令和６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　JIS Q 31000:2019（リスクマネジメント－指針）におけるリスクアセスメントを構成するプロセスの組合せはどれか。

ア　リスク特定，リスク評価，リスク受容
イ　リスク特定，リスク分析，リスク評価
ウ　リスク分析，リスク対応，リスク受容
エ　リスク分析，リスク評価，リスク対応

問２　情報の取扱基準の中で，社外秘情報の持出しを禁じ，周知した上で，従業員に情報を不正に持ち出された場合に，“社外秘情報とは知らなかった”という言い訳をさせないことが目的の一つになっている対策はどれか。

ア　権限がない従業員が文書にアクセスできないようにするペーパレス化
イ　従業員との信頼関係の維持を目的にした職場環境の整備
ウ　従業員に対する電子メールの外部送信データ量の制限
エ　情報の管理レベルについてのラベル付け

問３　マルウェアの検出方法のうち，検査対象のプログラムを実行する必要があるものはどれか。

ア　コンペア法　　イ　チェックサム法
ウ　パターンマッチング法　　エ　ビヘイビア法

問４　サイバーキルチェーンに関する説明として，適切なものはどれか。

ア　委託先の情報セキュリティリスクが委託元にも影響するという考え方を基にしたリスク分析のこと

イ　攻撃者がクライアントとサーバとの間の通信を中継し，あたかもクライアントとサーバが直接通信しているかのように装うことによって情報を盗聴するサイバー攻撃手法のこと

ウ　攻撃者の視点から，攻撃の手口を偵察から目的の実行までの段階に分けたもの

エ　取引データを複数の取引ごとにまとめ，それらを時系列につなげたチェーンに保存することによって取引データの改ざんを検知可能にしたもの

問５　リスクベース認証の説明として，適切なものはどれか。

ア　機器の画面に表示された点を正しい順序に一筆書きでなぞった場合，認証が成功し，機器のロックが解除される。

イ　通常とは異なる IP アドレス，Web ブラウザなどから認証要求があった場合に，追加の認証を行う。

ウ　認証局が，Web サイトへのサーバ証明書発行において，サーバ証明書に記載される組織のドメイン利用権，法的及び物理的実在性を確認する。

エ　ゆがんだ文字を含む画像を表示し，その文字が正しく入力された場合に認証が成功する。

問６　A 社の Web サーバは，サーバ証明書を使って TLS 通信を行っている。PC から A 社の Web サーバへの TLS を用いたアクセスにおいて，当該 PC がサーバ証明書を入手した後に，認証局の公開鍵を利用して行う動作はどれか。

ア　暗号化通信に利用する共通鍵を，認証局の公開鍵を使って復号する。
イ　暗号化通信に利用する共通鍵を生成し，認証局の公開鍵を使って暗号化する。
ウ　サーバ証明書の正当性を，認証局の公開鍵を使って検証する。
エ　利用者が入力して送付する秘匿データを，認証局の公開鍵を使って暗号化する。

問７　個人情報保護法が保護の対象としている個人情報に関する記述のうち，適切なものはどれか。

ア　企業が管理している顧客に関する情報に限られる。
イ　個人が秘密にしているプライバシーに関する情報に限られる。
ウ　生存する個人に関する情報に限られる。
エ　日本国籍を有する個人に関する情報に限られる。

問８　内部統制の基本的要素の一つである“統制活動”に該当するものはどれか。

ア　経営目的を達成するための経営方針及び経営戦略
イ　個人情報保護に関する脅威と脆弱(ぜい)性の分析
ウ　受注から出荷に至る業務プロセスに組み込まれた処理結果の検証
エ　定期的に計画して実施する内部業務監査

問９　システムの信頼性指標として RASIS がある。そのうちの A は可用性を表し，システムのサービス時間など，ある一定期間でのシステムの機能を維持する度合いを表している。この A を向上させるものはどれか。

