情報セキュリティマネジメント試験　科目A・B
サンプル問題

試験時間	120分
問題番号	問1～問60
選択方法	全問必須

問１　JIS Q 27001:2014（情報セキュリティマネジメントシステム－要求事項）において，リスクを受容するプロセスに求められるものはどれか。

ア　受容するリスクについては，リスク所有者が承認すること
イ　受容するリスクを監視やレビューの対象外とすること
ウ　リスクの受容は，リスク分析前に行うこと
エ　リスクを受容するかどうかは，リスク対応後に決定すること

問２　退職する従業員による不正を防ぐための対策のうち，IPA“組織における内部不正防止ガイドライン（第５版）”に照らして，適切なものはどれか。

ア　在職中に知り得た重要情報を退職後に公開しないように，退職予定者に提出させる秘密保持誓約書には，秘密保持の対象を明示せず，重要情報を客観的に特定できないようにしておく。
イ　退職後，同業他社に転職して重要情報を漏らすということがないように，職業選択の自由を行使しないことを明記した上で，具体的な範囲を設定しない包括的な競業避止義務契約を入社時に締結する。
ウ　退職者による重要情報の持出しなどの不正行為を調査できるように，従業員に付与した利用者 ID や権限は退職後も有効にしておく。
エ　退職間際に重要情報の不正な持出しが行われやすいので，退職予定者に対する重要情報へのアクセスや媒体の持出しの監視を強化する。

問３　JIS Q 27000:2019（情報セキュリティマネジメントシステム－用語）において，不適合が発生した場合にその原因を除去し，再発を防止するためのものとして定義されているものはどれか。

ア　継続的改善　　イ　修正
ウ　是正処置　　エ　リスクアセスメント

問４　JIS Q 27002:2014（情報セキュリティ管理策の実践のための規範）の“サポートユーティリティ”に関する例示に基づいて，サポートユーティリティと判断されるものはどれか。

ア　サーバ室の空調　　イ　サーバの保守契約
ウ　特権管理プログラム　　エ　ネットワーク管理者

問５　JIS Q 27000:2019（情報セキュリティマネジメントシステム－用語）における“リスクレベル”の定義はどれか。

ア　脅威によって付け込まれる可能性のある，資産又は管理策の弱点
イ　結果とその起こりやすさの組合せとして表現される，リスクの大きさ
ウ　対応すべきリスクに付与する優先順位
エ　リスクの重大性を評価するために目安とする条件

問６　サイバーセキュリティ基本法に基づき，内閣にサイバーセキュリティ戦略本部が設置されたのと同時に，内閣官房に設置された組織はどれか。

ア　IPA　　イ　JIPDEC　　ウ　JPCERT/CC　　エ　NISC

問７　CRYPTREC の役割として，適切なものはどれか。

ア　外国為替及び外国貿易法で規制されている暗号装置の輸出許可申請を審査，承認する。
イ　政府調達において IT 関連製品のセキュリティ機能の適切性を評価，認証する。
ウ　電子政府での利用を推奨する暗号技術の安全性を評価，監視する。
エ　民間企業のサーバに対するセキュリティ攻撃を監視，検知する。

問８　緊急事態を装って組織内部の人間からパスワードや機密情報を入手する不正な行為は，どれに分類されるか。

ア　ソーシャルエンジニアリング　　イ　トロイの木馬
ウ　踏み台攻撃　　エ　ブルートフォース攻撃

問９　A 社では現在，インターネット上の Web サイトを内部ネットワークの PC 上の Web ブラウザから参照している。新たなシステムを導入し，DMZ 上に用意した VDI（Virtual Desktop Infrastructure）サーバに PC からログインし，インターネット上の Web サイトを VDI サーバ上の仮想デスクトップの Web ブラウザから参照するように変更する。この変更によって期待できるセキュリティ上の効果はどれか。

ア　インターネット上の Web サイトから，内部ネットワークの PC へのマルウェアのダウンロードを防ぐ。
イ　インターネット上の Web サイト利用時に，MITB 攻撃による送信データの改ざんを防ぐ。
ウ　内部ネットワークの PC 及び仮想デスクトップの OS がボットに感染しなくなり，C&C サーバにコントロールされることを防ぐ。
エ　内部ネットワークの PC にマルウェアが侵入したとしても，他の PC に感染するのを防ぐ。

問10　デジタルフォレンジックスでハッシュ値を利用する目的として，適切なものはどれか。

ア　一方向性関数によってパスワードを復元できないように変換して保存する。
イ　改変されたデータを，証拠となり得るように復元する。
ウ　証拠となり得るデータについて，原本と複製の同一性を証明する。
エ　パスワードの盗聴の有無を検証する。

問11　利用者 PC の内蔵ストレージが暗号化されていないとき，攻撃者が利用者 PC から内蔵ストレージを抜き取り，攻撃者が用意した PC に接続して内蔵ストレージ内の情報を盗む攻撃の対策に該当するものはどれか。

ア　内蔵ストレージにインストールした OS の利用者アカウントに対して，ログインパスワードを設定する。

イ　内蔵ストレージに保存したファイルの読取り権限を，ファイルの所有者だけに付与する。

ウ　利用者 PC 上で HDD パスワードを設定する。

エ　利用者 PC に BIOS パスワードを設定する。

問12　ルートキットの特徴はどれか。

ア　OS などに不正に組み込んだツールの存在を隠す。

イ　OS の中核であるカーネル部分の脆弱性を分析する。

ウ　コンピュータがマルウェアに感染していないことをチェックする。

エ　コンピュータやルータのアクセス可能な通信ポートを外部から調査する。

問13　BEC（Business E-mail Compromise）に該当するものはどれか。

ア　巧妙なだましの手口を駆使し，取引先になりすまして偽の電子メールを送り，金銭をだまし取る。

イ　送信元を攻撃対象の組織のメールアドレスに詐称し，多数の実在しないメールアドレスに一度に大量の電子メールを送り，攻撃対象の組織のメールアドレスを故意にブラックリストに登録させて，利用を阻害する。

ウ　第三者からの電子メールが中継できるように設定されたメールサーバを，スパムメールの中継に悪用する。

エ　誹謗（ひぼう）中傷メールの送信元を攻撃対象の組織のメールアドレスに詐称し，組織の社会的な信用を大きく損なわせる。

問14　ボットネットにおける C&C サーバの役割として，適切なものはどれか。

ア　Web サイトのコンテンツをキャッシュし，本来のサーバに代わってコンテンツを利用者に配信することによって，ネットワークやサーバの負荷を軽減する。

イ　外部からインターネットを経由して社内ネットワークにアクセスする際に，CHAP などのプロトコルを中継することによって，利用者認証時のパスワードの盗聴を防止する。

ウ　外部からインターネットを経由して社内ネットワークにアクセスする際に，時刻同期方式を採用したワンタイムパスワードを発行することによって，利用者認証時のパスワードの盗聴を防止する。

