令和５年度
情報セキュリティマネジメント試験　科目Ａ・Ｂ
公開問題

問題番号	問１～問15
選択方法	全問必須

注意事項

1. 実際の試験は60問で構成されますが，そのうちの15問を公開しています。
2. **問題に関する質問にはお答えできません。**文意どおり解釈してください。

問１　情報セキュリティ管理基準（平成 28 年）に関する記述のうち，適切なものはどれか。

ア　“ガバナンス基準”，“管理策基準”及び“マネジメント基準”の三つの基準で構成されている。

イ　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）及び JIS Q 27002:2014（情報セキュリティ管理策の実践のための規範）との整合性をとっている。

ウ　情報セキュリティ対策は，“管理策基準”に挙げられた管理策の中から選択することとしている。

エ　トップマネジメントは，“マネジメント基準”に挙げられている事項の中から，自組織に合致する事項を選択して実施することとしている。

問２　入室時と退室時に ID カードを用いて認証を行い，入退室を管理する。このとき，入室時の認証に用いられなかった ID カードでの退室を許可しない，又は退室時の認証に用いられなかった ID カードでの再入室を許可しないコントロールを行う仕組みはどれか。

ア　TPMOR（Two Person Minimum Occupancy Rule）

イ　アンチパスバック

ウ　インターロックゲート

エ　パニックオープン

問３　デジタルフォレンジックスの説明はどれか。

ア　サイバー攻撃に関連する脅威情報を標準化された方法で記述し，その脅威情報をセキュリティ対策機器に提供すること

イ　受信メールに添付された実行ファイルを動作させたときに，不正な振る舞いがないかどうかをメールボックスへの保存前に確認すること

ウ　情報セキュリティインシデント発生時に，法的な証拠となるデータを収集し，保管し，調査分析すること

エ　内部ネットワークにおいて，通信データを盗聴されないように暗号化すること

問４　暗号方式に関する記述のうち，適切なものはどれか。

ア　公開鍵暗号方式，共通鍵暗号方式ともに，大きな合成数の素因数分解が困難であることが安全性の根拠である。

イ　公開鍵暗号方式では原則としてセッションごとに異なる鍵を利用するが，共通鍵暗号方式では一度生成した鍵を複数のセッションに繰り返し利用する。

ウ　公開鍵暗号方式は仕様が標準化されているが，共通鍵暗号方式はベンダーによる独自の仕様で実装されることが一般的である。

エ　大量のデータを短い時間で暗号化する場合には，公開鍵暗号方式よりも共通鍵暗号方式が適している。

問５　セキュアハッシュ関数 SHA-256 を用いてファイル A 及びファイル B のハッシュ値を算出すると，どちらも全く同じ次に示すハッシュ値 n（16 進数で示すと 64 桁）となった。この結果から考えられることとして，適切なものはどれか。

