令和８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　情報セキュリティのリスクマネジメントにおける残留リスクに関する記述のうち，適切なものはどれか。

ア　経営者の意思決定に従って保有したリスクは，残留リスクに含まれない。
イ　特定されていないリスクは，残留リスクに含まれない。
ウ　リスク対応を行った後に残るリスクは，残留リスクである。
エ　リスクを生じさせる活動を継続しないという決定によって回避したリスクは，残留リスクである。

問２　組織的なインシデント対応体制の構築を支援する目的で JPCERT コーディネーションセンターが作成したものはどれか。

ア　CSIRT マテリアル
イ　ISMS ユーザーズガイド
ウ　証拠保全ガイドライン
エ　組織における内部不正防止ガイドライン

問３　DMZ はどれか。

ア　インターネットと内部ネットワークとの間に設置されるネットワーク
イ　外部から持ち込んだ PC がマルウェアなどに感染していないかどうかを社内ネットワークに接続する前にチェックするための，社内ネットワークとは隔離された専用のネットワーク
ウ　通信内容を監視し，あらかじめ設定された不正な通信パターンと一致した場合に通信を遮断するネットワーク
エ　不正通信を検知する際に利用するためにセキュリティベンダーから入手するシグネチャ情報

問４　チャレンジレスポンス認証方式に該当するものはどれか。

ア　固定パスワードを，TLS による暗号通信を使い，クライアントからサーバに送信して，サーバで検証する。

イ　端末のシリアル番号を，クライアントで秘密鍵を使って暗号化し，サーバに送信して，サーバで検証する。

ウ　トークンという機器が自動的に表示する，認証のたびに異なる数字列をパスワードとしてサーバに送信して，サーバで検証する。

エ　利用者が入力したパスワードと，サーバから受け取ったランダムなデータとをクライアントで演算し，その結果をサーバに送信して，サーバで検証する。

問５　情報セキュリティでの脆弱(ぜいじゃく)性の検出に用いられるホワイトボックステストに該当するものはどれか。

ア　検査対象のソフトウェア製品に対して，外部仕様を基に，問題を引き起こしそうなデータを大量に送り込み，その応答や挙動を監視することによって脆弱性を検出する。

イ　検査対象のネットワークに対して，ネットワークの構成図や機器名などの情報を得ずに，TCP/IP に係る既知の脆弱性を攻撃し，実際に侵入できるかどうかを確認することによって脆弱性を検出する。

ウ　検査対象のプログラムの内部構造及び内部仕様を基に，脆弱性の可能性がある箇所の処理で使われる入力値を変化させて実行することによって脆弱性を検出する。

エ　検査対象のプログラムの内部仕様を参照せずに，変数領域のあふれを見つけ出すツールを利用して，バッファオーバフローの脆弱性を検出する。

問６　セキュア OS のアクセス制御と管理者権限管理を説明した適切な組みはどれか。

	アクセス制御	管理者権限管理
ア	リソースやプログラムのアクセス権は，OS の管理者が定めたセキュリティポリシーの下で一元的に制御され，リソースやプログラムの所有者が変更できない。	OS の管理の分野ごとに異なる管理用アカウントを作成し，各アカウントに必要最小限の管理者特権を与える。
イ	リソースやプログラムのアクセス権は，OS の管理者が定めたセキュリティポリシーの下で一元的に制御され，リソースやプログラムの所有者が変更できない。	OS の管理用に特権アカウントを作成し，特権アカウントに全ての権限を与える。
ウ	リソースやプログラムのアクセス権は，リソースやプログラムの所有者が保持し，制御する。	OS の管理の分野ごとに異なる管理用アカウントを作成し，各アカウントに必要最小限の管理者特権を与える。
エ	リソースやプログラムのアクセス権は，リソースやプログラムの所有者が保持し，制御する。	OS の管理用に特権アカウントを作成し，特権アカウントに全ての権限を与える。

問７　刑法の電子計算機損壊等業務妨害に該当する行為はどれか。

ア　自社の Web サイトで海賊版のソフトウェアを故意に販売した。

イ　存在しない商品をインターネットのオークションサイトに故意に出品し，落札者に現金を振り込ませてだまし取った。

ウ　他人の著作物を著作者に許可なく，引用元の記載もせずに，営業目的の自社の Web サイトに故意に掲載した。

エ　プロバイダのサーバに侵入し，サーバに保管されていたある企業が業務に使用している Web ページの内容を故意に消去したり，書き換えたりした。

問８　システム監査におけるフォローアップの説明として，適切なものはどれか。

ア　監査の品質管理体制を，システム監査人が事前に確かめておくこと
イ　監査報告書の指摘事項に基づいて監査対象先が実施した改善措置を，システム監査人が確認すること
ウ　システム監査の対象範囲に関する事項を，システム監査人が文書化すること
エ　システム監査の目的に応じた適切な形式で作成した監査報告書を，監査の依頼者及び関係者に提出すること

