実にできない。
エ：人的ライフサイクルとデジタルID管理を連携し、終了イベントが全対象システムへ確実に伝播する仕組みにする。
総合解説：Joiner-Mover-LeaverのイベントをID・権限管理へ結び付け、失効の完了確認と例外管理まで行う。

Q093 5-4 法務・コンプライアンス / 個人情報保護・マイナンバー

個人情報取扱事業者が、収集済みの顧客情報を当初特定した利用目的と関連性の乏しい新規サービスの営業に利用したい。個人情報保護法上の基本的な考え方として最も適切なものはどれか。
ア．本人の同意なく、当初の利用目的から合理的に関連すると認められる範囲を超えて利用目的を変更し、そのまま利用することはできない。
イ．一度適法に取得した個人情報であれば、社内利用に限り目的を問わず自由に利用できる。
ウ．利用目的は取得後にいつでも無制限に変更でき、本人への周知も不要である。
エ．営業部門が必要と判断すれば、個人情報保護法上の利用目的の制限は適用されない。

正答・4肢解説・総合解説

正答：ア．本人の同意なく、当初の利用目的から合理的に関連すると認められる範囲を超えて利用目的を変更し、そのまま利用することはできない。
ア：利用目的の変更には合理的な関連性の範囲という制約があり、範囲を超える利用には別途適法な根拠が必要になる。
イ：適法に取得したことと、取得後の利用目的制限は別問題である。
ウ：利用目的は無制限に変更できるわけではなく、通知・公表等も含め法のルールに従う必要がある。
エ：部門の業務上の必要性だけで法令上の制限が消えることはない。
総合解説：個人情報保護では、取得時だけでなく取得後の利用も、特定した利用目的との関係で管理する。目的外利用を避けるため、利用目的変更の可否や本人同意の要否を確認する。

Q094 5-4 法務・コンプライアンス / 個人情報保護・マイナンバー

個人データをクラウド事業者に取り扱わせるため業務委託する場合、委託元の対応として最も適切なものはどれか。
ア．委託契約を締結した時点で、委託元の安全管理上の責任は全て消滅する。
イ．委託するデータの内容やリスクに応じて委託先を選定し、契約を整備し、取扱状況を把握するなど必要かつ適切な監督を行う。
ウ．委託先が大企業であれば、委託元による監督は一切不要である。
エ．委託は第三者提供と同じなので、委託元は委託先の安全管理を確認してはならない。

正答・4肢解説・総合解説

正答：イ．委託するデータの内容やリスクに応じて委託先を選定し、契約を整備し、取扱状況を把握するなど必要かつ適切な監督を行う。
ア：委託によって委託元の監督義務が消えるわけではない。
イ：個人情報保護法の委託先監督では、適切な選定、契約、取扱状況の把握などをリスクに応じて行う。
ウ：企業規模だけで監督の要否は決まらない。
エ：委託先の安全管理状況を確認することは、むしろ必要な監督の一部である。
総合解説：個人データの委託では、委託先の選定、契約上の安全管理事項、実施状況の把握を一体として考える。立入検査だけが唯一の監督方法ではなく、リスクに応じた実効的な方法を選ぶ。

Q095 5-4 法務・コンプライアンス / 個人情報保護・マイナンバー

個人情報保護法に基づく個人データの安全管理措置を検討する際の方針として最も適切なものはどれか。
ア．暗号化だけを導入すれば、他の安全管理措置は不要である。
イ．従業者教育だけを実施し、アクセス制御や物理管理は行わない。
ウ．組織的・人的・物理的・技術的な観点を組み合わせ、取り扱うデータやリスクに応じた措置を講じる。
エ．個人データの件数が少なければ、漏えい防止策は一切不要である。

正答・4肢解説・総合解説

正答：ウ．組織的・人的・物理的・技術的な観点を組み合わせ、取り扱うデータやリスクに応じた措置を講じる。
ア：人的対策だけでは技術的・物理的リスクを十分に抑えられない。
イ：規模は措置の程度に影響し得るが、少量だから安全管理義務がなくなるわけではない。
ウ：安全管理は単一対策ではなく、規程・体制、教育、物理的保護、アクセス制御等を組み合わせる。
エ：暗号化は重要な技術的措置の一つだが、それだけで安全管理全体を代替できない。
総合解説：安全管理措置は、組織の規模、データの性質・量、取扱方法、想定される被害などを踏まえて多層的に設計する。単一対策への依存は避ける。

Q096 5-4 法務・コンプライアンス / 個人情報保護・マイナンバー

個人データの漏えい等が発覚し、法令上の報告対象に該当すると判断された場合の対応として最も適切なものはどれか。
ア．社内で原因調査が完全に終了するまで、外部への報告や本人通知を一律に禁止する。
イ．漏えいしたデータが暗号化されていれば、どのような場合でも報告対象にはならない。
ウ．委託先で発生した漏えいであれば、委託元は事案を把握する必要がない。
エ．被害拡大防止や原因調査等を進めつつ、個人情報保護委員会への報告と本人への通知について法令・ガイドラインに従って対応する。

正答・4肢解説・総合解説

正答：エ．被害拡大防止や原因調査等を進めつつ、個人情報保護委員会への報告と本人への通知について法令・ガイドラインに従って対応する。
ア：報告期限や初動を踏まえると、完全な原因確定まで一律に待つ考え方は適切でない。
イ：暗号化の有無だけで全ての報告要否が自動的に決まるわけではない。
ウ：委託元は委託先の取扱状況を把握し、必要な対応を行う必要がある。
エ：報告対象事案では、法令・ガイドラインに沿って報告・通知を行い、同時に初動対応や再発防止を進める。
総合解説：漏えい等への対応では、事実関係の把握、被害拡大防止、原因究明、影響範囲確認、報告・通知、再発防止を並行して進める。対象該当性と期限は現行ガイドラインで確認する。

Q097 5-4 法務・コンプライアンス / 個人情報保護・マイナンバー

従業員の個人番号を含む書類を、法令で認められた税・社会保障関係事務とは無関係な社内マーケティング分析に利用したいという提案があった。最も適切な判断はどれか。
ア．本人が同意していても、番号法で認められた範囲を超えて個人番号を利用することは原則としてできない。
イ．本人が口頭で同意すれば、個人番号はどのような社内目的にも利用できる。
ウ．個人番号を氏名と分離すれば、目的外利用は常に可能になる。
エ．社内だけで処理する限り、番号法の利用制限は適用されない。

正答・4肢解説・総合解説

正答：ア．本人が同意していても、番号法で認められた範囲を超えて個人番号を利用することは原則としてできない。
ア：個人番号は利用範囲が法令で限定されており、一般の個人情報より厳格な取扱いが求められる。
イ：本人同意だけで法定の利用範囲を自由に拡張できる制度ではない。
ウ：分離保存だけで利用目的の制限がなくなるわけではない。
エ：社内利用か社外提供かとは別に、番号法上の利用制限がある。
総合解説：マイナンバー制度では、個人番号の利用・提供・収集・保管が法令で限定される。一般の個人情報の同意モデルと同じ感覚で扱わないことが重要である。

Q098 5-4 法務・コンプライアンス / 個人情報保護・マイナンバー

「特定個人情報」の説明として最も適切なものはどれか。
ア．個人番号だけを単独で保存したものに限り、氏名などと組み合わせた情報は含まれない。
イ．個人番号をその内容に含む個人情報である。
ウ．法人番号を含む企業情報は全て特定個人情報になる。
エ．個人番号を暗号化した時点で、必ず特定個人情報ではなくなる。

正答・4肢解説・総合解説

正答：イ．個人番号をその内容に含む個人情報である。
ア：氏名等と結び付いた個人番号も特定個人情報に該当し得る。
イ：特定個人情報は、個人番号を内容に含む個人情報として扱われる。
ウ：法人番号は個人番号とは別制度であり、同じ定義ではない。
エ：暗号化は安全管理措置になり得るが、情報の法的性質を自動的に消すものではない。
総合解説：特定個人情報は、個人番号を含む個人情報である。取扱いでは番号法に基づく利用・提供・収集・保管の制限と安全管理措置を確認する。

Q099 5-4 法務・コンプライアンス / 個人情報保護・マイナンバー

個人番号関係事務を外部業者A社に委託している。A社が業務の一部をB社へ再委託したいと申し出た。番号法上の対応として最も適切なものはどれか。
ア．A社が責任を負うため、最初の委託者への連絡や許諾は不要である。
イ．B社が国内企業であれば、再委託の許諾は不要である。
ウ．最初の委託者の許諾を得た上で再委託し、再委託先を含めた安全管理が確保されるよう監督する。
エ．再委託先がISMS認証を取得していれば、番号法上の監督は不要である。

正答・4肢解説・総合解説

正答：ウ．最初の委託者の許諾を得た上で再委託し、再委託先を含めた安全管理が確保されるよう監督する。
ア：委託契約の当事者関係だけで番号法上の要件は消えない。
イ：国内外の別だけで許諾要件は決まらない。
ウ：番号法では、個人番号関係事務等の再委託には最初の委託者の許諾が必要であり、再委託先等にも監督が及ぶ。
エ：認証は評価材料になり得るが、法令上必要な監督や許諾を代替しない。
総合解説：マイナンバーの委託では、再委託を含めたサプライチェーンの見える化が重要である。許諾時には再委託先の安全管理能力を確認し、契約・報告等で継続的に把握する。