エ　侵入して乗っ取ったコンピュータに対して，他のコンピュータへの攻撃などの不正な操作をするよう，外部から命令を出したり応答を受け取ったりする。

問15　PC への侵入に成功したマルウェアがインターネット上の指令サーバと通信を行う場合に，宛先ポートとして使用される TCP ポート番号 80 に関する記述のうち，適切なものはどれか。

ア　DNS のゾーン転送に使用されることから，通信がファイアウォールで許可されている可能性が高い。

イ　Web サイトの HTTPS 通信での閲覧に使用されることから，マルウェアと指令サーバとの間の通信が侵入検知システムで検知される可能性が低い。

ウ　Web サイトの閲覧に使用されることから，通信がファイアウォールで許可されている可能性が高い。

エ　ドメイン名の名前解決に使用されることから，マルウェアと指令サーバとの間の通信が侵入検知システムで検知される可能性が低い。

問16　特定のサービスやシステムから流出した認証情報を攻撃者が用いて，認証情報を複数のサービスやシステムで使い回している利用者のアカウントへのログインを試みる攻撃はどれか。

ア　パスワードリスト攻撃　　イ　ブルートフォース攻撃

ウ　リバースブルートフォース攻撃　　エ　レインボーテーブル攻撃

問17　攻撃者が用意したサーバ X の IP アドレスが，A 社 Web サーバの FQDN に対応する IP アドレスとして，B 社 DNS キャッシュサーバに記憶された。これによって，意図せずサーバ X に誘導されてしまう利用者はどれか。ここで，A 社，B 社の各従業員は自社の DNS キャッシュサーバを利用して名前解決を行う。

ア　A 社 Web サーバにアクセスしようとする A 社従業員
イ　A 社 Web サーバにアクセスしようとする B 社従業員
ウ　B 社 Web サーバにアクセスしようとする A 社従業員
エ　B 社 Web サーバにアクセスしようとする B 社従業員

問18　攻撃者が，多数のオープンリゾルバに対して，“あるドメイン”の実在しないランダムなサブドメインを多数問い合わせる攻撃（ランダムサブドメイン攻撃）を仕掛け，多数のオープンリゾルバが応答した。このときに発生する事象はどれか。

ア　“あるドメイン”を管理する権威 DNS サーバに対して負荷が掛かる。
イ　“あるドメイン”を管理する権威 DNS サーバに登録されている DNS 情報が改ざんされる。
ウ　オープンリゾルバが保持する DNS キャッシュに不正な値を注入される。
エ　オープンリゾルバが保持するゾーン情報を不正に入手される。

問19　SEO ポイズニングの説明はどれか。

ア　Web 検索サイトの順位付けアルゴリズムを悪用して，検索結果の上位に，悪意のある Web サイトを意図的に表示させる。

イ　車などで移動しながら，無線 LAN のアクセスポイントを探し出して，ネットワークに侵入する。

ウ　ネットワークを流れるパケットから，侵入のパターンに合致するものを検出して，管理者への通知や，検出した内容の記録を行う。

エ　マルウェア対策ソフトのセキュリティ上の脆弱性を悪用して，システム権限で不正な処理を実行させる。

問20　データベースで管理されるデータの暗号化に用いることができ，かつ，暗号化と復号とで同じ鍵を使用する暗号方式はどれか。

ア　AES　　イ　PKI　　ウ　RSA　　エ　SHA-256

問21　OpenPGP や S/MIME において用いられるハイブリッド暗号方式の特徴はどれか。

ア　暗号通信方式として IPsec と TLS を選択可能にすることによって利用者の利便性を高める。

イ　公開鍵暗号方式と共通鍵暗号方式を組み合わせることによって鍵管理コストと処理性能の両立を図る。

ウ　複数の異なる共通鍵暗号方式を組み合わせることによって処理性能を高める。

エ　複数の異なる公開鍵暗号方式を組み合わせることによって安全性を高める。

問22　デジタル署名に用いる鍵の組みのうち，適切なものはどれか。

	デジタル署名の作成に用いる鍵	デジタル署名の検証に用いる鍵
ア	共通鍵	秘密鍵
イ	公開鍵	秘密鍵
ウ	秘密鍵	共通鍵
エ	秘密鍵	公開鍵

問23　メッセージが改ざんされていないかどうかを確認するために，そのメッセージから，ブロック暗号を用いて生成することができるものはどれか。

ア　PKI　　イ　パリティビット

ウ　メッセージ認証符号　　エ　ルート証明書

問24　リスクベース認証に該当するものはどれか。

ア　インターネットバンキングでの取引において，取引の都度，乱数表の指定したマス目にある英数字を入力させて認証する。

イ　全てのアクセスに対し，トークンで生成されたワンタイムパスワードを入力させて認証する。

ウ　利用者の IP アドレスなどの環境を分析し，いつもと異なるネットワークからのアクセスに対して追加の認証を行う。

エ　利用者の記憶，持ち物，身体の特徴のうち，必ず二つ以上の方式を組み合わせて認証する。

問25　Web サイトで利用される CAPTCHA に該当するものはどれか。

ア　人からのアクセスであることを確認できるよう，アクセスした者に応答を求め，その応答を分析する仕組み

イ　不正な SQL 文をデータベースに送信しないよう，Web サーバに入力された文字列をプレースホルダに割り当てて SQL 文を組み立てる仕組み

ウ　利用者が本人であることを確認できるよう，Web サイトから一定時間ごとに異なるパスワードを要求する仕組み

エ　利用者が本人であることを確認できるよう，乱数を Web サイト側で生成して利用者に送り，利用者側でその乱数を鍵としてパスワードを暗号化し，Web サイトに送り返す仕組み

問26　HTTP over TLS（HTTPS）を用いて実現できるものはどれか。

ア　Web サーバ上のファイルの改ざん検知

イ　Web ブラウザが動作する PC 上のマルウェア検査

ウ　Web ブラウザが動作する PC に対する侵入検知

エ　デジタル証明書によるサーバ認証

問27　SPF（Sender Policy Framework）を利用する目的はどれか。

ア　HTTP 通信の経路上での中間者攻撃を検知する。

イ　LAN への PC の不正接続を検知する。

ウ　内部ネットワークへの侵入を検知する。

エ　メール送信者のドメインのなりすましを検知する。

問28　電子メールをドメイン A の送信者がドメイン B の宛先に送信するとき，送信者をドメイン A のメールサーバで認証するためのものはどれか。

ア　APOP　　イ　POP3S　　ウ　S/MIME　　エ　SMTP-AUTH

問29　マルウェアの動的解析に該当するものはどれか。

ア　検体のハッシュ値を計算し，オンラインデータベースに登録された既知のマルウェアのハッシュ値のリストと照合してマルウェアを特定する。
イ　検体をサンドボックス上で実行し，その動作や外部との通信を観測する。
ウ　検体をネットワーク上の通信データから抽出し，さらに，逆コンパイルして取得したコードから検体の機能を調べる。
エ　ハードディスク内のファイルの拡張子とファイルヘッダの内容を基に，拡張子が偽装された不正なプログラムファイルを検出する。

