

## 平成 30 年度 秋期 情報処理安全確保支援士

## &lt;午前 I 解答・解説&gt;

## ●問 1 正解：ア

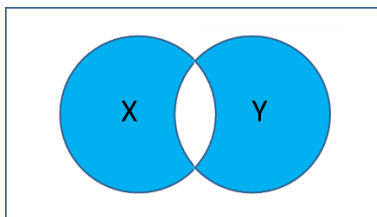
排他的論理和 (XOR) は、次のように、複数の入力値のうち、真 (1) の数が奇数の場合には真、偶数の場合には偽 (0) となる。

これを真理値表とベン図で表すと次のようになる。

## ■真理値表

入力値 X :	0	1	0	1
入力値 Y :	0	0	1	1
XOR :	0	1	1	0

## ■ベン図



XOR の相補演算では XOR と真偽が逆転するため、これは否定論理和と論理積の和である **ア** の等価演算となる。

## ●問 2 正解：イ

M/M/1 の待ち行列における窓口の平均待ち時間は、平均サービス時間（1 件の伝票データの処理時間）、窓口の利用率（ $\rho$ ）により、次の公式で表される。

$$\text{平均待ち時間} = \frac{\rho}{(1 - \rho)} \times \text{平均サービス時間}$$

「1 件の伝票データの処理時間は、平均 T 秒の指数分布に従う」とあることから、平均サービス時間は T となり、これが平均待ち時間 T 秒以上となる利用率は次の式で求められる。

$$\frac{\rho \times T}{(1 - \rho)} \geq T$$

$$\frac{\rho}{(1 - \rho)} \geq 1$$

$$\rho \geq 1 - \rho$$

$$2\rho \geq 1$$

$$\rho \geq 0.5$$

したがってイが正解。

### ●問3 正解：イ

正規分布とは、平均値を中心として、左右対称の山のような形となる確率分布である。  
標準偏差とは、データの分布のばらつきの大きさを表わす指標であり、母集団の標準偏差は  $\sigma$  で表される。

統計学において、正規分布における標準偏差には次の関係が成り立つことがわかっている。

- ・ 平均値  $-1 \times \sigma$  ～ 平均値  $+1 \times \sigma$  の範囲に、全体の約 68% のデータが含まれる。
- ・ 平均値  $-2 \times \sigma$  ～ 平均値  $+2 \times \sigma$  の範囲に、全体の約 95% のデータが含まれる。
- ・ 平均値  $-3 \times \sigma$  ～ 平均値  $+3 \times \sigma$  の範囲に、全体の約 99% のデータが含まれる。

これに従って各教科の分布を見ると、次のようになる。

- A：9 点～81 点の範囲に全体の約 95% が含まれる。残り約 5% に 0～8 点、82～100 点が含まれる。
- B：30 点～90 点の範囲に全体の約 95% が含まれる。残り約 5% に 0～29 点、91～100 点が含まれる。
- C：54 点～86 点の範囲に全体の約 95% が含まれる。残り約 5% に 0～53 点、87～100 点が含まれる。
- D：60 点～90 点の範囲に全体の約 99% が含まれる。残り約 1% に 0～59 点、91～100 点が含まれる。

この結果から、90 点以上の得点者が最も多かったと推定できる教科は B であることがわかる。したがって**イ**が正解。

**●問 4 正解：イ**

問題文の条件が成り立つのは、 $i$  が 1～99 のときであり、各要素の数は  $1+2+3+\dots$ （省略） $\dots+97+98+99$  となる。連続した 1 から  $n$  までの整数の和は次の式で求められる。

$$\frac{n(n+1)}{2} = \frac{99 \times 100}{2} = 4,950$$

したがって**イ**が正解。

**●問 5 正解：エ**

問題文に該当するのはハミング符号である。ハミング符号は、4 ビットの情報ビットに 3 ビットのパリティビットを付加することで、2 ビットの誤り検出と 1 ビットの誤り訂正ができるようにした方式である。メモリでは連続性のないランダムな誤りが発生する可能性が高いことからハミング符号が採用されている。ア～ウの各方式は誤りを検出することは可能だが、訂正する機能はない。したがって**エ**が正解。

**●問 6 正解：エ**

ページフォルトを伴わないページインだけの処理の割合を  $x$  とすれば、ページアウトを伴う処理の割合は  $(1 - x)$  となる。前者の処理時間が 20 ミリ秒、後者の処理時間が 60 ミリ秒、両者の平均処理時間が 30 ミリ秒となることから、次の式で表すことができる。

$$20x + 60(1 - x) = 30$$

この式を解いて  $x$  の値を求めればよい。

$$20x + 60 - 60x = 30$$

$$40x = 30$$

$$x = \frac{30}{40} = 0.75$$

したがって**エ**が正解。

---

**●問 7 正解：ア**

A, B は次の 4 つの組合せとなる。

A=0, B=0

A=1, B=0

A=0, B=1

A=1, B=1

このとき、問題文に該当する X, Y の値は次のようになる。

A=0, B=0 のとき : X=0, Y=0

A=1, B=0 のとき : X=0, Y=1

A=0, B=1 のとき : X=0, Y=1

A=1, B=1 のとき : X=1, Y=0

X は論理積 (AND) の出力結果、Y は排他的論理和 (XOR) の出力結果であるため、図で表すと**ア**の回路となる。

---

**●問 8 正解：イ**

レンダリングとは、仮想世界のデータの集まりをコンピュータプログラムで処理して、ディスプレイに描画可能な形式の画像に変換する技術である。したがって**イ**が正解。