問９　サービスマネジメントにおける，サービスレベル目標の説明はどれか。

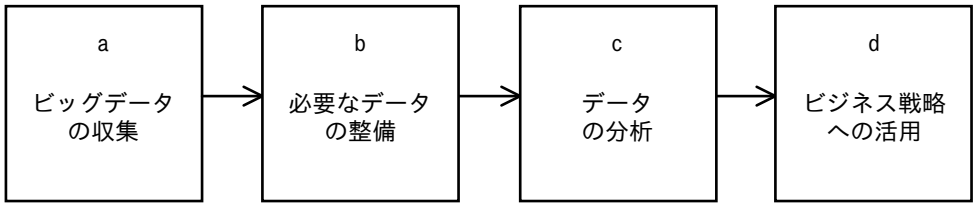
ア　意図した結果を達成するために，知識及び技能を適用する能力
イ　組織が約束する，具体的に測定可能なサービスの特性
ウ　トップマネジメントによって正式に表明された組織の意図及び方向付け
エ　明示されているか，通常，暗黙のうちに了解されているか，又は義務として要求されているニーズ又は期待

問10　次の IP アドレスとサブネットマスクをもつ PC がある。この PC のネットワークアドレスとして，適切なものはどれか。

IP アドレス：　　10.170.70.19
サブネットマスク：255.255.255.240

ア　10.170.70.0　　イ　10.170.70.16
ウ　10.170.70.31　　エ　10.170.70.255

問11　e コマース運営会社がビッグデータを用いて新たなニーズを発掘し，その後のビジネス戦略に生かそうとしている。ビッグデータの収集から活用までのフローを次の図のようにしたとき，データの分析で行うことはどれか。ここで，選択肢ア～エは，フロー図の a～d のいずれかに対応している。



ア　機械学習を用いて自然言語処理やクラスタリングを行い，新しい傾向を導き出す。

イ　取扱い製品に関する SNS での評価などを自動プログラムで取得する。

ウ　ノイズリダクション処理やデータクレンジング処理を行う。

エ　発見した新しい傾向を見極めて，注力すべきビジネス戦略を立案する。

問12　良品である確率が 0.9，不良品である確率が 0.1 の外注部品について，受入検査を行いたい。受入検査には四つの案があり，それぞれの良品と不良品 1 個に掛かる諸費用は表のとおりである。期待費用が最も低い案はどれか。

単位　円

案	良品に掛かる費用	不良品に掛かる費用
A	0	1,500
B	40	1,000
C	80	500
D	120	200

ア　A　　イ　B　　ウ　C　　エ　D

〔 メ モ 用 紙 〕

問13　A 社は，従業員 300 名の専門商社であり，機密性の高い情報も取り扱っている。最近，A 社は，駅前の B ビルの 6 階に移転した。6 階には A 社だけが入居している。

B ビルの 2 階から最上階の 17 階には多数の企業が入居しており，通常時はエレベーターを使用して各階に移動することができる。B ビルのビル管理業務は B 社が行っている。B 社はビルの入退館と入居企業の執務エリアの入退室を管理するシステム（以下，C システムという）を導入している。各入居企業は，C システムが発行する IC カード（以下，B カードという）を従業員に貸与している。各入居企業の執務エリアの出入口のドアは，当該企業が従業員に貸与した B カードをドア横の IC カードリーダーにかざすことによって解錠できる。

B ビルのエントランスホールは 1 階にあり，エレベーターホールとの境界には，フラッパーゲートが設置されている。フラッパーゲートを通過するには，フラッパーゲートのリーダーに B カード又は入館用に一時的に発行された QR コードをかざす必要がある。フラッパーゲートを通過すれば，平日の昼間はエレベーターの行先階ボタンを押すことで各階に自由に移動ができる。夜間と休日は，行先階の入居企業が従業員に貸与した B カードをエレベーター内の IC カードリーダーにかざす必要がある。

フラッパーゲートのすぐ外には階段室に入るための階段口があり，階段口にある非常ドアは通常時，エントランスホールには出られるが，階段室には入れない仕組みになっている。ほかの階の階段口にある非常ドアは通常時，各フロアには出られないが，階段室には入れる仕組みになっている。ただし，どの階の非常ドアも清掃時などに一時的に出入り可能になることがある。また，非常時は自動的に出入り可能になる。フラッパーゲートの脇にはごみ箱が設置されている。