問30　Web サーバの検査におけるポートスキャナの利用目的はどれか。

ア　Web サーバで稼働しているサービスを列挙して，不要なサービスが稼働していないことを確認する。
イ　Web サーバの利用者 ID の管理状況を運用者に確認して，情報セキュリティポリシからの逸脱がないことを調べる。
ウ　Web サーバへのアクセスの履歴を解析して，不正利用を検出する。
エ　正規の利用者 ID でログインし，Web サーバのコンテンツを直接確認して，コンテンツの脆弱(ぜい)性を検出する。

問31　個人情報保護委員会“特定個人情報の適正な取扱いに関するガイドライン（事業者編）令和 4 年 3 月一部改正”及びその“Q&A”によれば，事業者によるファイル作成が禁止されている場合はどれか。

なお，“Q&A”とは“「特定個人情報の適正な取扱いに関するガイドライン（事業者編)」及び「(別冊）金融業務における特定個人情報の適正な取扱いに関するガイドライン」に関する Q&A 令和 4 年 4 月 1 日更新”のことである。

ア　システム障害に備えた特定個人情報ファイルのバックアップファイルを作成する場合

イ　従業員の個人番号を利用して業務成績を管理するファイルを作成する場合

ウ　税務署に提出する資料間の整合性を確認するために個人番号を記載した明細表などチェック用ファイルを作成する場合

エ　保険契約者の死亡保険金支払に伴う支払調書ファイルを作成する場合

問32　企業が業務で使用しているコンピュータに，記憶媒体を介してマルウェアを侵入させ，そのコンピュータのデータを消去した者を処罰の対象とする法律はどれか。

ア　刑法　　イ　製造物責任法

ウ　不正アクセス禁止法　　エ　プロバイダ責任制限法

問33　企業が，“特定電子メールの送信の適正化等に関する法律”に定められた特定電子メールに該当する広告宣伝メールを送信する場合に関する記述のうち，適切なものはどれか。

ア　SMS で送信する場合はオプトアウト方式を利用する。

イ　オプトイン方式，オプトアウト方式のいずれかを企業が自ら選択する。

ウ　原則としてオプトアウト方式を利用する。

エ　原則としてオプトイン方式を利用する。

問34　A 社は，B 社と著作物の権利に関する特段の取決めをせず，A 社の要求仕様に基づいて，販売管理システムのプログラム作成を B 社に委託した。この場合のプログラム著作権の原始的帰属に関する記述のうち，適切なものはどれか。

ア　A 社と B 社が話し合って帰属先を決定する。
イ　A 社と B 社の共有帰属となる。
ウ　A 社に帰属する。
エ　B 社に帰属する。

問35　システムテストの監査におけるチェックポイントのうち，最も適切なものはどれか。

ア　テストケースが網羅的に想定されていること
イ　テスト計画は利用者側の責任者だけで承認されていること
ウ　テストは実際に業務が行われている環境で実施されていること
エ　テストは利用者側の担当者だけで行われていること

問36　アクセス制御を監査するシステム監査人の行為のうち，適切なものはどれか。

ア　ソフトウェアに関するアクセス制御の管理台帳を作成し，保管した。
イ　データに関するアクセス制御の管理規程を閲覧した。
ウ　ネットワークに関するアクセス制御の管理方針を制定した。
エ　ハードウェアに関するアクセス制御の運用手続を実施した。

問37　我が国の証券取引所に上場している企業において，内部統制の整備及び運用に最終的な責任を負っている者は誰か。

ア　株主　　イ　監査役　　ウ　業務担当者　　エ　経営者

問38　ヒューマンエラーに起因する障害を発生しにくくする方法に，エラープルーフ化がある。運用作業におけるエラープルーフ化の例として，最も適切なものはどれか。

ア　画面上の複数のウィンドウを同時に使用する作業では，ウィンドウを間違えないようにウィンドウの背景色をそれぞれ異なる色にする。

イ　長時間に及ぶシステム監視作業では，疲労が蓄積しないように，2 時間おきに交代で休憩を取得する体制にする。

ウ　ミスが発生しやすい作業について，過去に発生したヒヤリハット情報を共有して同じミスを起こさないようにする。

エ　臨時の作業を行う際にも落ち着いて作業ができるように，臨時の作業の教育や訓練を定期的に行う。

問39　あるデータセンタでは，受発注管理システムの運用サービスを提供している。次の受発注管理システムの運用中の事象において，インシデントに該当するものはどれか。

〔受発注管理システムの運用中の事象〕

夜間バッチ処理において，注文トランザクションデータから注文書を出力するプログラムが異常終了した。異常終了を検知した運用担当者から連絡を受けた保守担当者は，緊急出社してサービスを回復し，後日，異常終了の原因となったプログラムの誤りを修正した。

ア　異常終了の検知　　イ　プログラムの誤り

ウ　プログラムの異常終了　　エ　保守担当者の緊急出社

問40　ソフトウェア開発プロジェクトにおいてWBSを作成する目的として，適切なものはどれか。

ア　開発の期間と費用とがトレードオフの関係にある場合に，総費用の最適化を図る。
イ　作業の順序関係を明確にして，重点管理すべきクリティカルパスを把握する。
ウ　作業の日程を横棒（バー）で表して，作業の開始時点や終了時点，現時点の進捗を明確にする。
エ　作業を，階層的に詳細化して，管理可能な大きさに細分化する。

問41　プロジェクトの日程計画を作成するのに適した技法はどれか。

ア　PERT　　イ　回帰分析　　ウ　時系列分析　　エ　線形計画法

問42　一方のコンピュータが正常に機能しているときには，他方のコンピュータが待機状態にあるシステムはどれか。

ア　デュアルシステム　　イ　デュプレックスシステム
ウ　マルチプロセッシングシステム　　エ　ロードシェアシステム

問43　データベースの監査ログを取得する目的として，適切なものはどれか。

ア　権限のない利用者のアクセスを拒否する。
イ　チェックポイントからのデータ復旧に使用する。
ウ　データの不正な書換えや削除を事前に検知する。
エ　問題のあるデータベース操作を事後に調査する。

問44　社内ネットワークの PC から，中継装置を経由してインターネット上の Web サーバにアクセスする。中継装置は宛先の Web サーバのドメイン名から DNS を利用してグローバル IP アドレスを求め，そのグローバル IP アドレス宛てにアクセス要求の転送を行う機能を有する。この中継装置として，適切なものはどれか。

ア　プロキシサーバ　　イ　リピータ
ウ　ルータ　　エ　レイヤ 2 スイッチ

問45　BPO の説明はどれか。

ア　災害や事故で被害を受けても，重要事業を中断させない，又は可能な限り中断期間を短くする仕組みを構築すること
イ　社内業務のうちコアビジネスでない事業に関わる業務の一部又は全部を，外部の専門的な企業に委託すること
ウ　製品の基準生産計画，部品表及び在庫情報を基に，資材の所要量と必要な時期を求め，これを基準に資材の手配，納入の管理を支援する生産管理手法のこと
エ　プロジェクトを，戦略との適合性や費用対効果，リスクといった観点から評価を行い，情報化投資のバランスを管理し，最適化を図ること