Q100 5-4 法務・コンプライアンス / 個人情報保護・マイナンバー

法定保存期間が経過し、個人番号を利用する必要もなくなった特定個人情報ファイルの取扱いとして最も適切なものはどれか。
ア．将来使う可能性が少しでもあれば、利用目的に関係なく永久保存する。
イ．バックアップに残る限り、運用系データを削除する必要はない。
ウ．保存期間終了後も、アクセス権を一人に限定すれば無期限保管できる。
エ．個人番号を保有する必要がなくなった時点を確認し、復元困難な方法で速やかに削除・廃棄する運用を行う。

正答・4肢解説・総合解説

正答：エ．個人番号を保有する必要がなくなった時点を確認し、復元困難な方法で速やかに削除・廃棄する運用を行う。
ア：番号法は必要のない個人番号の収集・保管を制限するため、漠然とした将来可能性だけで永久保有するのは適切でない。
イ：バックアップを含め、削除・廃棄方針と実施確認を設計する必要がある。
ウ：アクセス制限は安全管理策だが、不必要な保管を正当化するものではない。
エ：必要性がなくなった個人番号は、保存期間等を踏まえ、削除・廃棄を適切に実施する。
総合解説：特定個人情報のライフサイクル管理では、取得・利用だけでなく、不要となった後の削除・廃棄も重要である。バックアップや委託先保管分を含め、実施方法と確認方法を定める。

Q101 5-4 法務・コンプライアンス / 個人情報保護・マイナンバー

企業が人事給与システムで特定個人情報を扱う際、アクセス権設計として最も適切なものはどれか。
ア．個人番号関係事務を担当する必要のある従業者を明確にし、その職務に必要な範囲だけアクセスを認める。
イ．人事部に所属していれば、全員に個人番号の閲覧権限を付与する。
ウ．システム管理者は保守上便利なので、業務上の必要性に関係なく常時全件閲覧できるようにする。
エ．同じ会社の従業員であれば、個人番号の閲覧権限は共有してよい。

正答・4肢解説・総合解説

正答：ア．個人番号関係事務を担当する必要のある従業者を明確にし、その職務に必要な範囲だけアクセスを認める。
ア：特定個人情報では、取扱担当者を明確にし、必要最小限のアクセス権とすることが安全管理の基本である。
イ：所属部門だけを根拠に一律の広い権限を与えるのは過剰権限になりやすい。
ウ：管理者権限も必要性・期間・利用記録等を管理すべきである。
エ：同一組織内であっても、職務上不要な者へのアクセスは制限する。
総合解説：法務・コンプライアンスと技術的アクセス制御は分離して考えず、法令上の取扱範囲を権限設計に落とし込む。権限棚卸しや操作記録も組み合わせると実効性が高まる。

Q102 5-4 法務・コンプライアンス / 個人情報保護・マイナンバー

同じ名簿データに氏名・連絡先と個人番号が含まれている。一般の顧客名簿と同じ社内ルールだけで運用する案を評価した結果として最も適切なものはどれか。
ア．氏名と連絡先が含まれるので、番号法は一切適用されない。
イ．個人番号を含むため、個人情報保護法だけでなく番号法上のより厳格な利用・提供・収集・保管制限を踏まえてルールを設計する必要がある。
ウ．個人番号が一項目でも含まれていれば、個人情報保護法は一切考慮しなくてよい。
エ．社内規程で「重要情報」と定義すれば、法令上の利用制限を独自に解除できる。

正答・4肢解説・総合解説

正答：イ．個人番号を含むため、個人情報保護法だけでなく番号法上のより厳格な利用・提供・収集・保管制限を踏まえてルールを設計する必要がある。
ア：他の個人情報と併存していても番号法の適用が消えるわけではない。
イ：個人番号を含む個人情報は特定個人情報として番号法の制約を受けるため、一般名簿より厳格な運用が必要になる。
ウ：番号法と個人情報保護法の関係を踏まえて両方の要件を確認する。
エ：内部規程は法令を上書きして利用制限を解除することはできない。
総合解説：特定個人情報は「一般の個人情報に少し厳しいラベルを付けたもの」ではなく、番号法特有の利用・提供・収集・保管制限がある。システム設計でもデータ項目単位の分離や権限管理を検討する。

Q103 5-4 法務・コンプライアンス / 不正アクセス・不正競争・刑法

退職した元従業員が、在職中に知った別人のID・パスワードを無断で用い、インターネット経由でアクセス制御された社内サービスにログインした。この行為に関する説明として最も適切なものはどれか。
ア．パスワードが以前の勤務中に知り得たものであれば、退職後に使用しても必ず適法である。
イ．実際にデータを削除しなければ、不正アクセス行為にはなり得ない。
ウ．他人の識別符号を無断で入力してアクセス制御を突破する行為は、不正アクセス禁止法上の不正アクセス行為に該当し得る。
エ．アクセス先が社内システムであれば、不正アクセス禁止法は適用されない。

正答・4肢解説・総合解説

正答：ウ．他人の識別符号を無断で入力してアクセス制御を突破する行為は、不正アクセス禁止法上の不正アクセス行為に該当し得る。
ア：過去に知る立場にあったことと、現在の利用権限があることは別である。
イ：不正アクセス行為の成立に、必ずデータ破壊まで必要というわけではない。
ウ：不正アクセス禁止法は、他人の識別符号を無断で入力してアクセス制御により制限された利用を可能にする行為等を禁止する。
エ：組織内システムでも、法の要件を満たすアクセス制御された特定電子計算機への行為は対象になり得る。
総合解説：認証情報を「知っている」ことと「使用する権限がある」ことを区別する。不正アクセス禁止法ではアクセス制御を無断で回避する行為自体が問題になる。

Q104 5-4 法務・コンプライアンス / 不正アクセス・不正競争・刑法

偽のログイン画面を公開し、正規サービスの管理者になりすまして利用者にID・パスワードの入力を求める行為について、最も適切な説明はどれか。
ア．実際に不正ログインを完了しなければ、識別符号の入力を求める行為自体は規制対象にならない。
イ．利用者が入力しなかった場合は、偽サイトの公開は常に適法となる。
ウ．金銭を要求していないフィッシングであれば、サイバーセキュリティ関連法令の問題にはならない。
エ．不正アクセス禁止法は、アクセス管理者であると誤認させて識別符号の入力を不正に要求する行為も禁止している。

正答・4肢解説・総合解説

正答：エ．不正アクセス禁止法は、アクセス管理者であると誤認させて識別符号の入力を不正に要求する行為も禁止している。
ア：不正ログインの成否とは別に、入力要求行為を禁止する規定がある。
イ：被害者が実際に入力したかどうかだけで行為の法的評価が決まるわけではない。
ウ：金銭要求の有無は、この規制の中心要件ではない。
エ：不正アクセス禁止法は、不正アクセスそのものだけでなく、識別符号の入力を不正に要求する行為も規制する。
総合解説：不正アクセス対策では、侵入行為だけでなく、認証情報を盗む準備段階・助長行為にも法規制がある。セキュリティ担当者はフィッシング対応時に証拠保全と関係部門への連携も考える。

Q105　5-4 法務・コンプライアンス / 不正アクセス・不正競争・刑法

不正アクセス行為に使う目的で、他人のID・パスワードを不正に入手して保管する行為について最も適切なものはどれか。
ア．不正アクセス禁止法では、目的や取得・保管の態様に応じて、識別符号の不正取得や不正保管自体も禁止対象となる。
イ．実際にログインしなければ、認証情報を不正に取得・保管しても同法上の問題は一切生じない。
ウ．紙に印刷して保管すれば、識別符号の保管には当たらない。
エ．本人の識別符号であれば、第三者に不正アクセス目的で提供しても常に適法である。

正答・4肢解説・総合解説

正答：ア．不正アクセス禁止法では、目的や取得・保管の態様に応じて、識別符号の不正取得や不正保管自体も禁止対象となる。
ア：同法は不正アクセス行為だけでなく、その用に供する目的での他人の識別符号の取得・保管等も規制している。
イ：実行前の一定の準備行為も独立して規制対象になり得る。
ウ：媒体だけで法的評価が自動的に変わるわけではない。
エ：識別符号の提供にも不正アクセス助長行為として規制がある。
総合解説：法令問題では「侵入したか」だけでなく、認証情報の取得・提供・保管・入力要求といった関連行為を分けて理解することが重要である。

Q106　5-4 法務・コンプライアンス / 不正アクセス・不正競争・刑法

不正アクセス禁止法の対象を判断する際の説明として最も適切なものはどれか。
ア．他人のPCに物理的に触れた行為は、ネットワークやアクセス制御の有無に関係なく全て同法の不正アクセス行為になる。
イ．同法の不正アクセス行為は、電気通信回線を通じ、アクセス制御機能による特定利用の制限を無断で免れる行為等を対象としている。
ウ．正規の利用権者が自分の識別符号で認められた範囲を利用する行為も、必ず不正アクセスになる。
エ．アクセス管理者の承諾を得た脆弱性診断でも、アクセス制御された機器に接続した時点で必ず違法となる。