ア　MTBF と MTTR をともに 2 倍にする。
イ　MTBF は変えず，MTTR を 2 倍にする。
ウ　MTBF を 2 倍にして，MTTR は変えない。
エ　MTBF を半分にして，MTTR は 2 倍にする。

問10　社内ネットワークからインターネットへのアクセスを中継し，Web コンテンツをキャッシュすることによってアクセスを高速にする仕組みで，セキュリティ確保にも利用されるものはどれか。

ア　DMZ　　イ　IP マスカレード（NAPT）
ウ　ファイアウォール　　エ　プロキシサーバ

問11　全社的な推進体制で RPA を導入するときの留意点として，適切なものはどれか。

ア　各業務部門が連携して，RPA の対象業務に対して業務プロセス全体の可視化と業務プロセスの見直しを行った上で，RPA の導入を行う。
イ　業務フローが固定的で画面の変更が少ない業務よりも，業務フローの変更や画面の変更が多い業務から優先的に導入する。
ウ　情報システム部門や他部門との連携は行わずに，個々の業務部門が主導して，RPA ツールの選定，ソフトウェアロボットの作成，活用及び運用を推進する。
エ　ルール化された処理や繰返し処理が多い業務よりも，例外処理が多い業務や条件が複雑な業務に対して，優先的に RPA の導入を行う。

問12　特性要因図を説明したものはどれか。

ア　原因と結果の関連を魚の骨のような形態に整理して体系的にまとめ，結果に対してどのような原因が関連しているかを明確にする。

イ　時系列的に発生するデータのばらつきを折れ線グラフで表し，管理限界線を利用して客観的に管理する。

ウ　収集したデータを幾つかの区間に分類し，各区間に属するデータの個数を棒グラフとして描き，品質のばらつきを捉える。

エ　データを幾つかの項目に分類し，出現頻度の大きさの順に棒グラフとして並べ，累積和を折れ線グラフで描き，問題点を絞り込む。

〔 メ モ 用 紙 〕

問13　A 社は，従業員 100 名の食品製造・販売会社である。A 社では，営業部が取り扱う顧客情報を X 社の SaaS である X 顧客管理サービス（以下，X サービスという）を利用して管理している。また，A 社は，X サービスの不正アクセス対策として，X サービスへのログインは，A 社の社内ネットワークからだけ許可しており，A 社の社外からはできないように設定している。

X サービスに備わっている不正ログインを防止するための機能と，A 社が X サービスに適用している現在の設定を表 1 に示す。

表 1　不正ログインを防止するための機能と現在の設定（抜粋）

不正ログインを防止するための機能		現在の設定
機能 1	指定した IP アドレスからアクセスした場合だけ，ログインできるよう制限する。	有効 [1)]
機能 2	利用者 ID とパスワードによって認証する。	有効
機能 3	英字，数字，記号の 3 種類全てを含む 8 文字以上のパスワードを強制する。	有効
機能 4	ワンタイムパスワードによって認証する。	無効
機能 5	ログイン画面に CAPTCHA を表示し，回答させる。	無効

注 [1)]　A 社が使用しているグローバル IP アドレスを指定している。

A 社では，昨今の社会情勢を鑑みて，営業部員を対象にテレワーク制度の導入を検討することにした。社外からも X サービスを利用できるようにしたい。また，社外から不正アクセスされるリスクを低減するために，利用者認証を強化したい。そこで，機能 1～5 の設定について，必要な変更を二つ実施することにした。

設問　A 社が実施することにした設定変更の組合せはどれか。解答群のうち，最も適切なものを選べ。

解答群

	有効から無効に変更する機能	無効から有効に変更する機能
ア	機能 1	機能 4
イ	機能 1	機能 5
ウ	機能 2	機能 4
エ	機能 2	機能 5
オ	機能 3	機能 4
カ	機能 3	機能 5

