令和７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）におけるリスクマネジメントプロセスに関する記述のうち，適切なものはどれか。

ア　リスク対応の意義は，プロセスの設計，実施及び結末の質及び効果を保証し，改善することである。

イ　リスク特定の意義は，リスクに対処するための選択肢を選定し，実施することである。

ウ　リスク評価の意義は，組織の目的の達成を助ける又は妨害する可能性のあるリスクを発見し，認識し，記述することである。

エ　リスク分析の意義は，必要に応じてリスクのレベルを含め，リスクの性質及び特徴を理解することである。

問２　SIEM 製品によるセキュリティ上の効果として，最も適切なものはどれか。

ア　様々な機器のログを集中管理することによって，横断的な分析や相関分析が可能になり，単純な目視だけでは発見困難な兆候を検知，分析，可視化することが可能になる。

イ　通信経路上を流れるパケットをキャプチャし，暗号化されたデータが改ざんされていないかどうかをチェックすることが可能になる。

ウ　ファイアウォール，IDS，マルウェア対策といった複数のネットワークセキュリティ機能を一つの機器で実現することが可能になる。

エ　ファイルの改ざんを検知すると，事前に取得済みのバックアップを用いて直ちに修復することが可能になる。

問３　ゼロトラストの説明として，最も適切なものはどれか。

ア　機器やソフトウェアの脆弱性のうち，開発元から対策方法，修正プログラムなどが提供されていない脆弱性が残っている状態のこと
イ　内部ネットワークであっても必ずしも安全ではないことを前提として対策を講じる考え方のこと
ウ　秘密情報そのものは明かさずに，自分が秘密情報を知っていることを相手に知らせる方法のこと
エ　マルウェア定義ファイルを用いず，PC の振る舞いからマルウェア感染を検知する手法のこと

問４　不正が発生する際には“不正のトライアングル”の 3 要素全てが存在すると考えられている。“不正のトライアングル”の構成要素の説明として，適切なものはどれか。

ア　“機会”とは，情報システムなどの技術や物理的な環境，組織のルールなど，内部者による不正行為の実行を可能又は容易にする環境の存在である。
イ　“情報と伝達”とは，必要な情報が識別，把握及び処理され，組織内外及び関係者相互に正しく伝えられるようにすることである。
ウ　“正当化”とは，ノルマによるプレッシャなどのことである。
エ　“動機”とは，良心のかしゃくを乗り越える都合の良い解釈や他人への責任転嫁など，内部者が不正行為を自ら納得させるための自分勝手な理由付けである。

問５　DNS キャッシュサーバでの DNS キャッシュポイズニング攻撃の対策はどれか。

ア　DNS サービスの待ち受けポートを 53 番に固定する。
イ　外部の DNS クライアントからの再帰的問合せを受け付けない設定にする。
ウ　権威 DNS サーバへの問合せに使用するトランザクション ID を固定する。
エ　権威 DNS サーバへの非再帰的問合せを行う設定にする。

問６　CVSS v3 について，基本評価基準，現状評価基準，環境評価基準のうち，現状評価基準の特徴はどれか。

ア　攻撃コードの出現の有無，利用可能な対策のレベルなどに応じ，評価結果は時間の経過で変化する。

イ　脆弱性及び想定される脅威に応じ，製品利用者ごとに評価結果は異なる。

ウ　製品利用者が脆弱性への対応を決めるための評価に用いる基準であり，評価結果は時間の経過で変化しない。

エ　評価結果は利用環境によらず同じで，かつ，時間の経過でも変化しない。

問７　特定電子メール法の説明として，適切なものはどれか。

ア　特定電子メール法は，広告のための電子メールの送信を受託した事業者だけを規制している。

イ　特定電子メール法の規制は，受信者から受信拒否の通知があった場合にだけ広告宣伝メールを禁止するオプトアウト方式を採用している。

ウ　特定電子メール法の目的は，取引の公平の観点から広告宣伝メールを規制すること及び犯罪捜査のための通信傍受である。

エ　特定電子メール法は，規制の対象となる電子メールの送信者及び送信委託者に対する義務を規定している。

問８　情報セキュリティ違反を犯した従業員に対する懲戒手続を規定した就業規則を含む社内規程の内容について，情報セキュリティ管理基準（平成 28 年）に基づき監査を実施した。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　従業員による情報セキュリティ違反の可能性を認識したら，直ちに懲戒手続を開始することを定めていた。