正答・4肢解説・総合解説

正答：イ．同法の不正アクセス行為は、電気通信回線を通じ、アクセス制御機能による特定利用の制限を無断で免れる行為等を対象としている。
ア：物理的な無断操作が別の問題になることはあるが、それだけで同法の不正アクセス行為と決まるわけではない。
イ：同法は「電気通信回線」「アクセス制御機能」「制限を免れる行為」等の法定要件に基づいて判断する。
ウ：正当な利用権限内の利用は無断で制限を免れる行為とは異なる。
エ：アクセス管理者等の承諾の有無は重要であり、適法な診断は明確な権限付与の下で行う。
総合解説：ペネトレーションテストや調査では、事前に対象、手法、時間帯、権限、緊急停止条件などを文書化する。技術的に可能かではなく、権限があるかを必ず確認する。

Q107 5-4 法務・コンプライアンス / 不正アクセス・不正競争・刑法

不正競争防止法上の「営業秘密」として保護されるための基本的な三要件の組合せとして最も適切なものはどれか。
ア．完全暗号化・特許登録・海外非公開
イ．個人情報該当性・著作物性・希少性
ウ．秘密管理性・有用性・非公知性
エ．社外秘表示・高額性・保存年数10年以上

正答・4肢解説・総合解説

正答：ウ．秘密管理性・有用性・非公知性
ア：暗号化や特許登録は営業秘密の三要件そのものではない。
イ：個人情報や著作物に該当するかどうかは営業秘密の三要件とは別である。
ウ：営業秘密は、秘密として管理されていること、事業活動に有用であること、公然と知られていないことが基本要件である。
エ：表示や金額、保存年数だけで自動的に営業秘密になるわけではない。
総合解説：営業秘密の保護では「重要そうな情報」だけでは足りず、三要件を満たす必要がある。特に秘密管理性は、組織が秘密として管理する意思を従業員等が認識できるようにすることが重要である。

Q108 5-4 法務・コンプライアンス / 不正アクセス・不正競争・刑法

営業秘密の秘密管理性を高める運用として最も適切なものはどれか。
ア．機密情報かどうかを誰にも知らせず、全社員が全ファイルへアクセスできるようにする。
イ．秘密表示だけを付ければ、アクセス制御や運用実態にかかわらず必ず秘密管理性が認められる。
ウ．情報価値が高ければ、社内で公開状態でも自動的に秘密管理性を満たす。
エ．重要情報を特定し、アクセス権限、表示、保管場所、持出しルールなどを通じて、秘密として管理する意思が従業員等に分かる状態を作る。

正答・4肢解説・総合解説

正答：エ．重要情報を特定し、アクセス権限、表示、保管場所、持出しルールなどを通じて、秘密として管理する意思が従業員等に分かる状態を作る。
ア：秘密性を示さず広範なアクセスを許す運用は、秘密管理の意思を示しにくい。
イ：表示は重要な手段の一つだが、実態を無視して必ず要件を満たすとはいえない。
ウ：有用性と秘密管理性は別要件であり、価値が高いだけでは足りない。
エ：秘密管理性は、秘密として扱う組織の意思が従業員等に認識可能となるよう、実態に応じた管理を行うことが中心となる。
総合解説：秘密管理性の評価は、単一の形式要件だけでなく、情報の性質や組織規模を踏まえた合理的な管理実態を見る。技術・規程・教育を一体化する。

Q109 5-4 法務・コンプライアンス / 不正アクセス・不正競争・刑法

競合企業の未公開設計情報を、権限のない者が不正な手段で取得して利用する行為について、セキュリティ担当者がまず確認すべき法的観点として最も適切なものはどれか。
ア．対象情報が営業秘密の要件を満たすか、不正競争防止法上の営業秘密侵害に該当し得る行為かを確認する。
イ．情報がデジタル形式なら、不正競争防止法は適用されない。
ウ．営業秘密は製造業の図面だけが対象で、顧客情報やノウハウは対象になり得ない。
エ．情報を複製せず画面で閲覧しただけなら、営業秘密に関する問題は絶対に生じない。

正答・4肢解説・総合解説

正答：ア．対象情報が営業秘密の要件を満たすか、不正競争防止法上の営業秘密侵害に該当し得る行為かを確認する。
ア：営業秘密に該当する情報の不正取得・使用・開示等は、不正競争防止法上の問題になり得る。
イ：営業秘密は媒体が紙かデジタルかだけで除外されるものではない。
ウ：技術情報だけでなく営業上の情報も要件を満たせば対象になり得る。
エ：具体的な行為態様を含め法的評価が必要で、単なる閲覧か否かだけで一律には決まらない。
総合解説：インシデント対応では、営業秘密性を維持する管理実態の証拠も重要になる。アクセスログ、権限設定、秘密表示、教育記録などを平時から整備しておく。

Q110 5-4 法務・コンプライアンス / 不正アクセス・不正競争・刑法

他人の業務を妨害する目的で、サーバに虚偽の情報や不正な指令を与え、意図された用途に従う動作をさせず、実際に業務を妨害した場合に関係し得る刑法上の犯罪として最も適切なものはどれか。
ア．単純な著作権侵害罪だけ
イ．電子計算機損壊等業務妨害罪
ウ．営業秘密の秘密管理性違反だけ
エ．個人情報保護法上の利用目的変更だけ

正答・4肢解説・総合解説

正答：イ．電子計算機損壊等業務妨害罪
ア：著作権侵害は別の法益・要件の問題であり、設問の行為を直接説明するものではない。
イ：刑法には、電子計算機や電磁的記録を損壊したり虚偽情報・不正指令を与えたりして業務を妨害する行為を対象とする規定がある。
ウ：営業秘密の管理要件と、電子計算機を用いた業務妨害の犯罪類型は別である。
エ：個人情報の利用目的の問題だけでは、サーバを不正に作動させて業務を妨害する行為を説明できない。
総合解説：サイバー事件では一つの行為が複数法令に関係することがある。セキュリティ担当者は犯罪類型を断定せず、事実とログを保全し、法務・捜査機関等と連携する。

Q111 5-4 法務・コンプライアンス / 不正アクセス・不正競争・刑法

正当な理由なく、人の電子計算機で実行させると利用者の意図に反する動作をさせる不正なプログラムを作成・提供する行為について、関係し得る刑法上の規定として最も適切なものはどれか。
ア．特定商取引法の訪問販売規制だけ
イ．独占禁止法の企業結合規制だけ
ウ．不正指令電磁的記録に関する罪
エ．商法の会社機関設計だけ

正答・4肢解説・総合解説

正答：ウ．不正指令電磁的記録に関する罪
ア：訪問販売規制は設問のプログラム作成・提供を直接説明する規定ではない。
イ：企業結合規制とは関係する法益が異なる。
ウ：刑法には、いわゆるコンピュータ・ウイルス等の不正指令電磁的記録の作成・提供等を対象とする規定がある。
エ：会社法制上の機関設計とは異なる問題である。
総合解説：マルウェア解析や検証のためのプログラム取扱いでは、正当な目的、承認された環境、アクセス制御、持出し禁止等を明確化する。法的評価は目的・態様を含めて行う。

Q112 5-4 法務・コンプライアンス / 契約・倫理・証拠保全

外部ベンダに重要システムの運用を委託する契約で、セキュリティ事故時の混乱を減らすために最も重要な条項の組合せはどれか。
ア．契約金額と支払日だけを定め、セキュリティ上の責任は口頭合意に任せる。
イ．秘密保持条項だけを置けば、事故対応や再委託の取扱いは定めなくてよい。
ウ．ベンダが有名企業であれば、事故報告や監査に関する条項は不要である。
エ．責任分界、事故の報告・連絡、再委託条件、監査・確認、データ返却・削除などを具体化する。

正答・4肢解説・総合解説

正答：エ．責任分界、事故の報告・連絡、再委託条件、監査・確認、データ返却・削除などを具体化する。
ア：口頭合意だけでは解釈の不一致や担当者変更時のリスクが高まる。
イ：NDAは重要だが、事故報告、再委託、監査等を全て代替するものではない。
ウ：企業の知名度は契約上の責任分界を不要にする理由にならない。
エ：セキュリティに関する役割・責任と運用条件を契約に落とすことで、有事の判断・連携を明確にできる。
総合解説：契約は「守ること」だけでなく、誰が・いつまでに・何を報告し、どこまで調査・復旧・証拠保全に協力するかまで具体化すると実効性が高い。

Q113 5-4 法務・コンプライアンス / 契約・倫理・証拠保全

秘密保持契約（NDA）を締結した後の情報保護について最も適切な考え方はどれか。
ア．NDAは重要だが、それだけに依存せず、アクセス制御、ログ、持出し管理、教育など実際の保護策も運用する。
イ．NDAがあれば、秘密情報を全社員に無制限で共有しても安全管理上問題はない。
ウ．NDA締結後は、秘密情報の分類やアクセス権管理を行う必要がなくなる。
エ．NDAがあれば、営業秘密の秘密管理性は運用実態に関係なく必ず認められる。