問14　A 社は医療品の販売を行う従業員 100 名の企業である。営業部では，オンプレミスのデータベースに顧客情報を格納している。

営業部では，図 1 に示すバックアップポリシーを順守している。

1. データベースは毎週日曜日にフルバックアップを，それ以外の日は毎日の増分バックアップを毎日，別のテープメディアに取得する。
2. バックアップは 1 週間分保存する。
3. データベースの目標復旧時点（RPO）は 24 時間とする。
4. バックアップからの目標復旧時間（RTO）は 6 時間とする。
5. バックアップを保存しているテープメディア（以下，バックアップテープという）は鍵付きのキャビネットに保管する。
6. バックアップはシステムを停止せずに取得する。

図 1　営業部におけるバックアップポリシー

先日，金曜日に営業部では，アプリケーションの不具合によってデータベースの内部構造の破損（以下，論理破損という）が生じたので，データベースを復旧する必要が生じた。しかし，火曜日のバックアップテープが物理的に破損していたので，データベースをバックアップポリシーどおりには復旧できなかった。

そのため，営業部の情報セキュリティリーダーである B 課長は，論理破損が起き，かつ，バックアップテープが物理的に破損していたとしてもデータベースを復旧できるようにする再発防止策を検討し，効果の高いものを選んだ。

設問　B 課長が選んだ再発防止策はどれか。解答群のうち，最も適切なものを選べ。

解答群

ア　DBMS を IaaS 上に構築したサーバで稼働させ，データベースも IaaS 上に格納する。

イ　データベースのレプリケーションを行って，データベースのコピーを確保する。

ウ　データベースを格納しているディスクを RAID5 構成にする。

エ　テープメディアに加え，NAS にもバックアップを 1 週間分保存する。

オ　毎日 1 回システムを停止させ，フルバックアップを取得する。

〔 メ モ 用 紙 〕

問15　A社は，飲食店へのコンサルティングを行う従業員50名の企業である。A社の全ての PC では，マルウェア対策ソフト（以下，X ソフトという）が有効にされている。ある日，総務部の情報セキュリティリーダーであるC課長は，部下のDさんから，次の連絡を受けた。

・A社の PC の Web ブラウザで Web サイトを閲覧していたところ，PC がマルウェアに感染しているとの警告画面（以下，警告画面という）が全画面に表示された。
・警告画面が表示されたあと何も PC の操作をせずに直ちに C 課長に連絡をした。

C 課長は，情報システム部に報告した。情報システム部は D さんの PC を確認し，数時間後，図1のとおり報告した。

1. 警告画面には，次が表示されていた。
・X ソフトの製品のロゴ
・マルウェアを削除するためのツールをインストールする指示
・サポートが必要な場合の電話番号とチャットウィンドウ
2. 念のため，X ソフトを使って D さんの PC をスキャンしたが，マルウェアは検出されなかった。また，警告画面の表示は，X ソフトによるものではないことを確認した。
3. 昨今，類似した警告画面の事例の報告が日本国内で増えている。

図1　情報システム部からの報告

A 社では，警告画面が表示された場合の適切な対応について全従業員に周知することにした。

設問　周知すべきことはどれか。解答群のうち，最も適切なものを選べ。

解答群

ア　警告画面に，急いで対応する必要があるとの表示がある場合は，直ちに警告画面に表示された指示に従ってツールをインストールすること及びその具体的方法

イ　警告画面に表示された指示には従わずに，直ちに Web ブラウザを終了すること及びその具体的方法

ウ　警告画面に表示されたツールと競合しないように，X ソフトをアンインストールし，警告画面に表示された指示に従ってツールをインストールすること及びその具体的方法

エ　警告画面に表示された電話番号に直ちに連絡し，サポートオペレーターの指示に従うこと

オ　警告画面に表示されている，X ソフトの製品のロゴが，製品開発元の Web サイトに掲載されている正規の製品のロゴと同じである場合は，警告画面に表示された指示に従ってツールをインストールすること及びその具体的方法

〔 メ モ 用 紙 〕

〔 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。