問46　製造業の企業が社会的責任を果たす活動の一環として，雇用創出や生産設備の環境対策に投資することによって，便益を享受するステークホルダは，株主，役員，従業員に加えて，どれか。

ア　近隣地域社会の住民　　イ　原材料の輸入元企業
ウ　製品を購入している消費者　　エ　取引をしている下請企業

問47　表から，期末在庫品を先入先出法で評価した場合の期末の在庫評価額は何千円か。

摘要		数量（個）	単価（千円）
期首在庫		10	10
仕入	4月	1	11
	6月	2	12
	7月	3	13
	9月	4	14
期末在庫		12	

ア　132　　イ　138　　ウ　150　　エ　168

問48　製造原価明細書から損益計算書を作成したとき，売上総利益は何千円か。

単位　千円

製造原価明細書

材料費	400
労務費	300
経　費	200
当期総製造費用	□
期首仕掛品棚卸高	150
期末仕掛品棚卸高	250
当期製品製造原価	□

単位　千円

損益計算書

売上高	1,000
売上原価	
期首製品棚卸高	120
当期製品製造原価	□
期末製品棚卸高	70
売上原価	□
売上総利益	□

ア　150　　イ　200　　ウ　310　　エ　450

〔 メ モ 用 紙 〕

問49　A 社は，放送会社や運輸会社向けに広告制作ビジネスを展開している。A 社は，人事業務の効率化を図るべく，人事業務の委託を検討することにした。A 社が委託する業務（以下，B 業務という）を図 1 に示す。

・採用予定者から郵送されてくる入社時の誓約書，前職の源泉徴収票などの書類を PDF ファイルに変換し，ファイルサーバに格納する。
（省略）

図 1　B 業務

委託先候補の C 社は，B 業務について，次のように A 社に提案した。

・B 業務だけに従事する専任の従業員を割り当てる。

・B 業務では，図 2 の複合機のスキャン機能を使用する。

・スキャン機能を使用する際は，従業員ごとに付与した利用者 ID とパスワードをパネルに入力する。
・スキャンしたデータを PDF ファイルに変換する。
・PDF ファイルを従業員ごとに異なる鍵で暗号化して，電子メールに添付する。
・スキャンを実行した本人宛てに電子メールを送信する。
・PDF ファイルが大きい場合は，PDF ファイルを添付する代わりに，自社の社内ネットワーク上に設置したサーバ（以下，B サーバという）に自動的に保存し，保存先の URL を電子メールの本文に記載して送信する。

図 2　複合機のスキャン機能（抜粋）

A 社は，C 社と業務委託契約を締結する前に，秘密保持契約を締結して，C 社を訪問し，業務委託での情報セキュリティリスクの評価を実施した。その結果，図 3 の発見があった。

・複合機のスキャン機能では，電子メールの差出人アドレス，件名，本文及び添付ファイル名を初期設定[1)]の状態で使用しており，誰がスキャンを実行しても同じである。
・複合機のスキャン機能の初期設定情報はベンダーの Web サイトで公開されており，誰でも閲覧できる。

注[1)]　C 社の情報システム部だけが複合機の初期設定を変更可能である。

図 3　発見事項

そこで，A 社では，初期設定の状態のままでは A 社にとって情報セキュリティリスクがあり，対策が必要であると評価した。

設問　対策が必要であると A 社が評価した情報セキュリティリスクはどれか。解答群のうち，最も適切なものを選べ。

解答群

ア　B 業務に従事する従業員が，B 業務に従事する他の従業員になりすまして複合機のスキャン機能を使用し，PDF ファイルを取得して不正に持ち出す。その結果，A 社の採用予定者の個人情報が漏えいする。

イ　B 業務に従事する従業員が，攻撃者からの電子メールを複合機からのものと信じて本文中にある URL をクリックし，攻撃者が用意した Web サイトにアクセスしてマルウェア感染する。その結果，A 社の採用予定者の個人情報が漏えいする。

ウ　攻撃者が，複合機から送信される電子メールを盗聴し，添付ファイルを暗号化して身代金を要求する。その結果，A 社が復号鍵を受け取るために多額の身代金を支払うことになる。

エ　攻撃者が，複合機から送信される電子メールを盗聴し，本文に記載されている URL を SNS に公開する。その結果，A 社の採用予定者の個人情報が漏えいする。

問50　A 社は，分析・計測機器などの販売及び機器を利用した試料の分析受託業務を行う分析機器メーカーである。A 社では，図 1 の“情報セキュリティリスクアセスメント手順”に従い，年一度，情報セキュリティリスクアセスメントの結果をまとめている。

・情報資産の機密性，完全性，可用性の評価値は，それぞれ 0～2 の 3 段階とし，表 1 のとおりとする。
・情報資産の機密性，完全性，可用性の評価値の最大値を，その情報資産の重要度とする。
・脅威及び脆弱(ぜいじゃく)性の評価値は，それぞれ 0～2 の 3 段階とする。
・情報資産ごとに，様々な脅威に対するリスク値を算出し，その最大値を当該情報資産のリスク値として情報資産管理台帳に記載する。ここで，情報資産の脅威ごとのリスク値は，次の式によって算出する。
　　リスク値＝情報資産の重要度×脅威の評価値×脆弱性の評価値
・情報資産のリスク値のしきい値を 5 とする。
・情報資産ごとのリスク値がしきい値以下であれば受容可能なリスクとする。
・情報資産ごとのリスク値がしきい値を超えた場合は，保有以外のリスク対応を行うことを基本とする。

図 1　情報セキュリティリスクアセスメント手順

表 1　情報資産の機密性，完全性，可用性の評価基準

評価値		評価基準	該当する情報の例
機密性	2	法律で安全管理措置が義務付けられている。	・健康診断の結果，保健指導の記録 ・給与所得の源泉徴収票
	2	取引先から守秘義務の対象として指定されている。	・取引先から秘密と指定されて受領した資料 ・取引先の公開前の新製品情報
	2	自社の営業秘密であり，漏えいすると自社に深刻な影響がある。	・自社の独自技術，ノウハウ ・取引先リスト ・特許出願前の発明情報
	1	関係者外秘情報又は社外秘情報である。	・見積書，仕入価格など取引先や顧客との商取引に関する情報 ・社内規程，事務処理要領
	0	公開情報である。	・自社製品カタログ，自社 Web サイト掲載情報
完全性	2	法律で安全管理措置が義務付けられている。	・健康診断の結果，保健指導の記録 ・給与所得の源泉徴収票
	2	改ざんされると自社に深刻な影響，又は取引先や顧客に大きな影響がある。	・社内規程，事務処理要領 ・自社の独自技術，ノウハウ ・設計データ（原本）
	1	改ざんされると事業に影響がある。	・受発注情報，決済情報，契約情報 ・設計データ（印刷物）
	0	改ざんされても事業に影響はない。	・廃版製品カタログデータ
可用性	（省略）		