正答・4肢解説・総合解説

正答：ア．NDAは重要だが、それだけに依存せず、アクセス制御、ログ、持出し管理、教育など実際の保護策も運用する。
ア：契約による義務付けと技術的・組織的管理は相互補完であり、いずれか一方だけで十分とは限らない。
イ：契約があっても不要なアクセスを広く許す設計はリスクを高める。
ウ：情報分類やアクセス制御は実際の保護と証跡のために必要である。
エ：営業秘密の秘密管理性は管理実態も含めて評価されるため、NDAだけで自動的に決まらない。
総合解説：契約上の義務をシステム設定や運用手続に対応付けることが重要である。秘密保持期間、例外、返却・廃棄、再委託等も情報の性質に応じて定める。

Q114 5-4 法務・コンプライアンス / 契約・倫理・証拠保全

情報処理安全確保支援士が業務上知り得た顧客の未公表インシデント情報を、正当な理由なく知人へ話す行為を倫理綱領の観点から評価したものとして最も適切なものはどれか。
ア．自己研鑽の原則に従った適切な行為である。
イ．秘密保持の原則に反する。
ウ．顧客名を伏せれば、どのような内容でも無条件に第三者へ話してよい。
エ．報酬を受け取っていなければ、秘密保持は適用されない。

正答・4肢解説・総合解説

正答：イ．秘密保持の原則に反する。
ア：自己研鑽は知識・技能の向上を求める原則で、秘密漏えいを正当化しない。
イ：倫理綱領は、正当な理由なく業務上知り得た秘密を漏らし、又は盗用しないことを求める。
ウ：匿名化の程度や再識別可能性などを含め、機密情報の扱いには慎重さが必要である。
エ：秘密保持は報酬の有無だけで解除されるものではない。
総合解説：専門家は技術能力だけでなく、信頼を維持する倫理的行動が求められる。事例共有が必要な場合は、契約・法令・組織ルールを確認し、十分な匿名化や承認を得る。

Q115 5-4 法務・コンプライアンス / 契約・倫理・証拠保全

情報処理安全確保支援士が、特定製品の導入可否を評価する際、販売会社から個人的な利益供与を受け、その事実を隠して推奨する行為を倫理綱領の観点から評価したものとして最も適切なものはどれか。
ア．専門知識が高ければ、利益相反は考慮しなくてよい。
イ．会社に損害が発生しなければ、利益供与の事実を開示する必要はない。
ウ．公正・誠実な判断を損ない、専門家としての信用にも影響するため不適切である。
エ．推奨製品が結果的に安全なら、判断過程の公正性は問題にならない。

正答・4肢解説・総合解説

正答：ウ．公正・誠実な判断を損ない、専門家としての信用にも影響するため不適切である。
ア：専門能力が高くても利益相反による判断の偏りは別問題である。
イ：結果だけでなく意思決定過程の透明性・公正性も重要である。
ウ：倫理綱領は、不当な影響を受けず公正な立場を保ち、公正・誠実に業務を遂行することを求める。
エ：安全性が高い製品であっても、利益供与を隠した評価は専門家への信頼を損なう。
総合解説：利益相反があり得る場合は、組織の規程に従い開示・回避・管理を行い、独立したレビューを入れるなど判断の公正性を担保する。

Q116 5-4 法務・コンプライアンス / 契約・倫理・証拠保全

インシデント調査で、法的手続にも利用する可能性があるディスクを保全する際の基本方針として最も適切なものはどれか。
ア．調査を急ぐため、原本上で自由にファイルを編集し、作業記録は残さない。
イ．証拠になりそうなファイルだけを手作業でコピーし、その他の情報は直ちに削除する。
ウ．調査担当者の記憶があれば、取得日時や保管者の記録は不要である。
エ．原本への変更をできるだけ避け、適切な方法で複製・保全し、誰がいつ何を行ったかを記録する。

正答・4肢解説・総合解説

正答：エ．原本への変更をできるだけ避け、適切な方法で複製・保全し、誰がいつ何を行ったかを記録する。
ア：原本を不用意に変更すると調査結果の信頼性を損なう可能性がある。
イ：一部ファイルだけを選別すると、重要なメタデータや関連情報を失うおそれがある。
ウ：人の記憶だけでなく、手順と記録により再現可能性・説明可能性を確保する。
エ：証拠保全では、原本性・完全性を損なわない取扱いと、取得・移送・保管・分析の記録が重要である。
総合解説：デジタル証拠は操作により状態が変化しやすい。保全手順、担当者、日時、媒体識別、ハッシュ値などを記録し、必要に応じてフォレンジック専門家と連携する。

Q117 5-4 法務・コンプライアンス / 契約・倫理・証拠保全

デジタル証拠の「チェーン・オブ・カストディ（保管の連鎖）」を維持する目的として最も適切なものはどれか。
ア．証拠を誰がいつ受領・保管・移送・分析したかを追跡できるようにし、取扱いの連続性と信頼性を説明できるようにする。
イ．証拠ファイルを暗号化せず公開共有するため。
ウ．ログの保存容量を減らすため。
エ．解析結果を必ず有罪立証に結び付けるため。

正答・4肢解説・総合解説

正答：ア．証拠を誰がいつ受領・保管・移送・分析したかを追跡できるようにし、取扱いの連続性と信頼性を説明できるようにする。
ア：チェーン・オブ・カストディは、証拠の取扱履歴を追跡し、不適切な改変・取り違え等がないことを説明するために重要である。
イ：公開共有はむしろ証拠や機密性を損なう可能性がある。
ウ：主目的は容量削減ではなく証拠の信頼性確保である。
エ：証拠保全は特定の結論を保証するものではなく、客観的な事実確認を支える。
総合解説：技術的な完全性確認だけでなく、物理媒体の識別、封印、保管場所、引渡し記録など手続面の管理も重要になる。

Q118 5-4 法務・コンプライアンス / 契約・倫理・証拠保全

取得したディスクイメージの完全性を後から確認しやすくする方法として最も適切なものはどれか。
ア．ファイル名だけを記録し、内容の完全性確認は行わない。
イ．取得時に暗号学的ハッシュ値を計算・記録し、分析用コピーについて再計算した値と比較する。
ウ．画像ファイルに変換して目視で同一に見えるかだけ確認する。
エ．調査終了後にだけ一度ハッシュを計算し、取得時の値は残さない。

正答・4肢解説・総合解説

正答：イ．取得時に暗号学的ハッシュ値を計算・記録し、分析用コピーについて再計算した値と比較する。
ア：ファイル名は容易に変更でき、内容の同一性を示す手段として不十分である。
イ：暗号学的ハッシュは、取得時と後続時点のデータが同一かを検証する補助情報として利用できる。
ウ：目視確認は大量データやメタデータの完全性検証には適さない。
エ：比較には基準となる取得時の値を記録しておくことが重要である。
総合解説：ハッシュ値だけで証拠管理の全要件を満たすわけではない。取得手順、ツール、担当者、日時、保管履歴などと組み合わせて説明可能性を確保する。

Q119 5-4 法務・コンプライアンス / 契約・倫理・証拠保全

ランサムウェア感染が疑われる端末を従業員が発見した。証拠保全と被害拡大防止を両立する初動として最も適切なものはどれか。
ア．証拠を消すため、直ちに全ログと疑わしいメールを削除する。
イ．原因を調べるため、感染端末から社内の全サーバへ管理者権限で接続する。
ウ．定められた手順に従ってネットワークから切り離し、CSIRT等へ連絡し、メールやファイルを勝手に削除せず、専門担当者の指示で保全する。
エ．被害を隠すため、CSIRTへの連絡を行わず端末を初期化する。

正答・4肢解説・総合解説

正答：ウ．定められた手順に従ってネットワークから切り離し、CSIRT等へ連絡し、メールやファイルを勝手に削除せず、専門担当者の指示で保全する。
ア：削除は調査に必要な証拠を失わせるおそれがある。
イ：感染端末からの横展開を助長する操作は避けるべきである。
ウ：被害拡大を抑えながら、痕跡を失わないよう規定された初動とエスカレーションに従う。
エ：独断の初期化は原因究明・影響範囲把握・法的対応を難しくする。
総合解説：初動手順は平時に定め、従業員が迷わずCSIRTへ連絡できるよう訓練する。端末の電源操作などは状況により証拠へ影響するため、組織の手順と専門家の指示に従う。

Q120 5-4 法務・コンプライアンス / 契約・倫理・証拠保全

外部フォレンジック事業者へ調査を依頼する契約を事前に整備する際、証拠保全の観点から盛り込む事項として最も適切なものはどれか。
ア．解析結果の結論を契約前に固定し、それに合う証拠だけを収集させる。
イ．委託先に無制限の本番アクセス権を恒久付与し、操作記録を残さない。
ウ．事故発生後に担当者の口頭判断で全て決めるため、事前条件は定めない。
エ．証拠の取得・移送・保管手順、機密保持、作業記録、返却・廃棄、緊急連絡と権限範囲を明確にする。

正答・4肢解説・総合解説

正答：エ．証拠の取得・移送・保管手順、機密保持、作業記録、返却・廃棄、緊急連絡と権限範囲を明確にする。
ア：調査は客観性が必要で、結論ありきの証拠選別は適切でない。
イ：最小権限・期限付き権限・操作記録などを適用すべきである。
ウ：緊急時こそ事前に連絡先・権限・手続を合意しておくことで混乱を減らせる。
エ：証拠保全では、技術手順と契約上の責任・機密性・取扱履歴を整合させることが重要である。
総合解説：外部専門家の活用は有効だが、委託元が証拠・個人情報・営業秘密の取扱責任を意識し、契約・アクセス制御・チェーンオブカストディを設計する必要がある。