ハッシュ値 n：86620f2f 152524d7 dbed4bcb b8119bb6 d493f734 0b4e7661 88565353 9e6d2074

ア　ファイル A とファイル B の各内容を変更せずに再度ハッシュ値を算出すると，ファイル A とファイル B のハッシュ値が異なる。

イ　ファイル A とファイル B のハッシュ値 n のデータ量は 64 バイトである。

ウ　ファイル A とファイル B を連結させたファイル C のハッシュ値の桁数は 16 進数で示すと 128 桁である。

エ　ファイル A の内容とファイル B の内容は同じである。

問６　迷惑メール対策の SPF（Sender Policy Framework）の仕組みはどれか。

ア　送信側ドメインの管理者が，正規の送信側メールサーバの IP アドレスを DNS に登録し，受信側メールサーバでそれを参照して，IP アドレスの判定を行う。

イ　送信側メールサーバでメッセージにデジタル署名を施し，受信側メールサーバでそのデジタル署名を検証する。

ウ　第三者によって提供されている，スパムメールの送信元 IP アドレスのデータベースを参照して，スパムメールの判定を行う。

エ　ファイアウォールを通過した要求パケットに対する応答パケットかどうかを判断して，動的に迷惑メールの通信を制御する。

問７　Web アプリケーションにおけるセキュリティ上の脅威とその対策に関する記述のうち，適切なものはどれか。

ア　OS コマンドインジェクションを防ぐために，Web アプリケーションが発行するセッション ID に推測困難な乱数を使用する。

イ　SQL インジェクションを防ぐために，Web アプリケーション内でデータベースへの問合せを作成する際にプレースホルダを使用する。

ウ　クロスサイトスクリプティングを防ぐために，Web サーバ内のファイルを外部から直接参照できないようにする。

エ　セッションハイジャックを防ぐために，Web アプリケーションからシェルを起動できないようにする。

問８　電子署名法に関する記述のうち，適切なものはどれか。

ア　電子署名には，電磁的記録ではなく，かつ，コンピュータで処理できないものも含まれる。

イ　電子署名には，民事訴訟法における押印と同様の効力が認められる。

ウ　電子署名の認証業務を行うことができるのは，政府が運営する認証局に限られる。

エ　電子署名は共通鍵暗号技術によるものに限られる。

問９　情報システムのインシデント管理に対する監査で判明した状況のうち，監査人が，指摘事項として監査報告書に記載すべきものはどれか。

ア　インシデント対応手順が作成され，関係者への周知が図られている。
イ　インシデントによってデータベースが被害を受けた場合の影響を最小にするために，規程に従ってデータのバックアップをとっている。
ウ　インシデントの種類や発生箇所，影響度合いに関係なく，連絡・報告ルートが共通になっている。
エ　全てのインシデントについて，インシデント記録を残し，責任者の承認を得ることが定められている。

問10　HTTP の cookie に関する記述のうち，適切なものはどれか。

ア　cookie に含まれる情報は HTTP ヘッダの一部として送信される。
イ　cookie に含まれる情報は Web サーバだけに保存される。
ウ　cookie に含まれる情報は Web ブラウザが全て暗号化して送信する。
エ　クライアントが cookie に含まれる情報の有効期限を設定する。

問11　BPM の説明はどれか。

ア　企業活動の主となる生産，物流，販売，財務，人事などの業務の情報を一元管理することによって，経営資源の全体最適を実現する。
イ　業務プロセスに分析，設計，実行，改善のマネジメントサイクルを取り入れ，業務プロセスの改善見直しや最適なプロセスへの統合を継続的に実施する。
ウ　顧客データベースを基に，商品の販売から保守サービス，問合せやクレームへの対応など顧客に関する業務プロセスを一貫して管理する。
エ　部品の供給から製品の販売までの一連の業務プロセスの情報をリアルタイムで交換することによって，在庫の削減とリードタイムの短縮を実現する。

問12　品質管理において，結果と原因との関連を整理して，魚の骨のような図にまとめたものはどれか。

ア　管理図　　イ　特性要因図　　ウ　パレート図　　エ　ヒストグラム

問13　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を行っている。

・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

図 1　情報セキュリティリスクアセスメント手順

A 社の情報セキュリティリーダーである B さんは，年次の情報セキュリティリスクアセスメントを行い，結果を情報資産管理台帳に表 1 のとおり記載した。

表１　A 社の情報資産管理台帳（抜粋）

情報資産	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
（一）従業員の健康診断の情報	2	2	2	（省略）	2	2	（省略）
（二）行動規範などの社内ルール	1	2	1	（省略）	1	1	（省略）
（三）自社 Web サイトに掲載している会社情報	0	2	2	（省略）	2	2	（省略）
（四）分析結果の精度を向上させるために開発した技術	2	2	1	（省略）	2	1	（省略）

設問　表１中の各情報資産のうち，保有以外のリスク対応を行うべきものはどれか。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　（一），（二）　　イ　（一），（二），（三）

ウ　（一），（二），（四）　　エ　（一），（三）

オ　（一），（三），（四）　　カ　（一），（四）

キ　（二），（三）　　ク　（二），（三），（四）

ケ　（二），（四）　　コ　（三），（四）

問14　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データ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.　（省略）
2.　（省略）
3.　（省略）
4.　バックアップ対象とするフォルダの設定ミスによって，データが復旧できなくなる。

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 4 のリスクを低減するための対策を検討し，効果が期待できるものを選んだ。

設問　次の対策のうち，効果が期待できるものを二つ挙げた組合せを，解答群の中から選べ。

（一）　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。

（二）　バックアップ後に，磁気テープ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ァイルのリストとを比較し，合致しているかを確認する。