A 社は，自社の Web サイトをインターネット上に公開している。A 社の Web サイトは，自社が取り扱う分析機器の情報を画像付きで一覧表示する機能を有しており，主に A 社で販売する分析機器に関する機能の説明や操作マニュアルを掲載している。A 社で分析機器を購入した顧客は，A 社の Web サイトからマニュアルをダウンロードして利用することが多い。A 社の Web サイトは，製品を販売する機能を有していない。

A 社は，年次の情報セキュリティリスクアセスメントの結果を，表 2 にまとめた。

表 2　A 社の情報セキュリティリスクアセスメント結果（抜粋）

情報資産名称	説明	機密性の評価値	完全性の評価値	可用性の評価値	情報資産の重要度	脅威の評価値	脆弱性の評価値	リスク値
社内規程	行動規範や判断基準を含めた社内ルール	1	2	1	2	1	1	2
設計データ（印刷物）	A 社における主力製品の設計図	（省略）						
自社 Web サイトにあるコンテンツ	分析機器の情報	a1	a2	2	a3	2	2	a4

設問　表 2 中の [a1] ～ [a4] に入れる数値の適切な組合せを，a に関する解答群から選べ。

a に関する解答群

	a1	a2	a3	a4
ア	0	0	2	8
イ	0	1	2	8
ウ	0	2	1	4
エ	0	2	2	8
オ	1	0	2	4
カ	1	1	2	8
キ	1	2	1	4
ク	1	2	2	8

問51　A 社は，金属加工を行っている従業員 50 名の企業である。同業他社がサイバー攻撃を受けたというニュースが増え，A 社の社長は情報セキュリティに対する取組が必要であると考え，新たに情報セキュリティリーダーをおくことにした。

社長は，どのような取組が良いかを検討するよう，情報セキュリティリーダーに任命された B 主任に指示した。B 主任は，調査の結果，IPA が実施している SECURITY ACTION への取組を社長に提案した。

SECURITY ACTION とは，中小企業自らが，情報セキュリティ対策に取り組むことを自己宣言する制度であるとの説明を受けた社長は，SECURITY ACTION の一つ星を宣言するために情報セキュリティ 5 か条に取り組むことを決め，B 主任に，情報セキュリティ 5 か条への自社での取組状況を評価するように指示した。

B 主任の評価結果は表 1 のとおりであった。

表 1　B 主任の評価結果

情報セキュリティ 5 か条		評価結果
1	OS やソフトウェアは常に最新の状態にしよう！	一部の PC について実施している
2	（省略）	（省略）
3	パスワードを強化しよう！	（省略）
4	共有設定を見直そう！	（省略）
5	脅威や攻撃の手口を知ろう！	（省略）

表 1 中の 1 の評価結果について B 主任は，次のとおり説明した。

・A 社が従業員に PC を貸与する時に導入した OS と A 社の業務で利用しているソフトウェア（以下，標準ソフトという）は，自動更新機能を使用して最新の状態に更新している。

・それ以外のソフトウェア（以下，非標準ソフトという）はどの程度利用されているか分からないので，試しに数台の PC を確認したところ，大半の PC で利用されていた。最新の状態に更新されていない PC も存在した。

A 社では表 1 中の 1 について評価結果を“実施している”にするために新たに追加すべき対策として 2 案を考え，どちらかを採用することにした。

設問　表 1 中の 1 の評価結果を“実施している”にするために A 社で新たに追加すべき対策として考えられるものは次のうちどれか。考えられる対策だけを全て挙げた組合せを，解答群の中から選べ。

（一） PC 上のプロセスの起動・終了を記録する Endpoint Detection and Response（EDR）の導入

（二） PC の OS 及び標準ソフトを最新の状態に更新するという設定ルールの導入

（三） 全ての PC への脆弱(ぜい)性修正プログラムの自動適用を行う IT 資産管理ツールの導入

（四） 非標準ソフトのインストール禁止及び強制アンインストール

（五） ログデータを一括管理，分析して，セキュリティ上の脅威を発見するための Security Information and Event Management（SIEM）の導入

解答群

ア （一），（二）	イ （一），（三）	ウ （一），（四）
エ （一），（五）	オ （二），（三）	カ （二），（四）
キ （二），（五）	ク （三），（四）	ケ （三），（五）
コ （四），（五）		

問52　A 社は，複数の子会社を持つ食品メーカーであり，在宅勤務に適用する PC セキュリティ規程（以下，A 社 PC 規程という）を定めている。

A 社は，20XX 年 4 月 1 日に同業の B 社を買収して子会社にした。B 社は，在宅勤務できる日数の上限を週 2 日とした在宅勤務制度を導入しており，全ての従業員が利用している。

B 社は，A 社 PC 規程と同様の規程を作成して順守することにした。B 社は，自社の規程の作成に当たり，表 1 のとおり A 社 PC 規程への対応状況の評価結果を取りまとめた。

表 1　A 社 PC 規程への B 社の対応状況の評価結果（抜粋）

項番	A 社 PC 規程	評価結果
1	（省略）	OK
2	（省略）	OK
3	会社が許可したアプリケーションソフトウェアだけを導入できるように技術的に制限すること	NG
4	外部記憶媒体へのアクセスを技術的に禁止すること	NG[1)]
5	Bluetooth の利用を技術的に禁止すること	NG

注記　評価結果が“OK”とは A 社 PC 規程を満たす場合，“NG”とは満たさない場合をいう。
注 [1)]　B 社は，外部記憶媒体へのアクセスのうち，外部記憶媒体に保存してあるアプリケーションソフトウェア及びファイルの NPC へのコピーだけは許可している。

評価結果のうち，A 社 PC 規程を満たさない項番については，必要な追加対策を実施することによって，情報セキュリティリスクを低減することにした。

設問　表 1 中の項番 4 について，B 社が必要な追加対策を実施することによって低減できる情報セキュリティリスクは次のうちどれか。低減できるものだけを全て挙げた組合せを，解答群の中から選べ。ここで，項番 3，5 への追加対策は実施しないものとする。

（一） B 社で許可していないアプリケーションソフトウェアが保存されている外部記憶媒体が NPC に接続された場合に，当該 NPC がマルウェア感染する。

（ニ） 外部記憶媒体が NPC に接続された場合に，当該外部記憶媒体に当該 NPC 内のデータを保存して持ち出される。

（三） マルウェア付きのファイルが保存されている外部記憶媒体が NPC に接続された場合に，当該 NPC がマルウェア感染する。

（四） マルウェアに感染している NPC に外部記憶媒体が接続された場合に，当該外部記憶媒体がマルウェア感染する。

解答群

ア （一），（ニ）	イ （一），（ニ），（三）
ウ （一），（ニ），（四）	エ （一），（三）
オ （一），（四）	カ （ニ），（三）
キ （ニ），（四）	ク （三），（四）