Q121 5-5 委託・サプライチェーン / 委託先管理

機密データを扱うSaaSの新規委託先を選定する際、最初に行うべきリスクベースの評価として最も適切なものはどれか。
ア．扱う情報の機密性、業務の重要度、接続権限、法令要件などを整理し、それに応じて委託先の管理策を評価する。
イ．企業規模だけで安全性を判断し、取扱データや接続範囲は確認しない。
ウ．最安価格の候補を先に決め、セキュリティ評価は契約後に初めて行う。
エ．Webサイトに「安全」と書いてあれば、他の確認は不要とする。

正答・4肢解説・総合解説

正答：ア．扱う情報の機密性、業務の重要度、接続権限、法令要件などを整理し、それに応じて委託先の管理策を評価する。
ア：委託先評価は、自組織がそのサービスへ何を依存させるかというリスク文脈から始める。
イ：企業規模は一要素に過ぎず、具体的なリスク評価を代替しない。
ウ：セキュリティ要件は選定・契約前から考慮する必要がある。
エ：自己宣言だけでなく、管理策、実績、第三者評価、契約条件等を確認する。
総合解説：同じ委託先でも、公開情報を扱う業務と機密情報・特権アクセスを扱う業務では必要な評価水準が異なる。委託リスクを先に分類する。

Q122 5-5 委託・サプライチェーン / 委託先管理

個人データの取扱いを委託する事業者が、委託先監督を実効的に行うための流れとして最も適切なものはどれか。
ア．選定時の確認だけで終了し、契約後の状況変化は一切確認しない。
イ．委託先を適切に選定し、安全管理に関する契約を整備し、契約後も取扱状況を把握して必要に応じ改善を求める。
ウ．契約書があれば、実施状況を確認する必要はない。
エ．個人データの委託では、委託先へ安全管理を要求してはならない。

正答・4肢解説・総合解説

正答：イ．委託先を適切に選定し、安全管理に関する契約を整備し、契約後も取扱状況を把握して必要に応じ改善を求める。
ア：一度の評価では、担当者、システム、再委託先等の変化を捉えられない。
イ：個人情報保護法の委託先監督は、選定・契約・取扱状況把握を組み合わせた継続的な管理を想定する。
ウ：契約と実態が一致しているかを確認する必要がある。
エ：安全管理の確保は委託元が監督すべき事項である。
総合解説：委託先管理は「契約して終わり」ではない。評価頻度や証跡はリスクに応じて設定し、重大変更や事故時には臨時評価も行う。

Q123 5-5 委託・サプライチェーン / 委託先管理

重要業務の委託先が複数の再委託先を利用している。サプライチェーン上の可視性を高める対応として最も適切なものはどれか。
ア．一次委託先と契約しているため、再委託先の存在は一切把握しない。
イ．再委託先が国外にある場合だけ確認し、国内再委託は無条件で認める。
ウ．再委託の範囲、重要な再委託先、処理場所・役割、変更通知条件などを把握し、リスクに応じた承認・監督ルールを定める。
エ．再委託先の追加・変更を委託元に知らせないことを契約条件にする。

正答・4肢解説・総合解説

正答：ウ．再委託の範囲、重要な再委託先、処理場所・役割、変更通知条件などを把握し、リスクに応じた承認・監督ルールを定める。
ア：一次委託先だけを見ても、実際の処理主体や依存関係を把握できない。
イ：国内外を問わず、重要性・データ・権限に応じて確認する。
ウ：再委託が増えるほど可視性が低下するため、重要な依存先と変更を把握する仕組みが必要である。
エ：重要な再委託変更はリスクに影響するため、通知・承認等のルールを検討する。
総合解説：委託先の「先」にある依存関係は、インシデント時の影響範囲や法令対応に直結する。契約上のフローダウン要求も検討する。

Q124 5-5 委託・サプライチェーン / 委託先管理

クラウド運用委託で、事故時に委託元と委託先の責任が曖昧にならないようにする管理として最も適切なものはどれか。
ア．「双方が適切に対応する」とだけ記載し、具体的な担当は決めない。
イ．全責任を委託先に移したとみなし、委託元の連絡体制を廃止する。
ウ．事故発生時に初めて担当者を決める。
エ．監視、検知、一次対応、証拠保全、対外報告、復旧などの役割と責任分界を事前に文書化する。

正答・4肢解説・総合解説

正答：エ．監視、検知、一次対応、証拠保全、対外報告、復旧などの役割と責任分界を事前に文書化する。
ア：抽象的な表現だけでは初動の判断基準が不明確になりやすい。
イ：委託しても委託元が自組織の業務・法令対応を担う場面は残る。
ウ：緊急時の担当決めは時間を浪費するため、平時に定める。
エ：役割分担を具体化すると、重複・抜け・報告遅延を減らせる。
総合解説：責任分界は契約だけでなく、連絡網・Runbook・演習まで連動させる。クラウドの責任共有モデルとも整合を確認する。

Q125 5-5 委託・サプライチェーン / 委託先管理

委託先でセキュリティインシデントが発生した場合の報告条項を設計する際、最も適切な内容はどれか。
ア．報告対象、初報の期限又は条件、連絡経路、継続報告、証拠保全、影響範囲調査への協力を具体化する。
イ．事故の最終原因が完全に確定するまで、初報は禁止する。
ウ．委託先の判断で公表した場合だけ、委託元へ報告する。
エ．インシデント報告は契約終了後にまとめて行えばよい。

正答・4肢解説・総合解説

正答：ア．報告対象、初報の期限又は条件、連絡経路、継続報告、証拠保全、影響範囲調査への協力を具体化する。
ア：初動に必要な情報を早期に共有し、その後更新していく設計が現実的である。
イ：完全確定まで待つと被害拡大防止や法令報告に間に合わないおそれがある。
ウ：委託元の業務影響や法令義務の判断のため、委託元への連絡が必要になる。
エ：有事対応はリアルタイム性が重要で、契約終了時の事後報告では遅い。
総合解説：「重大事故は速やかに報告」だけでは解釈が分かれる。重大度、初報情報、更新頻度、最終報告、連絡不能時の代替経路を具体化すると実効性が高い。

Q126 5-5 委託・サプライチェーン / 委託先管理

高リスクな委託先に対する監査権条項を設ける主な目的として最も適切なものはどれか。
ア．委託先の全ての営業秘密を無制限に取得するため。
イ．契約で要求したセキュリティ対策が実際に実施されているかを、必要に応じて証跡や監査等で確認できるようにする。
ウ．監査を実施すれば、委託元は自社のリスク評価をしなくてよくなるため。
エ．監査権があれば、日常の報告やKPIは不要になるため。

正答・4肢解説・総合解説

正答：イ．契約で要求したセキュリティ対策が実際に実施されているかを、必要に応じて証跡や監査等で確認できるようにする。
ア：監査範囲は目的・機密性・法令等に配慮し、無制限な情報取得を意味しない。
イ：監査権は、契約要求と実施状況のギャップを確認する手段の一つである。
ウ：委託元自身のリスク評価・意思決定は引き続き必要である。
エ：監査は継続監視の一手段であり、報告や指標と組み合わせる。
総合解説：実地監査だけが方法ではない。第三者報告書、証明書、質問票、ログ・KPIなど、リスクとコストに応じた証跡を組み合わせる。

Q127 5-5 委託・サプライチェーン / 委託先管理

委託契約終了時のセキュリティ管理として最も適切なものはどれか。
ア．将来再契約する可能性に備え、全ての特権アカウントを無期限で残す。
イ．契約終了後のデータは委託先の自由利用に任せる。
ウ．委託先・再委託先のアカウントや接続権限を失効させ、データの返却・削除を確認し、必要な証跡を保存する。
エ．本番データを削除すれば、バックアップや再委託先のコピーは確認不要である。

正答・4肢解説・総合解説

正答：ウ．委託先・再委託先のアカウントや接続権限を失効させ、データの返却・削除を確認し、必要な証跡を保存する。
ア：休眠特権アカウントは侵害時の入口となり得る。
イ：データの利用・返却・削除条件は契約と法令に従う必要がある。
ウ：終了時にはアクセスとデータ双方の残存リスクを解消し、実施確認を残す。
エ：バックアップや再委託先を含むデータ残存も事前の条件に沿って確認する。
総合解説：委託先管理は契約開始から終了までのライフサイクルで考える。終了時チェックリストを用意し、ID、証明書、VPN、APIキー等も漏れなく失効させる。

Q128 5-5 委託・サプライチェーン / 委託先管理

運用委託先が本番環境へ管理者アクセスする方式を見直す。最も適切な管理はどれか。
ア．委託先全社員で共通の管理者IDを共有する。
イ．緊急時に便利なので、退職者を含む過去担当者の権限も残す。
ウ．接続元や操作ログを記録せず、委託先の自主性に任せる。
エ．業務上必要な担当者に限定し、多要素認証、期限付き又は申請承認型の特権付与、操作ログを組み合わせる。