イ　懲戒手続は，情報セキュリティ違反による業務への影響度，違反を犯した従業員に対する教育の実施状況などを考慮した段階別の対応を定めていた。

ウ　懲戒手続は，情報セキュリティ違反を犯した従業員に対する恣意性を排除した公平な取扱いを定めていた。

エ　懲戒手続を具体化した細則を策定すること，及び従業員に周知徹底することを定めていた。

問９　サービス満足度の目標値を“サービス満足度に関する調査アンケートの満足度の平均点が 5 点満点中 4.0 点”と設定したサービスがある。調査アンケートの集計結果が表のとおりであるとき，目標達成率は幾らか。ここで，目標達成率は次式で計算するものとする。

目標達成率 ＝ 満足度の平均点 ÷ 満足度の目標値

〔集計結果〕

満足度（点）	回答数
5	50
4	250
3	150
2	50
1	0

ア　0.6　　イ　0.72　　ウ　0.8　　エ　0.9

問10　システムの信頼性指標である RASIS の，安全性を除く四つに関する記述のうち，適切なものはどれか。

ア　R の信頼性は，システムの MTBF によって表す。
イ　A の可用性は，システムが稼働している時間の平均値によって表す。
ウ　S の保守性は，システムの稼働率によって表す。
エ　I の完全性は，システムの故障率によって表す。

問11　企業全体で使用するデータを統合・整理したデータウェアハウスから，特定の分析目的のためにデータを加工して構築したものはどれか。

ア　データカタログ　　イ　データマート
ウ　データリネージ　　エ　データレイク

問12　経済産業省が取りまとめた“DX レポート 2”では，組織が DX 実現に至る段階をデジタイゼーション，デジタライゼーション，デジタルトランスフォーメーションに分けている。製造業のデジタル化事例において，デジタルトランスフォーメーションの段階に達しているものはどれか。

DX 実現に至る段階	説明
デジタイゼーション	アナログ・物理データのデジタルデータ化
デジタライゼーション	個別の業務・製造プロセスのデジタル化
デジタルトランス フォーメーション	組織横断／全体の業務・製造プロセスのデジタル化， “顧客起点の価値創出”のための事業やビジネスモデルの変革

ア　3D 画像撮影用の高性能カメラを生産ラインに設置し，カメラの前を通過する製造物のデジタル画像をリアルタイムで記録して，出荷検査の証拠データとする。

イ　技術継承のために，生産ラインに設置したカメラと，熟練工の手に装着したウェアラブルセンサーによって，熟練工の所作をデジタルデータとして保存した上で，AI を用いて熟練工の動きをモデル化する。

ウ　顧客から販売・在庫情報を，部品メーカーから生産・在庫情報をデジタルデータで逐次入手し，AI を用いて複数の需給調整案を高速でシミュレーションすることによって，サプライチェーン全体を最適化する。

エ　生産ラインで取得したデジタル画像データから良品，不良品の特徴を AI に学習させた上で，AI で画像解析を行うことによって，自社の出荷時検品作業を効率化する。

問13　A社は従業員300名のITサービス企業であり，ヘルプデスク業務のアウトソーシングサービスを提供している。A 社はオンプレミスのシステムを所有しておらず，顧客向けサービスのほか，社内業務でもクラウドサービスを利用している。A 社では，各従業員に PC 及びスマートフォンを貸与している。スマートフォンは勤怠管理などの社内業務だけに利用している。

A 社では，クラウドサービスについての可用性に関する重要度の評価（以下，可用性に関する重要度の評価を可用性評価という）を本来実施すべきであったが，実施できていなかった。そこで，A 社の情報セキュリティリーダーである B 主任が，表 1 のとおり，A 社がリスク評価で用いる可用性評価の基準を用いて可用性評価を実施することになった。

表 1　A 社がリスク評価で用いる可用性評価の基準

重要度	可用性評価の基準	該当するサービスの例
2	サービスが利用できなくなると自社だけではなく，顧客にも直ちに影響がある。	顧客に提供しているサービス，顧客にサービスを提供するために利用している外部のサービス
1	サービスが利用できなくなると自社にだけ，直ちに影響がある。	重要度 0 のサービスを除く，社内で利用しているサービス
0	サービスが利用できなくなっても自社及び顧客に，直ちに影響はない。	社内でデータの長期保存に利用しているサービス