問53　A 社は，高級家具を販売する企業である。A 社は 2 年前に消費者に直接通信販売する新規事業を開始した。それまで A 社は，個人情報はほとんど取り扱っていなかったが，通信販売事業を開始したことによって，複合機で印刷した送り状など，顧客の個人情報を大量に扱うようになってきた。そのため，オフィス内に通販事業部エリアを設け，個人情報が漏えいしないよう対策した。具体的には，通販事業部エリアの出入口に，IC カード認証でドアを解錠するシステムを設置し，通販事業部の従業員だけが通販事業部エリアに入退室できるようにした。他のエリアは A 社の全従業員が自由に利用できるようにしている。図 1 は，A 社のオフィスのレイアウトである。

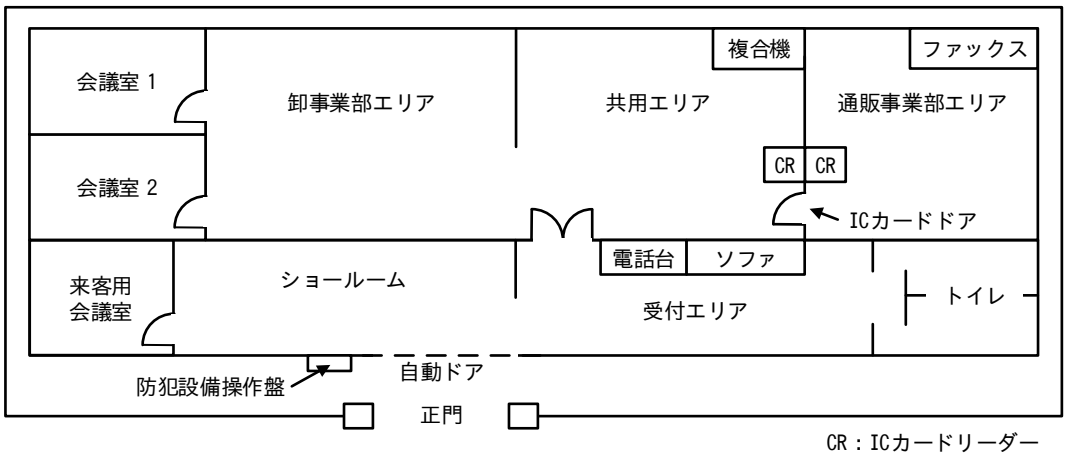

図 1　A 社のオフィスのレイアウト

このレイアウトでの業務を観察したところ，通販事業部エリアへの入室時に，A 社の従業員同士による共連れが行われているという問題点が発見され，改善案を考えることになった。

設問　改善案として適切なものだけを全て挙げた組合せを，解答群の中から選べ。

（一） IC カードドアに監視カメラを設置し，1 年に 1 回監視カメラの映像をチェックする。

（二） IC カードドアの脇に，共連れのもたらすリスクを知らせる標語を掲示する。

（三） IC カードドアを，AES の暗号方式を用いたものに変更する。

（四） IC カードの認証に加えて指静脈認証も行うようにする。

（五） 正門内側の自動ドアに共連れ防止用のアンチパスバックを導入する。

（六） 通販事業部エリア内では，従業員証を常に見えるところに携帯する。

（七） 共連れを発見した場合は従業員同士で個別に注意する。

解答群

ア （一），（二）	イ （一），（四）	ウ （一），（五）
エ （二），（三）	オ （二），（七）	カ （三），（六）
キ （三），（七）	ク （四），（六）	ケ （五），（六）
コ （五），（七）		

問54　A 社は旅行商品を販売しており，業務の中で顧客情報を取り扱っている。A 社が保有する顧客情報は，A 社のファイルサーバ 1 台に保存されている。ファイルサーバは，顧客情報を含むフォルダにある全てのファイルを磁気テープに毎週土曜日にバックアップするよう設定されている。バックアップは 2 世代分が保存され，ファイルサーバの隣にあるキャビネットに保管されている。

A 社では年に一度，情報セキュリティに関するリスクの見直しを実施している。情報セキュリティリーダーである E 主任は，A 社のデータ保管に関するリスクを見直して図 1 にまとめた。

1.　ランサムウェアによってデータが暗号化され，最新のデータが利用できなくなることによって，最大 1 週間分の更新情報が失われる。 2.　（省略） 3.　（省略） 4.　（省略）

図 1　A 社のデータ保管に関するリスク（抜粋）

E 主任は，図 1 の 1 に関するリスクを現在の対策よりも，より低減するための対策を検討した。

設問　E 主任が検討した対策はどれか。解答群のうち，最も適切なものを選べ。

解答群

ア　週 1 回バックアップを取得する代わりに，毎日 1 回バックアップを取得して 7 世代分保存する。

イ　バックアップ後に磁気テープの中のファイルのリストと，ファイルサーバのバックアップ対象フォルダ中のファイルのリストを比較し，差分がないことを確認する。

ウ　バックアップに利用する磁気テープ装置を，より高速な製品に交換する。

エ　バックアップ用の媒体を磁気テープからハードディスクに変更する。

オ　バックアップを二組み取得し，うち一組みを遠隔地に保管する。

カ　ファイルサーバにマルウェア対策ソフトを導入する。

〔 メ モ 用 紙 〕

問55　A 社は，SaaS 形式の給与計算サービス（以下，A サービスという）を法人向けに提供する，従業員 100 名の IT 会社である。A 社は，自社でも A サービスを利用している。A 社の従業員は，Web ブラウザで A サービスのログイン画面にアクセスし，A サービスのアカウント（以下，A アカウントという）の利用者 ID 及びパスワードを入力する。ログインに成功すると，自分の給与及び賞与の確認，パスワードの変更などができる。利用者 ID は，個人ごとに付与した不規則な 8 桁の番号である。ログイン時にパスワードを連続して 5 回間違えると A アカウントはロックされる。ロックを解除するためには，A サービスの解除画面で申請する。

A 社は，半年に 1 回，標的型攻撃メールへの対応訓練（以下，H 訓練という）を実施しており，表 1 に示す 20XX 年下期の H 訓練計画案が経営会議に提出された。

表 1　20XX 年下期の H 訓練計画案（抜粋）

項目	内容
電子メールの送信日時	次の日時に，H 訓練の電子メールを全従業員宛に送信する。 ・20XX 年 10 月 1 日　10 時 00 分
送信者メールアドレス	A サービスを装ったドメインのメールアドレス
電子メールの本文	次を含める。 ・A アカウントはロックされていること ・ロックを解除するには，次の URL にアクセスすること ・偽解除サイトの URL
偽解除サイト	・氏名，所属部門名並びに A アカウントの利用者 ID 及びパスワードを入力させる。 ・全ての項目の入力が完了すると，H 訓練であることを表示する。
結果の報告	経営会議への報告予定日：20XX 年 10 月 31 日