正答・4肢解説・総合解説

正答：エ．業務上必要な担当者に限定し、多要素認証、期限付き又は申請承認型の特権付与、操作ログを組み合わせる。
ア：共有IDは責任追跡を難しくし、資格情報の漏えいリスクも高める。
イ：不要権限は速やかに削除する。
ウ：操作記録がなければ異常検知や事後調査が難しくなる。
エ：委託先アクセスも最小権限・強い認証・特権管理・監査証跡の対象とする。
総合解説：委託先だから特権管理を弱めるのではなく、外部主体であることを踏まえ、接続時間・対象・作業内容を必要最小限にする。

Q129 5-5 委託・サプライチェーン / 委託先管理

長年利用しているSaaS事業者が、重要な処理を新しいサブプロセッサへ移すと通知してきた。委託元の対応として最も適切なものはどれか。
ア．データの取扱い、地域、セキュリティ管理、再委託条件などへの影響を評価し、必要に応じ契約・管理策を見直す。
イ．既存ベンダなので、委託構造の変更はリスク評価に影響しない。
ウ．サブプロセッサは契約相手ではないため、どのような変更でも無条件で受け入れる。
エ．変更通知を受けた記録を削除し、評価を行わない。

正答・4肢解説・総合解説

正答：ア．データの取扱い、地域、セキュリティ管理、再委託条件などへの影響を評価し、必要に応じ契約・管理策を見直す。
ア：重要な再委託・処理場所等の変更は、リスク、法令、責任分界に影響し得るため再評価する。
イ：長期利用実績があっても環境変化を無視できない。
ウ：直接契約がなくても自組織のデータ処理依存関係として重要である。
エ：変更管理の証跡を残し、必要な意思決定を記録する。
総合解説：継続的委託先管理では、事故だけでなく、買収、サービス構成変更、再委託先変更、データ所在地変更などをトリガとして再評価する。

Q130 5-5 委託・サプライチェーン / 委託先管理

多数の委託先を同じ頻度・同じ深さで評価しており、管理工数が不足している。改善策として最も適切なものはどれか。
ア．全委託先の評価を停止して、事故が起きた先だけ調査する。
イ．扱う情報、業務重要度、接続権限、代替可能性などで委託先をリスク階層化し、高リスク先へ監視資源を重点配分する。
ウ．委託金額が小さい先は、機密データを扱っていても評価対象外とする。
エ．認証取得の有無だけで全ての委託リスクを一律判定する。

正答・4肢解説・総合解説

正答：イ．扱う情報、業務重要度、接続権限、代替可能性などで委託先をリスク階層化し、高リスク先へ監視資源を重点配分する。
ア：事後対応だけでは予防・早期検知ができない。
イ：リスクベースで評価強度を変えることで、限られた資源を重要な依存先へ集中できる。
ウ：委託金額と情報・業務リスクは必ずしも一致しない。
エ：認証は有力な証拠の一つだが、サービス範囲や自社固有要件も確認する。
総合解説：リスク階層は固定せず、サービス変更、インシデント、重要度上昇などに応じて見直す。評価頻度・証跡・承認権限を階層ごとに標準化すると運用しやすい。

Q131 5-5 委託・サプライチェーン / 委託先管理

委託先がISO/IEC 27001認証を取得していることを確認した。委託元の判断として最も適切なものはどれか。
ア．認証取得済みなら、委託契約のセキュリティ要件を全て削除する。
イ．認証があれば、インシデント報告や再委託管理の確認は不要である。
ウ．認証の適用範囲や自社サービスとの関係を確認し、認証を有力な証拠の一つとして使いつつ、自社固有のリスクも評価する。
エ．認証範囲を確認せず、会社全体の全サービスが同じ管理下だとみなす。

正答・4肢解説・総合解説

正答：ウ．認証の適用範囲や自社サービスとの関係を確認し、認証を有力な証拠の一つとして使いつつ、自社固有のリスクも評価する。
ア：自社固有の責任分界や法令・データ条件は契約で別途明確化する。
イ：事故報告や再委託等の運用要件は認証だけでは自動的に定まらない。
ウ：第三者認証は有用だが、適用範囲と自組織が利用するサービスの一致を確認する必要がある。
エ：スコープ外の拠点・サービスがある可能性があるため確認が必要である。
総合解説：第三者評価を「免罪符」にせず、監査報告書、認証範囲、例外事項、契約条項、サービス実態を組み合わせて判断する。

Q132 5-5 委託・サプライチェーン / 委託先管理

基幹業務を単一のクラウド委託先へ全面依存しており、代替手段がない。委託先管理上の重要なリスクとして最も適切なものはどれか。
ア．一社へ集約すれば管理対象が減るため、可用性リスクは必ずゼロになる。
イ．クラウド契約がある限り、事業撤退やサービス終了は考慮不要である。
ウ．セキュリティ事故だけを想定し、経営・供給・災害による停止は委託リスクに含めない。
エ．委託先の長期停止や事業撤退が自社業務へ直結する集中リスクがあるため、復旧・代替・退出計画を検討する。

正答・4肢解説・総合解説

正答：エ．委託先の長期停止や事業撤退が自社業務へ直結する集中リスクがあるため、復旧・代替・退出計画を検討する。
ア：集約は管理面の利点があっても集中リスクを自動的に消さない。
イ：サービス終了や経営変化もライフサイクル上のリスクである。
ウ：委託リスクにはサイバー攻撃だけでなく、供給能力や継続性も含めて考える。
エ：特定供給者への過度な依存は単一障害点となり、供給停止・障害・撤退時の影響を増幅する。
総合解説：重要サービスでは、RTO/RPOだけでなく、データ移行性、設定・ログの持出し、代替サービス、契約解除時の支援など退出可能性を確認する。

Q133 5-5 委託・サプライチェーン / サプライチェーンリスク

信頼しているソフトウェアベンダの正規更新サーバが侵害され、悪意あるコードを含む更新プログラムが配布された。この攻撃の特徴として最も適切なものはどれか。
ア．信頼された供給経路を悪用して利用組織へ侵入するサプライチェーン攻撃である。
イ．利用者が必ずフィッシングメールを開くことを前提とする攻撃である。
ウ．自社の公開Webサーバだけを直接狙うDDoS攻撃である。
エ．物理的盗難だけを利用する攻撃である。

正答・4肢解説・総合解説

正答：ア．信頼された供給経路を悪用して利用組織へ侵入するサプライチェーン攻撃である。
ア：供給者の開発・配布・更新経路が侵害されると、正規チャネルへの信頼を攻撃者に悪用される。
イ：フィッシングを伴わないサプライチェーン攻撃もある。
ウ：DDoSとは攻撃経路・目的が異なる。
エ：ソフトウェア供給網への侵害は物理盗難に限られない。
総合解説：サプライチェーン攻撃では、自社の境界防御だけでなく、供給者の開発プロセス、更新署名、SBOM、異常検知、分離・最小権限など多層対策が必要になる。

Q134 5-5 委託・サプライチェーン / サプライチェーンリスク

SBOM（Software Bill of Materials）の主な活用目的として最も適切なものはどれか。
ア．SBOMが存在すれば、そのソフトウェアに脆弱性が一切ないことを証明できる。
イ．ソフトウェアを構成する部品や依存関係を把握し、脆弱性や影響範囲の特定を迅速化する。
ウ．SBOMはネットワーク通信を暗号化するための鍵一覧である。
エ．SBOMはインシデントを自動的に復旧させるバックアップ形式である。

正答・4肢解説・総合解説

正答：イ．ソフトウェアを構成する部品や依存関係を把握し、脆弱性や影響範囲の特定を迅速化する。
ア：部品表は安全性の絶対保証ではなく、脆弱性評価や対応を支援する情報である。
イ：SBOMは構成要素の可視性を高め、脆弱なコンポーネント利用の有無を調べる基礎情報になる。
ウ：暗号鍵管理のための一覧ではない。
エ：バックアップそのものではなく、ソフトウェア構成管理の情報である。
総合解説：SBOMの価値は「作ること」ではなく、脆弱性情報と突合し、影響分析、更新判断、供給者への問い合わせに継続利用することにある。

Q135 5-5 委託・サプライチェーン / サプライチェーンリスク

供給されたソフトウェアのデジタル署名を検証する主な目的として最も適切なものはどれか。
ア．署名が有効なら、ソフトウェアに設計上の脆弱性がないことを保証する。
イ．署名検証に成功すれば、ライセンス条件や法令適合性も全て保証される。
ウ．配布元の真正性と、署名後に内容が改変されていないことの確認を支援する。
エ．署名はソフトウェア内の全OSS部品の一覧を示す。

正答・4肢解説・総合解説

正答：ウ．配布元の真正性と、署名後に内容が改変されていないことの確認を支援する。
ア：正規に署名されたソフトウェアにも脆弱性や悪意ある機能が存在する可能性はある。
イ：署名は法務・ライセンス適合性の総合保証ではない。
ウ：デジタル署名は、発行主体と改ざん検知の確認に役立つ。
エ：部品一覧を提供する役割はSBOM等が担う。
総合解説：サプライチェーン対策では、署名検証、配布経路保護、SBOM、脆弱性情報、挙動監視など複数の証拠を組み合わせて信頼性を高める。