〔来訪者管理〕

B ビルへの来訪者は，C システムで管理している。入居企業が C システムに，来訪者氏名，所属，来訪日，来訪者メールアドレスを登録すると，来訪日にだけ有効なゲスト入館用の QR コード付き入館証（以下，ゲスト入館証という）の画像ファイルが添付された電子メールが来訪者メールアドレスに送付される。来訪者は，来訪日当日に有効なゲスト入館証の QR コードを自身のスマートフォンの画面に表示するか又は印刷してフラッパーゲートのリーダーにかざすことによってフラッパーゲートを通過できる。当日に限り，同じ入館証で繰り返し入退館が可能なように C システムは設定

されている。

〔B ビルの物理的セキュリティにおける課題と B 社への依頼〕

ある日，突然，取引先の D 社の E 氏が予約なしに，A 社の情報セキュリティリーダーの F 部長を訪ねて 6 階の受付エリアにやって来た。驚いた F 部長は，E 氏が来たことをきっかけに B ビルの物理的セキュリティについて調査し，複数の課題があることを発見した。そして，F 部長はその課題と B 社への依頼を表 1 にまとめた。

表 1　B ビルの物理的セキュリティにおける課題と B 社への依頼（抜粋）

項番	課題	B 社への依頼
1	フラッパーゲート脇に設置されたごみ箱から印刷された使用済のゲスト入館証を拾えば，1 階のフラッパーゲートを通過し入館できてしまう。	a1
2	6 階以外への来訪者が，ゲスト入館証で 1 階のフラッパーゲートを通過すれば，平日の昼間はエレベーターで 6 階に移動できてしまう。	a2

設問　次の依頼のうち，表 1 中の［ a1 ］，［ a2 ］に入れるものの組合せはどれか。a に関する解答群のうち，最も適切なものを選べ。

（一） C システムの設定を変更し，ゲスト入館証の QR コードの誤り訂正レベルの設定を高くする。

（二） C システムの設定を変更し，ゲスト入館証は 1 回限り入館可能にする。

（三） エレベーターで行先階に移動するためには，平日の昼間も IC カードリーダーに B カードをかざすことを必要とする。そのため，各入居企業には，当該企業の従業員が 1 階のエレベーター前から当該企業まで来訪者をアテンドするよう要請する。

（四） 警備員を 1 階のフラッパーゲート脇に配置し，不正に入館しようとしている者がいないかどうかを監視する。

a に関する解答群

	a1	a2
ア	(一)	(二)
イ	(一)	(三)
ウ	(二)	(一)
エ	(二)	(三)
オ	(二)	(四)
カ	(三)	(一)
キ	(三)	(二)
ク	(三)	(四)
ケ	(四)	(一)
コ	(四)	(二)

〔 メ モ 用 紙 〕

問14　A 社は従業員 200 名の電子機器メーカーである。東京に本社があり，新潟に工場がある。

A 社では，ファイルサーバを図 1 のように運用している。

・ファイルサーバは本社と工場のサーバルームに設置している。
・ファイルサーバは，磁気テープを使用してファイルのバックアップを取得している。
・土曜日の午前 2 時からフルバックアップを取得し，翌週の火曜日と木曜日の午前 2 時から増分バックアップを取得している。
・情報システム部の担当者は毎週月曜日，火曜日，木曜日の朝 10 時頃，バックアップジョブの実行結果の確認と磁気テープの交換を行い，磁気テープは耐火金庫に保管している。
・磁気テープには上書きモードでバックアップを取得し，1 か月分の磁気テープを世代管理している。
・これまで，フルバックアップからのリストアには平均して 4 時間，1 回の増分バックアップからは平均して 0.25 時間掛かっている。
・A 社は ICT 継続のための試験を実施しており，ファイルサーバも試験対象である。

注記　事業影響度分析の結果に基づき，ファイルサーバは，72 時間の目標復旧時点（RPO）と 120 時間の目標復旧時間(RTO)が要求事項として定められている。

図 1　A 社のファイルサーバの運用

A 社は ISMS 認証を取得しており，最高情報セキュリティ責任者（CISO）を中心に情報セキュリティに取り組み，定期的に，情報セキュリティリスクアセスメントを行っている。今般，ISMS 認証基準が JIS Q 27001:2023 に改正されたことを受け，情報セキュリティリーダーの B さんは，新基準への移行審査に向けて準備することになった。改正によって新たに追加された情報セキュリティ管理策について，B さんは情報システム部の担当者に取組状況を確認し，その評価結果を表 1 にまとめた。

表 1　B さんの評価結果（抜粋）

項番	情報セキュリティ管理策	評価結果
1	（事業継続のための ICT の備え）事業継続の目的及び ICT 継続の要求事項に基づいて，ICT の備えを計画し，実施し，維持し，試験しなければならない。	実施している

