

平成 26 年度 春期 情報セキュリティスペシャリスト

<午前 I 解答・解説>

●問 1 正解：イ

2進数の小数は，次のように桁が下がるごとに 10 進数 0.5 のべき乗となる。

$$0.1(2) = \frac{1}{2^1} = 0.5(10)$$

$$0.01(2) = \frac{1}{2^2} = 0.25(10)$$

$$0.001(2) = \frac{1}{2^3} = 0.125(10)$$

$$0.0001(2) = \frac{1}{2^4} = 0.0625(10)$$

解答群の中で，アの 0.375，ウの 0.625，エの 0.75 については，2 進数で表すとそれぞれ 0.011, 0.101, 0.11 となり，無限小数とはならない。したがって正解はイの 0.45 である。

●問 2 正解：ウ

表より，最後のビットが「0」で終わるのは a か c しかないとわかる。

ビット列 110 を読み込む直前の状態が不明であるため，a～d に当てはめてみると，次のようにいずれの場合も c が受理状態となる。

110 を読み込む直前の状態が a の場合：a→(1)→b→(1)→d→(0)→c

110 を読み込む直前の状態が b の場合：b→(1)→d→(1)→d→(0)→c

110 を読み込む直前の状態が c の場合：c→(1)→b→(1)→d→(0)→c

110 を読み込む直前の状態が d の場合：d→(1)→d→(1)→d→(0)→c

一方，a が受理状態となるには，次のように，末尾の 2 ビットが「00」である必要がある。

a→(0)→a→(0)→a

b→(0)→c→(0)→a
 c→(0)→a→(0)→a
 d→(0)→c→(0)→a

したがってウが正解。

●問3 正解：イ

ベストフィット方式は、メモリの空きブロック群のリスト全体を検索し、要求サイズに合致した最小の空きブロックを割り当てる方式である。大きな空きブロックを分割して割り当てることはなく、最もフィットする空きブロックを使用する。その結果、割り当てごとに小さい空き領域が生じ、最終的には小さな空きブロックが多数残る傾向がある。したがってイが正解。

●問4 正解：ア

0 ミリ秒から 5 ミリ秒までの間にメイン処理、割込み A、割込み B が使用する CPU 時間を図で表すと次のようになり、メイン処理が利用できるのは 2 ミリ秒であることがわかる。したがってアが正解。

	割込みA		↓0.5		↓0.5	↓0.5				
	割込みB	↓0.5	0.5	0.5					↓	
	メイン処理				0.5	0.5	0.5	0.5		
		0	1	2	3	4	5	時間 (ミリ秒)		

●問5 正解：ア

稼働率は、**MTBF** (Mean Time Between Failure : 平均故障間隔) と **MTTR** (Mean Time To Repair : 平均修理時間) を用いて次の式で表すことができる。

$$\text{稼働率} = \text{MTBF} / (\text{MTBF} + \text{MTTR})$$

上の式より、MTBF と MTTR が等しい場合、稼働率は $\frac{1}{2} = 0.5$ となることがわかる。

したがってアが正解。

●問6 正解：エ

プリエンプティブ、ノンプリエンプティブとは、マルチタスク OS においてプロセスを切り替える方式のことである。

プリエンプティブは、OS が CPU の割り当てを管理し、優先度などによりプロセスを強制的に切り替えて実行する方式である。

一方、ノンプリエンプティブは、OS が CPU の割り当てを管理せず、プロセスの切り替えをプロセス自身が行う方式である。

ア 各プロセスではなく OS が管理する。

イ ノンプリエンプティブ方式に比べ、オーバーヘッドは大きくなる。

ウ OS が強制的にプロセスを切り替えるため、特定のプロセスがプロセッサを独占することは少なくなる。

エ 正しい記述である。

したがってエが正解。

●問7 正解：イ

NAND とは、「NOT AND」であり、AND 演算と逆の結果となる。

X, Y は、次の組合せとなる。

X: 0 1 0 1

Y: 0 0 1 1

このとき、図の左上の NAND 素子 ($X \text{ NAND } X$)、左下の NAND 素子 ($Y \text{ NAND } Y$)、Z の出力結果はそれぞれ次のようになる。

$X \text{ NAND } X$: 1 0 1 0

$Y \text{ NAND } Y$: 1 1 0 0

Z : 0 1 1 1

そして、ア～エの出力はそれぞれ次のようになる。

ア : $X \cdot Y$: 0 0 0 1

イ : $X + Y$: 0 1 1 1

ウ : $X \cdot Y$: 1 1 1 0

エ : $X + Y$: 1 0 0 0

この結果から、出力 Z を表す式は $X + Y$ であることがわかる。したがってイが正解。

●問8 正解：ウ

UML (Unified Modeling Language) とは、オブジェクト指向型のソフトウェア開発における分析・設計段階で、システムをモデル化するための表記方法を統一したものである。