Q136 5-5 委託・サプライチェーン / サプライチェーンリスク

自社アプリが直接利用していないライブラリCに脆弱性が見つかった。アプリはライブラリAを利用し、AがBを、BがCを依存関係として利用している。対応として最も適切なものはどれか。
ア．自社がCを直接指定していないので、必ず影響はない。
イ．脆弱性がCにあるため、AやBのバージョン情報を確認する必要はない。
ウ．SBOMにCが記載されていても、脆弱性情報との照合は不要である。
エ．推移的依存関係を含めてCが実際に組み込まれているか、到達可能性や影響を確認し、必要な更新・緩和策を行う。

正答・4肢解説・総合解説

正答：エ．推移的依存関係を含めてCが実際に組み込まれているか、到達可能性や影響を確認し、必要な更新・緩和策を行う。
ア：直接利用していないことは影響なしの証明にならない。
イ：依存関係のバージョン・更新経路を確認して対応可能な版を特定する。
ウ：SBOMは脆弱性情報と突合して初めて迅速な影響分析に役立つ。
エ：サプライチェーンでは直接依存だけでなく推移的依存がリスクとなるため、実際の構成と利用経路を確認する。
総合解説：OSS依存関係は深くなるほど可視性が低下しやすい。ビルド時のロックファイルやSBOMを更新し、継続的な脆弱性監視につなげる。

Q137 5-5 委託・サプライチェーン / サプライチェーンリスク

NIST SP 800-161 Rev.1 Update 1が扱うC-SCRMのリスク例として最も適切なものはどれか。
ア．供給された製品・サービスに悪意ある機能、偽造品、脆弱な開発・製造に起因する弱点が含まれるリスクである。
イ．従業員の通勤時間だけを最適化するリスクである。
ウ．広告デザインの好みだけを評価するリスクである。
エ．サプライヤとは無関係に為替レートだけを予測するリスクである。

正答・4肢解説・総合解説

正答：ア．供給された製品・サービスに悪意ある機能、偽造品、脆弱な開発・製造に起因する弱点が含まれるリスクである。
ア：C-SCRMは、供給網を通じて持ち込まれる悪意ある機能、偽造、脆弱性、品質・完全性問題などを対象とする。
イ：通勤時間の最適化はC-SCRMの中心ではない。
ウ：広告デザインの嗜好はサイバー供給網リスクとは異なる。
エ：経済リスクが調達に影響する場合はあるが、C-SCRMの代表的なセキュリティ課題を説明していない。
総合解説：供給網リスクはソフトウェアだけではなく、ハードウェア、サービス、開発・運用プロセス、人・組織など複数階層にまたがる。

Q138 5-5 委託・サプライチェーン / サプライチェーンリスク

サプライチェーンリスク管理を「調達時の一回限りのチェック」にしてはいけない主な理由として最も適切なものはどれか。
ア．調達後はサプライヤの環境が法律で固定され、変化しないから。
イ．供給者、依存部品、脆弱性、サービス構成、所有関係などが契約期間中にも変化するため、継続的な監視と再評価が必要だから。
ウ．契約書には変更が起きないことが自動的に保証されるから。
エ．一度のチェックで将来のゼロデイ脆弱性まで全て検出できるから。

正答・4肢解説・総合解説

正答：イ．供給者、依存部品、脆弱性、サービス構成、所有関係などが契約期間中にも変化するため、継続的な監視と再評価が必要だから。
ア：供給者環境が固定されるという前提は現実的でない。
イ：供給網は動的であり、M&A、再委託、部品更新、新規脆弱性等によりリスク状態が変わる。
ウ：契約は変更管理を求める手段にはなるが、変化そのものを完全に防げない。
エ：将来未知の脆弱性を一度の評価で全て検出することはできない。
総合解説：C-SCRMは、計画、調達、導入、運用、変更、廃棄までライフサイクルへ統合する。重要な変更やインシデントを再評価トリガにする。

Q139 5-5 委託・サプライチェーン / サプライチェーンリスク

複数の重要サービスが実は同じ下位クラウド事業者に依存していることが判明した。最も適切なリスク評価はどれか。
ア．契約先が複数なら、下位依存先が同じでも必ず完全冗長になる。
イ．一次ベンダが異なれば、サプライチェーンの共通依存を調べる必要はない。
ウ．見かけ上は複数ベンダでも共通の下位依存先が単一障害点となるため、集中リスクとして評価する。
エ．下位依存は自社と直接契約がないため、事業継続には影響しない。

正答・4肢解説・総合解説

正答：ウ．見かけ上は複数ベンダでも共通の下位依存先が単一障害点となるため、集中リスクとして評価する。
ア：契約先の数だけで実際の技術的冗長性は判断できない。
イ：四次・五次の依存先でも重要なら把握対象になり得る。
ウ：共通の下位サービス障害が複数サービスへ同時波及する可能性があり、集中リスクとなる。
エ：直接契約がなくても、停止時には自社業務へ影響が及ぶ。
総合解説：サプライチェーンの可視化では「会社名の多さ」ではなく、実際の基盤・部品・サービスの共通依存を確認する。BCPや代替策にも反映する。

Q140 5-5 委託・サプライチェーン / サプライチェーンリスク

取引先VPNから自社ネットワークへ侵入された場合の被害拡大を抑えるサプライチェーン対策として最も適切なものはどれか。
ア．取引先は信頼済みなので、VPN接続後は社内全セグメントへ無制限アクセスを許可する。
イ．取引先専用アカウントは複数社で共用し、利用者を識別しない。
ウ．接続ログを保存せず、異常通信の監視もしない。
エ．取引先接続を必要なシステム・通信だけに限定し、強い認証、セグメンテーション、監視を適用する。

正答・4肢解説・総合解説

正答：エ．取引先接続を必要なシステム・通信だけに限定し、強い認証、セグメンテーション、監視を適用する。
ア：信頼関係があっても取引先環境が侵害される可能性はある。
イ：共有アカウントは追跡性を低下させる。
ウ：ログと監視がなければ侵入の検知・調査が難しい。
エ：サプライチェーン経由の侵害を前提に、接続後の権限と到達範囲を最小化して被害半径を抑える。
総合解説：「信頼する取引先だから広く許可する」のではなく、接続単位で認証・認可し、必要に応じてネットワーク分離やジャンプサーバを利用する。

Q141 5-5 委託・サプライチェーン / サプライチェーンリスク

ソフトウェア供給者のセキュリティを評価する際、「完成品の脆弱性スキャン結果だけ」では不十分と考える理由として最も適切なものはどれか。
ア．供給網リスクには、開発環境・ビルド・署名・配布・依存部品・脆弱性対応などライフサイクル全体のプロセスが影響するから。
イ．完成品スキャンは法令で全面禁止されているから。
ウ．サプライチェーンリスクはソフトウェア開発とは無関係だから。
エ．供給者の開発プロセスは、製品の完全性や脆弱性に影響しないから。

正答・4肢解説・総合解説

正答：ア．供給網リスクには、開発環境・ビルド・署名・配布・依存部品・脆弱性対応などライフサイクル全体のプロセスが影響するから。
ア：最終成果物だけでは、ビルドパイプライン侵害や依存部品、署名鍵管理等のリスクを十分に見抜けない。
イ：脆弱性スキャンは有用な一手段であり、全面禁止ではない。
ウ：開発・供給プロセスはサプライチェーンリスクの中心である。
エ：開発プロセスの品質と完全性は製品リスクに直結する。
総合解説：供給者評価では、セキュア開発、変更管理、脆弱性受付、パッチ提供、署名・配布経路、SBOMなどを組み合わせて確認する。

Q142 5-5 委託・サプライチェーン / 調達・契約・セキュリティ要件

新しいIT製品を調達する際、セキュリティ要件を定義する手順として最も適切なものはどれか。
ア．製品を購入した後で初めて、どの情報を扱うかを確認する。
イ．利用環境、保護対象、想定脅威、必要な保証水準を整理し、調達仕様へ検証可能なセキュリティ要件として落とし込む。
ウ．最安価格の製品を先に決定し、セキュリティ要件は設定しない。
エ．他社の要件表を利用環境の違いを確認せずそのままコピーする。

正答・4肢解説・総合解説

正答：イ．利用環境、保護対象、想定脅威、必要な保証水準を整理し、調達仕様へ検証可能なセキュリティ要件として落とし込む。
ア：購入後では要件を満たす製品を選ぶ機会を失う。
イ：調達要件は、自組織の利用環境と脅威分析を起点に定義し、選定・受入れで確認できる形にする。
ウ：価格だけでなくリスクとセキュリティを調達判断へ含める。
エ：テンプレートは参考になるが、自組織の環境・重要度に合わせて調整する。
総合解説：調達時にセキュリティ要件を明確化すると、見積比較、契約、受入試験、運用、更新まで一貫した管理がしやすい。

Q143 5-5 委託・サプライチェーン / 調達・契約・セキュリティ要件

調達仕様書に記載するセキュリティ要件として、受入れ時に最も検証しやすいものはどれか。
ア．できるだけ安全であること。
イ．業界最高水準のセキュリティであること。
ウ．管理者認証は多要素認証に対応し、監査ログには利用者ID・日時・操作結果を記録し、指定期間保持できること。
エ．重大事故が絶対に発生しないこと。