注記　偽解除サイトで入力された情報は，保存しない。A 社は，従業員の氏名，所属部門名及び A アカウントの情報を個人情報としている。

経営会議では，表 1 の計画案はどのような標的型攻撃メールを想定しているのかという質問があった。

設問　表 1 の計画案が想定している標的型攻撃メールはどれか。解答群のうち，最も適切なものを選べ。

解答群

ア　従業員を A サービスに誘導し，A アカウントのロックが解除されるかを試行する標的型攻撃メール

イ　従業員を攻撃者が用意した Web サイトに誘導し，A アカウントがロックされない連続失敗回数の上限を発見する標的型攻撃メール

ウ　従業員を攻撃者が用意した Web サイトに誘導し，従業員の個人情報を不正に取得する標的型攻撃メール

エ　複数の従業員を A サービスに同時に誘導し，アクセスを集中させることによって，一定期間，A サービスを利用不可にする標的型攻撃メール

問56　A 社は学習塾を経営している会社であり，全国に 50 の校舎を展開している。A 社には，教務部，情報システム部，監査部などがある。学習塾に通う又は通っていた生徒（以下，塾生という）の個人データは，学習塾向けの管理システム（以下，塾生管理システムという）に格納している。塾生管理システムのシステム管理は情報システム部が行っている。塾生の個人データ管理業務と塾生管理システムの概要を図 1 に示す。

・教務部員は，入塾した塾生及び退塾する塾生の登録，塾生プロフィールの編集，模試結果の登録，進学先の登録など，塾生の個人データの入力，参照及び更新を行う。
・教務部員が使用する端末は教務部の共用端末である。
・塾生管理システムへのログインには利用者 ID とパスワードを利用する。
・利用者 ID は個人別に発行されており，利用者 ID の共用はしていない。
・塾生管理システムの利用者のアクセス権限には参照権限及び更新権限の 2 種類がある。参照権限があると塾生の個人データを参照できる。更新権限があると塾生の個人データの参照，入力及び更新ができる。アクセス権限は塾生の個人データごとに設定できる。
・教務部員は，担当する塾生の個人データの更新権限をもっている。担当しない塾生の個人データの参照権限及び更新権限はもっていない。
・共用端末の OS へのログインには，共用端末の識別子（以下，端末 ID という）とパスワードを利用する。
・共用端末のパスワード及び塾生管理システムの利用者のアクセス権限は情報システム部が設定，変更できる。

図 1　塾生の個人データ管理業務と塾生管理システムの概要

教務部は，今年実施の監査部による内部監査の結果，Web ブラウザに塾生管理システムの利用者 ID とパスワードを保存しており，情報セキュリティリスクが存在するとの指摘を受けた。

設問　監査部から指摘された情報セキュリティリスクはどれか。解答群のうち，最も適切なものを選べ。

解答群

ア　共用端末と塾生管理システム間の通信が盗聴される。

イ　共用端末が不正に持ち出される。

ウ　情報システム部員によって塾生管理システムの利用者のアクセス権限が不正に変更される。

エ　教務部員によって共用端末のパスワードが不正に変更される。

オ　塾生の個人データがアクセス権限をもたない教務部員によって不正にアクセスされる。

問57　A 社は従業員 600 名の投資コンサルティング会社である。東京の本社には，情報システム部，監査部などの管理部門があり，関西に B 支店がある。B 支店の従業員は 10 名である。

B 支店では，情報システム部が運用管理しているファイルサーバを使用しており，顧客情報を含むファイルを一時的に保存する場合がある。その場合，ファイルのアクセス権は，当該ファイルを保存した従業員が最小権限の原則に基づいて設定する。今年，B 支店では，従業員にヒアリングを行い，ファイルのアクセス権がそのとおりに設定されていることを確認した。

〔自己評価の実施〕

A 社では，1 年に 1 回，監査部が各部門に，評価項目を記載したシート（以下，自己評価シートという）を配布し，自己評価の実施と結果の提出を依頼している。

B 支店で情報セキュリティリーダーを務める C 氏は，監査部から送付されてきた自己評価シートに従って，職場の状況を観察したり，従業員にヒアリングしたりして評価した。自己評価シートの評価結果は図 1 の判定ルールに従って記入する。C 氏が作成した B 支店の評価結果を表 1 に示す。

・評価項目どおりに実施している場合：“OK”
・評価項目どおりには実施していないが，代替コントロールによって，“OK”の場合と同程度にリスクが低減されていると考えられる場合：“(OK)”（代替コントロールを具体的に評価根拠欄に記入する。）
・評価項目どおりには実施しておらず，かつ，代替コントロールによって評価項目に関するリスクが抑えられていないと考えられる場合：“NG”
・評価項目に関するリスクがそもそも存在しない場合：“NA”

図 1　評価結果の判定ルール

表 1　B 支店の評価結果（抜粋）

No.	評価項目	評価結果	評価根拠
10	（省略）	OK	（省略）
19	ファイルサーバ上の顧客情報のアクセス権は最小権限の原則に基づいて設定されている。	a	
25	（省略）	OK	（省略）

設問　表 1 中の［　a　］に入れる字句はどれか。解答群のうち，最も適切なものを選べ。

a に関する解答群

	評価結果	評価根拠
ア	OK	アクセス権の設定状況が適切であることを確認した。
イ	OK	アクセス権を適切に設定するルールが存在することを確認した。
ウ	OK	ファイルサーバは情報システム部が運用管理している。
エ	NA	顧客情報をファイルサーバに保存することは禁止されている。

問58　国内外に複数の子会社をもつ A 社では，インターネットに公開する Web サイトについて，A 社グループの脆弱性診断基準（以下，A 社グループ基準という）を設けている。A 社の子会社である B 社は，会員向けに製品を販売する Web サイト（以下，B 社サイトという）を運営している。B 社サイトは，会員だけが B 社の製品やサービスを検索できる。会員の氏名，メールアドレスなどの会員情報も管理している。