図中の"1", "*"は多重度を表しており, "1"は最小の値を, "*"は任意の数(n)まで多重することを意味している。

このことから、問題のデータモデルは次のように解釈できる。

- ・社員から見た部門の多重度は"1"であるため、社員は一つの部署に所属する。
- ・部門から見た社員の多重度は"*"であるため、部門には複数（任意の数）の社員が所属する。

ア 社員が 0 人の部門も登録可能である。

イ 社員は一つの部門に所属する。

ウ 社員は必ず一つの部門に所属するため、正しい記述である。

エ 一つの部門には複数の社員が所属できる。

したがってウが正解。

●問9 正解：イ

図は 2 相コミットプロトコルのコマンドシーケンスを表している。

2 相コミットは、コミットを開始する一人の「調停者」と、複数の「参加者」によって行われる。まず、調停者が参加者全員に対してコミットの可否を問い合わせる。その結果、すべての参加者が了承した場合はコミットが成立し、調停者はコミットの決定を参加者に送る。一方、一つでも拒否があればコミットは成立せず、調停者はロールバックの決定を参加者に送る。

図では、調停者からの **COMMIT** 可否問合せに対し、システム 1 は「可」、システム 2 は「否」を返しているため、コミットは成立せず、調停者はシステム 1 とシステム 2 に「**ROLLBACK** の実行要求」を発行する。したがってイが正解。

●問 10 正解：イ

トランザクションの信頼性を保証するための条件として、原子性 (atomicity)、一貫性 (consistency)、独立性 (isolation)、耐久性 (Durability) の 4 つがあり、頭文字をとって ACID 特性と呼ばれる。ACID 特性の内容は次の通り。

- ・原始性：トランザクションは完全に実行されるか、まったく実行されないかのいずれかであること
- ・一貫性：データベースの内容に矛盾がないこと
- ・独立性：複数のトランザクションを並行して実行した場合と、順番に実行した場合の処理結果が一致すること
- ・耐久性：正常終了したトランザクションの処理結果は、障害が発生してもデータベースから失われないこと

したがってイが正解。

●問 11 正解：エ

問題文に該当するのは SNMP (Simple Network Management Protocol) である。

SNMP は、サーバやルータなど、TCP/IP ネットワークに接続された機器の状態を監視・管理するためのプロトコルであり、ネットワーク上に存在する管理対象の機器 (エージェント) と、その管理を司る機器 (マネージャ) との間で管理情報をやり取りする。したがってエが正解。

ア NNTP (Network News Transfer Protocol) は、NetNews においてメッセージ転送に用いられるプロトコルである。

イ NTP (Network Time Protocol) は、複数のコンピュータで時刻同期をとるために用いるプロトコルである。

ウ SMTP (Simple Mail Transfer Protocol) は、電子メールを送信するために使用するプロトコルである。

●問 12 正解：エ

認証局が侵入されたのであるから、ブラウザで当該認証局を信頼していない設定にするのが適切な対処である。そうすることにより、当該認証局により発行されたデジタル証明書を使用したサイトにアクセスしようとするときブラウザでエラーが表示される。したがってエが正解。

●問 13 正解：ア

SQL インジェクションとは、ユーザの入力値を基にデータベースに SQL 命令を発行するしくみになっている Web アプリケーションにおいて、不正な SQL 命令を混入させることで、データを改ざんしたり、不正に取得したりする攻撃手法である。SQL インジェクションを防ぐには、データベースのバインド機構を用いるのが有効である。

バインド機構とは、変数部分にプレースホルダと呼ばれる特殊文字（「?」など）を使用して SQL 文の雛形をあらかじめ用意しておき、後からそこに実際の値を割り当てて SQL 文を完成させる方法である。割り当てられる変数は完全な数値定数もしくは文字列定数として扱われるため、変数の中に SQL 文として特別な意味をもつ文字が含まれていたとしても、それらは自動的にエスケープ処理され、単なる文字として認識される。したがってアが正解。

なお、バインド機構以外の SQL インジェクション対策として、入力値を処理する Web アプリケーションにおいて、入力値中の"'"、";", "%", "+"など、SQL 文として特別な意味をもつ文字（メタキャラクタ）を取り除いたり、他の文字に置き換えたりする方法（これをエスケープ処理という）もある。

●問 14 正解：エ

フォレンジックス（フォレンジックともいう）とは、事件や事故の証拠を収集し、裁判で立証する行為を意味する。デジタルフォレンジックス（コンピュータフォレンジックスともいう）とは、データの改ざんや不正アクセスなどコンピュータに関する犯罪の法的な証拠性を明らかにするために、原因究明に必要な機器やデータ、ログなどを保全したり、収集・分析したりすることである。したがってエが正解。