B 主任は A 社が利用しているクラウドサービスについて可用性評価を実施し，利用方法及び可用性に関する重要度を表 2 のとおりまとめた。

表 2　B 主任がまとめた可用性評価の結果（抜粋）

A 社が利用しているクラウドサービス	利用方法	可用性に関する重要度
電子メール	ヘルプデスク利用者からの電子メールによる問合せの受付及び回答に利用する。回答は原則として電子メールで行うが，回答に機密性の高い情報が含まれる場合は，あらかじめ登録されているヘルプデスク利用者の電話番号に A 社から電話する。	a1
人事・労務管理	マイナンバーを含む人事情報の管理及び労務管理に利用する。	a2

B 主任は，表 2 の内容を A 社の情報セキュリティ委員会に報告し，可用性に関する重要度が適切であることの承認を得た。

設問　表 2 中の [a1] ，[a2] に入れる数値の適切な組合せを，a に関する解答群の中から選べ。

a に関する解答群

	a1	a2
ア	0	0
イ	0	1
ウ	0	2
エ	1	0
オ	1	1
カ	1	2
キ	2	0
ク	2	1
ケ	2	2

問14　A 社は，従業員 300 名の部品メーカーである。A 社ではこれまで，業務に必要なファイルを他社との間で受け渡す場合には電子メール（以下，メールという）を利用してきた。最近になって，取引先の B 社から，ファイルの受渡しについては，C サービスというクラウドストレージサービスを利用して欲しいとの要請を受けた。図 1 は，C サービスを利用した場合のファイル受渡しの流れである。

1　ファイルの送信者は，受信者に渡したいファイルを C サービス上にアップロードする。アップロードされたファイルは，C サービス上では暗号化されて保存される。
2　ファイルの送信者は，受信者をメールアドレスで指定して，ファイルのアクセス権を付与する。アクセス権の付与や取消しはいつでも行える。
3　受信者にアクセス権が付与されると，ファイルのダウンロード用 URL が生成され，指定されたメールアドレスにメールで通知される。なお，URL には推測困難な文字列が含まれている。
4　受信者が，メールに記載された URL にアクセスして自身のメールアドレスを入力すると，復号されたファイルがダウンロードされる。
5　ファイルがダウンロードされると，送信者の利用者 ID，アップロード日時，ファイル名，ファイルのダウンロード用 URL，ダウンロードの際のアクセス元 IP アドレス，4 で入力したメールアドレス及びダウンロード日時がログに記録される。
6　送信者は，自身のアップロードしたファイルについて，ダウンロードのログを確認できる。

注記　C サービスとの通信には HTTPS（HTTP over TLS）が用いられている。

図 1　ファイル受渡しの流れ

そこで A 社では，C サービスを利用した場合のリスクを評価するために，検討会を開催した。検討会において，情報セキュリティリーダーの D 主任は，次のとおり説明した。

C サービスを利用することによって，情報漏えいのリスクを低減でき，さらに情報漏えいの有無も確認できる。具体的には，ファイルの送信者は，誤ったメールアドレスを指定してメールを送信してしまった場合に，誤りに気付いた時点で，すぐに［　a1　］を行うことができる。次に，ファイルが［　a2　］されていないことがログによって確認できれば，［　a3　］していないと判断することができる。

設問　本文中の［ a1 ］～［ a3 ］に入れる次の字句の組合せはどれか。a に関する解答群のうち，最も適切なものを選べ。

（一） アクセス権の取消し

（二） アップロード

（三） 情報漏えい

（四） ダウンロード

（五） メールで通知

（六） メールに記載された URL に受信者はまだアクセス

a に関する解答群

	a1	a2	a3
ア	（一）	（二）	（三）
イ	（一）	（二）	（六）
ウ	（一）	（四）	（三）
エ	（一）	（四）	（六）
オ	（五）	（二）	（三）
カ	（五）	（二）	（六）
キ	（五）	（四）	（三）
ク	（五）	（四）	（六）

問15　A 社は，スマートフォン用ヘルスケア関連アプリケーションソフトウェア（以下，A アプリという）の開発，販売を行う会社である。A アプリは，ヘルスケアデータ収集機能によって，利用者の体重や歩数のデータを収集するとともに，アンケート機能によって，勤務先の業種，年収などのデータを収集している。