B さんは，移行審査前の内部監査で，内部監査室から表 1 の項番 1 に関するファイルサーバの運用について何点か質問を受け，表 2 のとおり回答した。

表 2　内部監査室への B さんの回答（抜粋）

項番	B さんの回答
1	例えば，金曜日の正午に障害が発生した場合，少なくとも［ a1 ］の時点のデータは復元しなければならない。
2	例えば，木曜日の正午に障害が発生し，ファイルサーバの全データが消失したとすると，バックアップからのリストアには［ a2 ］時間掛かると予想される。
3	ICT 継続の計画書は，［ a3 ］が承認している。

設問　表 2 中の［ a1 ］～［ a3 ］に入れる字句の適切な組合せを，a に関する解答群の中から選べ。

a に関する解答群

	a1	a2	a3
ア	月曜日の正午	4.25	CISO
イ	月曜日の正午	4.25	情報システム部の担当者
ウ	月曜日の正午	4.25	内部監査室長
エ	月曜日の正午	4.50	CISO
オ	月曜日の正午	4.50	情報システム部の担当者
カ	火曜日の正午	4.25	情報システム部の担当者
キ	火曜日の正午	4.25	内部監査室長
ク	火曜日の正午	4.50	CISO
ケ	火曜日の正午	4.50	情報システム部の担当者
コ	火曜日の正午	4.50	内部監査室長

問15　A 社は従業員 300 名の商社である。総務部が定めた A 社の文書管理ルールを図 1 に示す。

〔文書の機密区分〕
極秘　　：経営に関する重要な文書であり，経営企画に関わる者だけに開示する。経営企画書など。
関係者外秘　：特定の関係者だけに開示する。議事メモ，顧客情報など。
社外秘　　：社内だけに開示する。クレーム情報，社内報など。
公開　　：社外に公開可能なもの。商品カタログなど。

〔機密区分のラベリング〕
・文書を作成した部署の責任者が，機密区分を判断する。
・“極秘”，“関係者外秘”及び“社外秘”の文書は，機密区分をその文書のヘッダー部に明記する。
・“極秘”と“関係者外秘”に関しては開示範囲を明示するため，“役員だけ 極秘”や“○○部だけ 関係者外秘”という形式で明記する。

〔文書の保管〕
・“極秘”及び“関係者外秘”の紙の文書は，使わないときや利用中に離席するときはキャビネットに保管する。キャビネットは常時施錠し，関係者だけが解錠できるようにする。

〔文書の廃棄〕
・“極秘”，“関係者外秘”及び“社外秘”の紙の文書を廃棄する際は，シュレッダーで細断する。

図 1　文書管理ルール（抜粋）

総務部の情報セキュリティリーダーである S さんは，各部に対し年次の自己点検を指示した。その結果を基に，図 1 のルールに沿って文書を取り扱っているかを確認するために，A 社の一部の従業員にヒアリングしたところ，図 2 に示す事例が得られた。

(1) 営業部の B さんの大学の後輩である C さんは，A 社の入社試験を受ける予定なので，B さんは C さんに社内報を見せた。
(2) “営業部だけ 関係者外秘”の議事メモは，営業部員だけが解錠できるキャビネットに保管している。不要となったものは毎週水曜日に，シュレッダーで細断して廃棄している。
(3) 昨年営業部に異動した元人事部の D さんが，営業部の事業計画の参考にするため，人事部の E さんから“人事部だけ 関係者外秘”の来年度の採用計画を見せてもらった。
(4) 経営企画部の G さんは，来期の経営企画書のうち一部の作成を指示されていたが，机の上の本立てに最終原稿を差し込んで会議に向かった。
(5) 人事部の I さんは就職セミナーで，営業部から借りた商品カタログを参加者に見せながら会社紹介をした。

図 2　S さんが A 社の従業員へのヒアリングによって得た事例

S さんは図 2 の事例について，図 1 に沿っているかどうかを評価し，表 1 のとおりまとめた。

表 1　ヒアリングで得た事例に対する評価

図 2 の項番	評価
(1)	(省略)
(2)	a1
(3)	a2
(4)	a3
(5)	(省略)

注記　評価は，図 1 に沿っていれば“○”，沿っていなければ“×”とする。

設問　表 1 中の [a1] ～ [a3] に入れる評価の適切な組合せを解答群の中から選べ。

a に関する解答群

	a1	a2	a3
ア	○	○	○
イ	○	○	×
ウ	○	×	○
エ	○	×	×
オ	×	○	○
カ	×	○	×
キ	×	×	○
ク	×	×	×

〔 メ モ 用 紙 〕

〔 メ モ 用 紙 〕

〔 メ モ 用 紙 〕