●問 15 正解：エ

SSH（Secure SHell）は、当初は rlogin, rsh など BSD 系 UNIX を起源とする r 系のコマンドや、X11, Telnet など安全に行うための手段として使用されていたが、現在では FTP, POP3 など、暗号化機能を備えていないプロトコルを安全に使用する技術として広く使用されている。したがってエが正解。

●問 16 正解：ア

経済産業省が発行している「システム／ソフトウェア製品の品質要求定義と品質評価のためのメトリクスに関する調査報告書」によれば、システム／ソフトウェア製品の品質特性として、次のような項目がある。

- ・機能適合性

製品やシステムが定められた利用状況下で定められて包含されたニーズを満たす機能を提供する度合い

- ・性能効率性

定められた利用状況下で利用される資源量の性能の度合い

- ・互換性

製品、システム、コンポーネントが他の製品、システムコンポーネントと情報を変換できる度合い、また、同じハードウェアやソフトウェア環境を共有し、要求される機能を実行する度合い

- ・使用性

製品やシステムが、定められたユーザにより、定められた使用状況下で効果的、効率的、満足度が達成される度合い

- ・信頼性

システム、製品やコンポーネントが制限時間内で定められた状況の下で機能を実行する度合い

- ・セキュリティ

人やシステムによる読み込み・修正などが不当にアクセスされることなく情報やデータが保護されている度合い

- ・保守性

製品やシステムが保守担当により修正するにあたっての効果性、効率性の度合い

- ・移植性

システムや製品、コンポーネントがハードウェアやソフトウェア、運用、利用環境を他へ移行するときの効果性や効率性の度合い

また、使用性の副品質特性の一つに「習得性：指定された作業の操作方法を習得し、効率的に操作を開始するまでに要する時間」がある。

ア オンラインヘルプを充実させることは使用性を向上させる施策となる。

イ 機能適合性を向上させる施策となる。

ウ 機能適合性を向上させる施策となる。

エ 信頼性を向上させる施策となる。

したがってアが正解。

●問 17 正解：エ

マッシュアップ（Mashup）とは、既存の複数のサービスやコンテンツなどを組み合わせることで、新たなサービスを創出することである。たとえば、API が公開された既存の Web サービスを組み合わせることで、複合的な機能をもった新たな Web サービスを短期

間で開発することなどが可能となる。したがってエが正解。

●問 18 正解：ウ

EVM (Earned Value Management) は、プロジェクトの進捗や作業のパフォーマンスを定量化（金額換算）し、プロジェクトの現状及び将来の状況を評価する進捗管理手法である。進捗を金額で表すため、コスト実績を把握しやすいなどの利点がある。

EVM における基本指標として、次の値がある。

- ・ EV (Earned Value : 出来高) … 現時点で完了した作業の工数
- ・ PV (Planned Value : 計画値) … 現時点までの計画工数
- ・ AC (Actual Cost : 実績値) … 現時点で実際にかかった工数
- ・ BAC (Budget At Completion : 計画総工数) … プロジェクト完了までの計画上の総工数

基本指標を次のように組み合わせることで、プロジェクトの現状及び将来の状況を評価する。

- ・ $EV - PV = SV$ (Schedule Variance : スケジュール差異)
- ・ $EV - AC = CV$ (Cost Variance : コスト差異)
- ・ $EV / PV = SPI$ (Schedule Performance Index : スケジュール効率指標)
- ・ $EV / CV = CPI$ (Cost Performance Index : コスト効率指標)
- ・ $AC + (BAC - EV) / CPI = EAC$ (Estimate At Completion : 完了時コスト予測)
- ・ $EAC - AC = ETC$ (Estimate To Completion : 残作業コスト予測)
- ・ $BAC - EAC = VAC$ (Variance At Completion : 完了時コスト差異)

CV の値が正の場合は予算に対して実コストが少ないので問題はない。SV の値が負の場合は作業の進捗に遅れが出ているので、遅れを改善するための対策が必要である。したがってウが正解。

●問 19 正解：イ

クラッシングは、メンバの増員や時間外勤務の増加など、コストを追加投入することにより、プロジェクト全体のスケジュールを短縮する技法である。クラッシングを行う際には、各作業工程の中で最も日数を要する経路（クリティカルパス）上のスケジュールアクティビティに対して優先的にコストを追加投入すべきである。したがってイが正解。