営業部は，保険会社である B 社と共同のビジネスを検討している。その中で，A アプリで収集したデータ及び今後収集するデータから匿名加工情報を作成した上で，その匿名加工情報を B 社に第三者提供することを検討している。B 社では，提供を受けた匿名加工情報を分析して，B 社の保険商品のマーケティングに活用しようとしている。分析の対象は，年代，性別，年収区分，住んでいる地域区分及び勤務先の業種と体重及び歩数との関係である。ここで，地域区分とは，北海道，東北，南関東などの区分のことをいう。

加工対象となる“個人情報データベース等”（以下，加工対象情報という）は，表 1 の顧客属性データと表 2 のヘルスケアデータの 2 種類からなり，利用者番号によって関連付けられている。

表 1　顧客属性データ

利用者番号	氏名	性別	生年月日	電子メールアドレス	住所	勤務先の業種	年収
114567	情報 一郎	男	1984 年 4 月 4 日	ichiro@●●●.ne.jp	愛知県名古屋市中区上前津 X-X-X	金融業	1,850 万
114568	積招 花子	女	2003 年 3 月 31 日	sekimane@▲▲▲.ne.jp	東京都文京区本駒込 X-X-X	小売業	380 万
114573	試験 五郎	男	1951 年 12 月 9 日	shiken@■■■.ne.jp	東京都中央区月島 X-X-X	製造業	630 万
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

表 2　ヘルスケアデータ

利用者番号	記録日	体重	歩数
114567	202N 年 02 月 11 日	121.3	5,321
114568	202N 年 02 月 11 日	43.5	33,012
114568	202N 年 02 月 12 日	43.0	12,007
114573	202N 年 02 月 12 日	63.0	7,604
⋮	⋮	⋮	⋮

営業部の情報セキュリティリーダーであるC課長は，加工対象情報に含まれる各情報の項目について，適用する匿名加工情報の作成に係る手法（以下，匿名加工情報の作成に係る手法を匿名加工手法という）を表3にまとめた。

表3　匿名加工手法

項番	手法名	解説
(一)	項目削除	加工対象情報に含まれる個人情報の項目を削除すること。例えば，年齢のデータを加工対象情報から削除すること。
(二)	一般化	加工対象情報に含まれる記述などについて，上位概念に置き換えること。例えば，購買履歴のデータで“きゅうり”を“野菜”に置き換えること。
(三)	トップ（ボトム）コーディング	加工対象情報に含まれる数値について，特に大きい又は小さい数値をまとめること。例えば，年齢に関するデータで，“98歳”，“115歳”といった数値データを“80歳以上”というデータにまとめること。
(四)	丸め	加工対象情報に含まれる数値について，四捨五入などして丸めること。例えば，生年月日から“34歳”とされる場合について，“30代”のように年代に置き換えること。

注記　本表は，個人情報保護委員会事務局“仮名加工情報・匿名加工情報 信頼ある個人情報の利活用に向けて一制度編一(第2版)”を基にC課長が作成した。

C課長は，加工対象情報である表1及び表2に示す各データに対して，表3の匿名加工手法を必要に応じて適用し匿名加工情報を作成する案を用意した。その案を法務部のD課長に報告したところ，D課長からは，想定するマーケティング用途にも有効であり，匿名加工手法の適用も適切であるとの回答を得た。

設問　解答群に示した 3 項目それぞれについて，C 課長が適用した匿名加工手法はどれか。表 3 の手法のうち，適用したものの組合せを，解答群の中から選べ。なお，各項目に対して複数の匿名加工手法を適用しても構わないし，一つも適用せずに“加工なし”としても構わない。

解答群

	電子メールアドレス	勤務先の業種	体重
ア	加工なし	加工なし	(三)
イ	加工なし	加工なし	(三)，(四)
ウ	加工なし	(一)	(一)
エ	加工なし	(一)	(三)
オ	加工なし	(一)	(三)，(四)
カ	(一)	加工なし	(三)
キ	(一)	加工なし	(三)，(四)
ク	(一)	(一)	(一)
ケ	(一)	(一)	(三)
コ	(一)	(一)	(三)，(四)

〔 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。