正答・4肢解説・総合解説

正答：ウ．管理者認証は多要素認証に対応し、監査ログには利用者ID・日時・操作結果を記録し、指定期間保持できること。
ア：「できるだけ」は基準が曖昧で合否判定が困難である。
イ：「最高水準」は比較基準が不明確で、契約解釈がぶれやすい。
ウ：具体的な機能・記録項目・保持条件などを記載すると試験や証跡で確認しやすい。
エ：絶対に事故が起きないという要求は現実的に検証できない。
総合解説：セキュリティ要件は、MUST/SHOULD等の優先度、受入基準、証跡、例外承認手続まで定義すると調達後の争いを減らせる。

Q144 5-5 委託・サプライチェーン / 調達・契約・セキュリティ要件

重要システムの運用委託契約で、インシデント対応を実効的にする要件として最も適切なものはどれか。
ア．契約期間中のインシデントは委託先だけの問題とし、委託元への報告を禁止する。
イ．事故対応は担当者の善意に任せ、連絡方法や報告情報を決めない。
ウ．全ての事故について最終報告だけを契約終了日に提出させる。
エ．重大度に応じた初報条件、連絡先、提供情報、ログ・証拠の保全、調査協力、復旧・再発防止報告を定める。

正答・4肢解説・総合解説

正答：エ．重大度に応じた初報条件、連絡先、提供情報、ログ・証拠の保全、調査協力、復旧・再発防止報告を定める。
ア：委託元の業務や法令義務に影響するため報告が必要である。
イ：善意ではなく手順・契約・連絡網として固定する。
ウ：初報と継続報告が必要で、契約終了時では遅すぎる。
エ：有事の役割と情報共有を事前に定めることで、初動と法令・顧客対応を迅速化できる。
総合解説：報告条項は、何を「インシデント」とするか、いつ時計が始まるか、初報に最低限含める項目まで定めると運用しやすい。

Q145 5-5 委託・サプライチェーン / 調達・契約・セキュリティ要件

長期間利用するネットワーク機器の調達条件として、脆弱性管理の観点から最も適切なものはどれか。
ア．脆弱性情報の提供方法、セキュリティ更新の提供期間、更新手順、サポート終了通知などを確認・契約条件化する。
イ．購入時点で既知脆弱性がなければ、その後の更新提供は不要とする。
ウ．EOL後も更新が永久に提供されると仮定し、終了条件を確認しない。
エ．脆弱性情報は利用者に知らせないことを契約条件にする。

正答・4肢解説・総合解説

正答：ア．脆弱性情報の提供方法、セキュリティ更新の提供期間、更新手順、サポート終了通知などを確認・契約条件化する。
ア：長期利用製品では、導入後に発見される脆弱性への対応能力とサポート期間が重要である。
イ：未知脆弱性は将来発見され得るため、購入時点だけの確認では不足する。
ウ：サポート終了時期を把握し、更新・更改計画へ反映する。
エ：脆弱性情報の適切な提供は利用者のリスク対応を支える。
総合解説：調達段階でセキュリティサポート期間を確認すると、EOL直前の慌ただしい更改や未修正機器の長期使用を避けやすい。

Q146 5-5 委託・サプライチェーン / 調達・契約・セキュリティ要件

ソフトウェア調達でSBOMの提供を要件に含める狙いとして最も適切なものはどれか。
ア．SBOM提出だけで、受入試験や脆弱性管理を全て不要にする。
イ．利用組織が構成部品を把握し、脆弱性発生時の影響確認や供給者との対応を迅速化できるようにする。
ウ．SBOMを秘密鍵の代わりに使ってソフトウェアへ署名する。
エ．SBOMがあれば、全てのOSSライセンス問題とセキュリティ問題が自動解決する。

正答・4肢解説・総合解説

正答：イ．利用組織が構成部品を把握し、脆弱性発生時の影響確認や供給者との対応を迅速化できるようにする。
ア：SBOMは重要な情報源だが、テストや監視を代替するものではない。
イ：SBOMは構成要素の可視性を高め、継続的な脆弱性管理に活用できる。
ウ：署名鍵とは役割が異なる。
エ：部品情報を基に別途ライセンス・脆弱性評価が必要で、自動解決を保証しない。
総合解説：SBOM要件では、形式、更新タイミング、対象範囲、脆弱性通知との連携を定めると実務利用しやすい。

Q147 5-5 委託・サプライチェーン / 調達・契約・セキュリティ要件

重要ソフトウェアの調達で、供給者のセキュア開発能力を評価するための証拠として最も適切な組合せはどれか。
ア．企業ロゴと広告文だけを確認する。
イ．売上高が高いことだけを根拠に、開発プロセスの確認を省略する。
ウ．開発・ビルドのアクセス管理、コードレビューやテスト、脆弱性受付・修正プロセス、署名・リリース管理などの実施証跡を確認する。
エ．営業担当者の口頭で「安全」と聞くだけで合格とする。

正答・4肢解説・総合解説

正答：ウ．開発・ビルドのアクセス管理、コードレビューやテスト、脆弱性受付・修正プロセス、署名・リリース管理などの実施証跡を確認する。
ア：ブランド表示は開発プロセスの安全性を示す証拠にならない。
イ：企業規模は参考情報に過ぎず、開発統制の確認を代替しない。
ウ：供給者のセキュア開発は、実際のプロセスと証跡で評価することが重要である。
エ：口頭説明だけでなく、手順・結果・第三者評価等の客観的証跡を求める。
総合解説：調達時には製品機能だけでなく、脆弱性が見つかった後に供給者がどのように受け付け、評価し、修正し、通知するかも確認する。

Q148 5-5 委託・サプライチェーン / 調達・契約・セキュリティ要件

一次委託先が再委託を利用する可能性があるシステム開発契約で、セキュリティ要件をサプライチェーンへ波及させる方法として最も適切なものはどれか。
ア．一次委託先だけが要件を守れば、再委託先には一切の要求をしない。
イ．再委託先の事故は必ず一次委託先で遮断されるため、報告条項は不要とする。
ウ．再委託先を増やすほど安全になると仮定し、管理対象から除外する。
エ．重要なセキュリティ要求を再委託先にも適用すること、再委託条件や変更通知、委託元が確認できる仕組みを契約に定める。

正答・4肢解説・総合解説

正答：エ．重要なセキュリティ要求を再委託先にも適用すること、再委託条件や変更通知、委託元が確認できる仕組みを契約に定める。
ア：一次委託先だけの統制では、下位委託先のリスクを十分に管理できない場合がある。
イ：下位委託先の事故も自社へ波及し得るため報告・連携が必要である。
ウ：再委託先の数が増えるほど可視性・複雑性のリスクが高まる場合がある。
エ：フローダウンにより、実際にデータや開発環境へアクセスする再委託先にも必要な管理策を及ぼす。
総合解説：全ての要件を機械的に同じ形で流すのではなく、扱うデータ・権限・重要性に応じて必須要件と証跡を定義する。

Q149 5-5 委託・サプライチェーン / 調達・契約・セキュリティ要件

クラウドサービスを調達する際、契約終了時のデータ管理要件として最も適切なものはどれか。
ア．データのエクスポート方法、返却・削除、バックアップや再委託先に残るデータの扱い、削除確認方法を定める。
イ．契約終了後のデータはサービス事業者が自由に利用できるとする。
ウ．本番画面から消えれば、バックアップ等の残存は一切確認しない。
エ．データ移行性や削除方法は、契約終了時まで確認しない。

正答・4肢解説・総合解説

正答：ア．データのエクスポート方法、返却・削除、バックアップや再委託先に残るデータの扱い、削除確認方法を定める。
ア：退出時のデータ移行・削除は、機密性・法令・事業継続に直結するため調達時から要件化する。
イ：契約・法令に反する自由利用は認められない。
ウ：バックアップや再委託先の残存も条件に応じて確認する。
エ：終了時に初めて確認すると、移行不能や高額な退出コストが判明するおそれがある。
総合解説：出口戦略はベンダロックインとデータ残存リスクの双方に関係する。可搬形式、移行支援、削除証明、保存期間等を確認する。

Q150 5-5 委託・サプライチェーン / 調達・契約・セキュリティ要件

重要なICT/OT製品の調達で、価格だけを最優先してセキュリティ評価をほぼ行わない方針を評価したものとして最も適切なものはどれか。
ア．安価な製品ほど攻撃者の関心が低いため、セキュリティ評価は不要である。
イ．ミッション重要度やデータ機密性、運用環境、供給網リスクを考慮し、価格とともにセキュリティを調達判断へ組み込むべきである。
ウ．調達後に脆弱性が判明しても、価格が安ければ総コストは必ず低くなる。
エ．セキュリティは運用部門だけの問題なので、調達時に考慮する必要はない。

正答・4肢解説・総合解説

正答：イ．ミッション重要度やデータ機密性、運用環境、供給網リスクを考慮し、価格とともにセキュリティを調達判断へ組み込むべきである。
ア：価格と攻撃対象性にそのような単純な関係はない。
イ：重要製品では供給網リスクを含むセキュリティを調達ライフサイクルへ統合する必要がある。
ウ：事故対応・停止・更改・法令対応を含むライフサイクルコストが増える可能性がある。
エ：調達仕様の段階で要求しなければ、後から実装できない安全機能もある。
総合解説：NIST SP 800-161は、ICT/OT調達でセキュリティを重要な意思決定要素として扱うことを示している。日本の調達要件リストも利用環境の脅威分析から要件を定義する考え方を取る。