●問 20 正解：エ

フルバックアップを取得する時間間隔を 2 倍にしてもフルバックアップで取得するデータの量は変わらないため、1 回当たりの磁気テープ使用量や平均実行時間は変わらない。一方、フルバックアップを取得する時間間隔を 2 倍にすると、その間に行われたデータの追加・変更・削除などのログ情報は約 2 倍になるため、当該ログ情報によって復旧するときの処理時間も平均して約 2 倍になる。したがってエが正解。

●問 21 正解：エ

システム監査基準の「V.報告基準 4. 監査報告についての責任」に、「システム監査人は、監査報告書の記載事項について、その責任を負わなければならない」とあるように、システム監査人は監査報告書に記載した監査意見などについて責任を負う。したがってエが正解。

●問 22 正解：ア

- ア 売掛金回収条件を営業部門が行っている場合、取引先の財務状況などが適切に評価されず、営業部門の都合で勝手な条件が設定されてしまう可能性がある。その結果、取引先の倒産などによって売掛金が回収できなくなる可能性もある。したがって、内部統制上は営業部門からは独立した存在である審査部門が設定するのが適切である。
- イ 売掛金の消込み入力と承認処理は、営業部門ではなく経理部門が実施する必要がある。
- ウ 顧客ごとの与信限度の決定は、取引先の財務状況などを審査する審査部門が行う必要がある。
- エ 不当な値引き処理などを防ぐため、値引き又は割戻し処理は営業部門の担当者ではなく、経理事務の担当者が実施すべきである。

したがってアが正解。

●問 23 正解：ウ

問 8 で解説した通り、UML (Unified Modeling Language) とは、オブジェクト指向型のソフトウェア開発における分析・設計段階で、システムをモデル化する際の表記方法を統一したものである。

UML では目的に応じて次のようなモデル図が用いられる。

- ・オブジェクト図：オブジェクト間の関係を表す。
- ・クラス図：クラス間の関係を表す。

- ・コンポーネント図：コンポーネント間の構造や依存関係を表す。
- ・シーケンス図：オブジェクト間のメッセージ送受信による相互作用を時系列的に表す。
- ・状態チャート図：オブジェクトの状態遷移を表す。
- ・ユースケース図：ユーザなどシステムの外のオブジェクトから見たときのシステムの機能を表す。

したがってウが正解。

●問 24 正解：エ

ROI (Return on Investment：投下資本利益率) は、企業全体や特定の事業部、個別のプロジェクトなどにおいて、投下した資本がどれだけの利益を生んでいるか(投資対効果)を評価するための指標である。投資額を分母に、投資による収益を分子とした比率を算出する。したがってエが正解。

●問 25 正解：ウ

BABOK (Business Analysis Body of Knowledge：ビジネスアナリシス知識体系) は、ビジネスアナリシスにおけるベストプラクティスを体系化した文書である。ビジネスアナリシスの計画とモニタリング、引き出し、要求アナリシス、基礎コンピテンシ、エンタープライズアナリシス、要求管理とコミュニケーション、ソリューションの評価と妥当性確認、の七つの知識エリアからなる。したがってウが正解。

●問 26 正解：イ

ダイバーシティ (Diversity) は「多様性」を意味する。ダイバーシティマネジメントとは、性別や年齢、国籍などの違いから生じる多様な価値観を尊重することにより、組織の活力を向上させようとする取組みのことである。したがってイが正解。

●問 27 正解：イ

バリューチェーン (Value Chain) は、製品が顧客に届くまでの「モノの流れ」に着目して企業活動を分類し、それらのどの部分で付加価値が生み出されているかを分析する手法である。企業の活動を、購買物流、製造、出荷物流、販売・マーケティング、サービスという五つの主活動と、人事・労務管理、技術開発などの四つの支援分野に分類する。したがってイが正解。

●問 28 正解：イ

技術の S カーブとは、技術の進歩の過程を表すものである。横軸を時間、縦軸を成長の度合いとしたとき、当初は穏やかに成長するが、その後急激に成長し、成熟期を迎えると成長は鈍化する様子が S の字を描くことからこのように呼ばれる。したがってイが正解。

●問 29 正解：ウ

- ア 事業部制組織の説明である。
- イ マトリックス組織の説明である。
- ウ 職能部門別組織の説明である。
- エ プロジェクト組織の説明である。

したがってウが正解。

●問 30 正解：ウ

労働者派遣とは、派遣元事業主が自己の雇用する労働者を、当該雇用関係の下にかつ他人（派遣先事業主）の指揮命令を受けて当該他人のために労働に従事させることをいう。労働者派遣法に基づいた労働者の派遣において、派遣元事業主と派遣先事業主、派遣労働者との間は次のような関係になる。

- ・派遣元事業主と派遣先事業主：労働者派遣契約関係
- ・派遣元事業主と派遣労働者：雇用関係
- ・派遣先事業主と派遣労働者：指揮命令関係

したがってウが正解。