（三）　バックアップ対象とするフォルダの設定を，必ず 2 名で行うようにする。

（四）　バックアップ用の媒体を磁気テープから外付けハードディスクに変更する。

（五）　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。

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15　消費者向けの化粧品販売を行うA社では，電子メール（以下，メールという）の送受信にクラウドサービスプロバイダB社が提供するメールサービス（以下，Bサービスという）を利用している。A社が利用するBサービスのアカウントは，A社の情報システム部が管理している。

〔Bサービスでの認証〕

Bサービスでの認証は，利用者IDとパスワードに加え，あらかじめ登録しておいたスマートフォンの認証アプリを利用した2要素認証である。入力された利用者IDとパスワードが正しかったときは，スマートフォンに承認のリクエストが来る。リクエストを1分以内に承認した場合は，Bサービスにログインできる。

〔社外のネットワークからの利用〕

社外のネットワークから社内システム又はファイルサーバを利用する場合，従業員は貸与されたPCから社内ネットワークにVPN接続する。

〔PCでのマルウェア対策〕

従業員に貸与されたPCには，マルウェア対策ソフトが導入されており，マルウェア定義ファイルを毎日16時に更新するように設定されている。マルウェア対策ソフトは，毎日17時に，各PCのマルウェア定義ファイルが更新されたかどうかをチェックし，更新されていない場合は情報システム部のセキュリティ担当者に更新されていないことをメールで知らせる。

〔メールに関する報告〕

ある日の15時頃，販売促進部の情報セキュリティリーダーであるC課長は，在宅で勤務していた部下のDさんから，メールに関する報告を受けた。報告を図1に示す。

・販売促進キャンペーンを委託しているE社のFさんから9時30分にメールが届いた。
・Fさんとは直接会ったことがある。この数か月頻繁にやり取りもしていた。
・そのメールは，これまでのメールに返信する形で作成されており，メールの本文には販売キャンペーンの内容やFさんがよく利用する挨拶文が記載されていた。
・急ぎの対応を求める旨が記載されていたので，メールに添付されていたファイルを開いた。
・メールの添付ファイルを開いた際，特に見慣れないエラーなどは発生せず，ファイルの内容も閲覧できた。
・ファイルの内容を確認した後，返信した。
・11時頃，Dさんのスマートフォンに，承認のリクエストが来たが，Bサービスにログインしようとしたタイミングではなかったので，リクエストを承認しなかった。
・12時までと急いでいた割にその後の返信がなく不審に思ったので，14時50分にFさんに電話で確認したところ，今日はメールを送っていないと言われた。
・現在までのところ，PCの処理速度が遅くなったり，見慣れないウィンドウが表示されたりするなどの不具合や不審な事象は発生していない。
・現在，PCは，インターネットには接続しているが，社内ネットワークへのVPN接続は切断している。
・Dさんはすぐに会社に向かうことは可能で，Dさんの自宅から会社までは1時間掛かる。

図1　Dさんからの報告

C課長は，すぐにPCを会社に持参し，オフラインでマルウェア対策ソフトの定義ファイルを最新版に更新した後，フルスキャンを実施するよう，Dさんに指示をした。スキャンを実行した結果，Dさんの PC からマルウェアが検出された。このマルウェアは，マルウェア対策ソフトのベンダーが9時に公開した最新の定義ファイルで検出可能であることが判明した。

A社では，今回のマルウェア感染による情報セキュリティインシデントの問題点を整理し，再発を防止するための対策を講じることにした。

設問　A 社が講じることにした対策はどれか。解答群のうち，最も適切なものを選べ。

解答群

ア　PC が起動したらすぐに自動的に VPN 接続するように，PC を構成する。

イ　これまでメールをやり取りしたことがない差出人からメールを受信した場合は，添付されているファイルを開かず，すぐに削除するよう社内ルールに定める。

ウ　マルウェア定義ファイルは，10 分ごとに更新されるように，マルウェア対策ソフトの設定を変更する。

エ　マルウェア定義ファイルは，8 時にも更新されるように，マルウェア対策ソフトの設定を変更する。

オ　メールに添付されたファイルを開く場合は，一旦 PC に保存し，マルウェア対策ソフトでスキャンを実行してから開くよう社内ルールに定める。

〔 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。