B 社では，11 月に情報セキュリティ活動の一環として，A 社グループ基準を基に自己点検を実施し，その結果を表 1 のとおりまとめた。

表 1　B 社自己点検結果（抜粋）

項番	点検項目	A 社グループ基準	点検結果
(一)	Web アプリケーションプログラム（以下，Web アプリという）に対する脆弱性診断の実施	・インターネットに公開している Web サイトについて，Web アプリの新規開発時，及び機能追加時に行う。 ・機能追加などの変更がない場合でも，年 1 回以上行う。	・3 年前に B 社サイトをリリースする 1 か月前に，Web アプリに対する脆弱性診断を行った。リリース以降は実施していない。 ・3 年前の脆弱性診断では，軽微な脆弱性が 2 件検出された。
(二)	OS 及びミドルウェアに対する脆弱性診断の実施	・インターネットに公開している Web サイトについて，年 1 回以上行う。	・毎年 4 月及び 10 月に，B 社サイトに対して行っている。 ・今年 4 月の脆弱性診断では，脆弱性が 3 件検出された。
(三)	脆弱性診断結果の報告	・Web アプリ，OS 及びミドルウェアに対する脆弱性診断を行った場合，その結果を，診断後 2 か月以内に各社の情報セキュリティ委員会に報告する。	・3 年前に Web アプリに対する脆弱性診断を行った 2 週間後に，結果を情報セキュリティ委員会に報告した。 ・OS 及びミドルウェアに対する脆弱性診断の結果は，4 月と 10 月それぞれの月末の情報セキュリティ委員会に報告した。
(四)	脆弱性診断結果の対応	・Web アプリ，OS 及びミドルウェアに対する脆弱性診断で，脆弱性が発見された場合，緊急を要する脆弱性については，速やかに対応し，その他の脆弱性については，診断後，1 か月以内に対応する。指定された期限までの対応が困難な場合，対応の時期を明確にし，最高情報セキュリティ責任者（CISO）の承認を得る。	・3 年前に検出した Web アプリの脆弱性 2 件について，B 社サイトのリリースの 1 週間前に対応した。 ・今年 4 月に検出した OS 及びミドルウェアに対する脆弱性のうち，2 件は翌日に対応した。残り 1 件は，恒久的な対策は来年 1 月の B 社サイトの更改時に対応するものとし，それまでは，設定変更による暫定対策をとるという対応計画について，脆弱性診断の 10 日後に CISO の承認を得た。

設問　表 1 中の自己点検の結果のうち，A 社グループ基準を満たす項番だけを全て挙げた組合せを，解答群の中から選べ。

解答群

ア　(一)，(二)　　イ　(一)，(二)，(三)

ウ　(一)，(二)，(三)，(四)　　エ　(一)，(二)，(四)

オ　(一)，(三)，(四)　　カ　(一)，(四)

キ　(二)，(三)　　ク　(二)，(三)，(四)

ケ　(三)，(四)

問59　A 社は従業員 200 名の通信販売業者である。一般消費者向けに生活雑貨，ギフト商品などの販売を手掛けている。取扱商品の一つである商品 Z は，Z 販売課が担当している。

〔Z 販売課の業務〕

現在，Z 販売課の要員は，商品 Z についての受注管理業務及び問合せ対応業務を行っている。商品 Z についての受注管理業務の手順を図 1 に示す。

商品 Z の顧客からの注文は電子メールで届く。 (1) 入力 販売担当者は，届いた注文（変更，キャンセルを含む）の内容を受注管理システム [1]（以下，J システムという）に入力し，販売責任者 [2] に承認を依頼する。 (2) 承認 販売責任者は，注文の内容と J システムへの入力結果を突き合わせて確認し，問題がなければ承認する。問題があれば差し戻す。

注 [1]　A 社情報システム部が運用している。利用者は，販売責任者，販売担当者などである。
注 [2]　Z 販売課の課長 1 名だけである。

図 1　受注管理業務の手順

〔J システムの操作権限〕

Z 販売課では，J システムについて，次の利用方針を定めている。

［方針 1］　ある利用者が入力した情報は，別の利用者が承認する。

［方針 2］　販売責任者は，Z 販売課の全業務の情報を閲覧できる。

J システムでは，業務上必要な操作権限を利用者に与える機能が実装されている。

この度，商品 Z の受注管理業務が受注増によって増えていることから，B 社に一部を委託することにした（以下，商品 Z の受注管理業務の入力作業を行う B 社従業員を商品 Z の B 社販売担当者といい，商品 Z の B 社販売担当者の入力結果をチェックする B 社従業員を商品 Z の B 社販売責任者という）。

委託に当たって，Z 販売課は情報システム部に J システムに関する次の要求事項を伝えた。

［要求 1］　B 社が入力した場合は，A 社が承認する。

［要求 2］　A 社の販売担当者が入力した場合は，現状どおりに A 社の販売責任者が承認する。

上記を踏まえ，情報システム部は今後の各利用者に付与される操作権限を表 1 にまとめた。

表 1　操作権限案

付与される操作権限 / 利用者	J システム		
	閲覧	入力	承認
a	○		○
（省略）	○	○	
（省略）	○		
（省略）	○	○	

注記　○は，操作権限が付与されることを示す。

設問　表 1 中の［　a　］に入れる適切な字句を解答群の中から選べ。

解答群

ア　Z 販売課の販売責任者

イ　Z 販売課の販売担当者

ウ　Z 販売課の要員

エ　商品 Z の B 社販売責任者

オ　商品 Z の B 社販売担当者

問60　A 社は輸入食材を扱う商社である。ある日，経理課の B 課長は，A 社の海外子会社である C 社の D さんから不審な点がある電子メール（以下，メールという）を受信した。B 課長は，A 社の情報システム部に調査を依頼した。A 社の情報システム部が C 社の情報システム部と協力して調査した結果を図 1 に示す。

1　B 課長へのヒアリング並びに受信したメール及び添付されていた請求書からは，次が確認された。
［項番 1］D さんが早急な対応を求めたことは今まで 1 回もなかったが，メール本文では送金先の口座を早急に変更するよう求めていた。
［項番 2］添付されていた請求書は，A 社が C 社に支払う予定で進めている請求書であり，C 社が 3 か月前から利用を開始したテンプレートを利用したものだった。
［項番 3］添付されていた請求書は，振込先が，C 社が所在する国ではない国にある銀行の口座だった。
［項番 4］添付されていた請求書が作成された PC のタイムゾーンは，C 社のタイムゾーンとは異なっていた。
［項番 5］メールの送信者（From）のメールアドレスには，C 社のドメイン名とは別の類似するドメイン名が利用されていた。
［項番 6］メールの返信先（Reply-To）は D さんのメールアドレスではなく，フリーメールのものであった。
［項番 7］メール本文では，B 課長と D さんとの間で 6 か月前から何度かやり取りしたメールの内容を引用していた。
2　不正ログインした者が，以降のメール不正閲覧の発覚を避けるために実施したと推察される設定変更が D さんのメールアカウントに確認された。

図 1　調査の結果（抜粋）

設問　B 課長に疑いをもたれないようにするためにメールの送信者が使った手口として考えられるものはどれか。図 1 に示す各項番のうち，該当するものだけを全て挙げた組合せを，解答群の中から選べ。

解答群

ア　［項番 1］,［項番 2］,［項番 3］
イ　［項番 1］,［項番 2］,［項番 6］
ウ　［項番 1］,［項番 4］,［項番 6］
エ　［項番 1］,［項番 4］,［項番 7］
オ　［項番 2］,［項番 3］,［項番 6］
カ　［項番 2］,［項番 5］,［項番 7］
キ　［項番 3］,［項番 4］,［項番 5］
ク　［項番 3］,［項番 5］,［項番 7］
ケ　［項番 4］,［項番 5］,［項番 6］
コ　［項番 5］,［項番 6］,［項番 7］

〔 メ モ 用 紙 〕

試験問題に記載されている会社名又は製品名は，それぞれ各社の商標又は登録商標です。

なお，試験問題では，™ 及び ® を明記していません。