---

**●問 9 正解：ウ**

解答群の各数値を除数として剰余を求める。

ア

$$571 \div 193 = 2 \text{ 余り } 185$$

$$1168 \div 193 = 6 \text{ 余り } 10$$

$$1566 \div 193 = 8 \text{ 余り } 22$$

イ

$$571 \div 197 = 2 \text{ 余り } 177$$

$$1168 \div 197 = 5 \text{ 余り } 183$$

$$1566 \div 197 = 7 \text{ 余り } 187$$

ウ

$$571 \div 199 = 2 \text{ 余り } 173$$

$$1168 \div 199 = 5 \text{ 余り } 173$$

$$1566 \div 199 = 7 \text{ 余り } 173$$

エ

$$571 \div 211 = 2 \text{ 余り } 149$$

$$1168 \div 211 = 5 \text{ 余り } 113$$

$$1566 \div 211 = 7 \text{ 余り } 89$$

剰余が全て一致することから、使用した除数は 199 である。したがって**ウ**が正解。

**●問 10 正解：エ**

先行プログラム、後続プログラムのいずれかが「排他」の場合、二つのプログラムを並行して実行することはできない。解答群の中で、二つのプログラムが並行して実行されるのは、先行プログラム、後続プログラムがいずれも「共用」の場合のみである。したがって**エ**が正解。

**●問 11 正解：イ**

スイッチングハブと同様に、OSI 参照モデルの第 2 層であるデータリンク層のレベルで動作し、同様の機能をもつ装置としてブリッジがある。したがって**イ**が正解。

**●問 12 正解：エ**

利用者の PC は DMZ 上の公開 Web サーバとの間で TLS 通信を行うため、当該通信データを暗号化することができる。また利用者個人のデジタル証明書により、利用者を認証することができるようになる。したがって**エ**が正解。

**●問 13 正解：ウ**

クロスサイトスクリプティング (Cross-Site Scripting : XSS) とは、ユーザ情報登録や問合せ受付の入力確認画面など、ユーザが入力したデータを元に、Web アプリケーションが動的に HTML を作成するページにおいて、入力データのチェックの不備を突いてクライアント環境で不正なスクリプトを実行させる攻撃手法である。XSS への対策としては、入力データを処理する Web アプリケーションにおいて、出力データが HTML タグとして解釈されないように処理 (エスケープ処理) するのが有効である。したがって**ウ**が正解。

**●問 14 正解：ウ**

ブルートフォース攻撃とは、鍵や文字列として考えられるすべてのパターンを用いて暗号解読やパスワード破りを試みる攻撃手法である。総当たり攻撃とも呼ばれる。したがって**ウ**が正解。

- ア セッションハイジャックの説明である。
- イ キーロガーの説明である。
- エ リプレイ攻撃の説明である。

**●問 15 正解：イ**

ファジングとは、ソフトウェア製品の脆弱性を検出することを目的としたブラックボックス検査手法の一つである。

ファジングでは、検査対象となるソフトウェア製品に対し、極端に長い文字列や通常使わない制御コードなど、問題を引き起こしそうなデータ（ファズ：fuzz）を大量に送り込み、その応答や挙動を監視することで、脆弱性を見つけ出す。したがって**イ**が正解。

**●問 16 正解：ア**

問題文に該当するのはフルブルーフであり、**ア**が正解。

フルブルーフとは、不特定多数のユーザが操作しても誤動作などが起こりにくいように設計することである。

- イ フェールセーフとは、システムに障害が発生した場合に、安全な方向に向かうように制御することである。
- ウ フェールソフトとは、システムに障害が発生した場合に、機能を縮退させて運用を継続することである。
- エ フォールトトレランスとは、機器を多重化することにより、高信頼性、高可用性を確保することである。

**●問 17 正解：ア**

イテレーション（Iteration）とは、繰り返し、反復を意味する言葉であり、アジャイル開発においては、要求分析、設計、開発、テスト等の一連の工程（繰り返す単位）である。

アジャイル開発では、イテレーションを繰り返すことで、ソフトウェアに存在する顧客の要求との不一致を解消したり、要求の変化に柔軟に対応したりすることが可能となる。したがって**ア**が正解。

- イ タスクボードの目的である。
- ウ ピンポンペアプログラミング、ペアプログラミングピンポン、などと呼ばれる方式

である。

エ 日次スクラムの目的である。

●問 18 正解：ウ

トレンドチャートは、作業の進捗状況と予算の消費状況を関連付けて 2 本の折れ線グラフで示したものであり、両者の差異や傾向を分析することができる。したがって**ウ**が正解。

●問 19 正解：イ

ファンクションポイント法は、アプリケーションの機能の数がソフトウェア開発の規模に相関するという考え方に基づいており、入出力データ数やファイル数などによって機能を定量的に測定するとともに、複雑さや特性による調整を行うことにより開発規模を見積もる手法である。調整前 FP を求めるために必要なのは機能量の情報であるため、該当するのは画面数である。したがって**イ**が正解。

●問 20 正解：イ

a は、IT サービス及び IT サービスマネジメントに対する全体的な戦略を確立することであるから、「サービスストラテジ」が該当する。

b は、IT サービスと、それを支えるプラクティス管理ツールを作り出すことであるから、「サービスデザイン」が該当する。

c は、IT サービス及びサービス変更についてテストし、本番環境に展開することであるから、「サービストランジション」が該当する。なお、トランジション (transition) は「移行」「変化」「過渡期」といった意味である。

d は、IT サービスを提供し、サポートすることであるから、「サービスオペレーション」が該当する。

したがって**イ**が正解。

●問 21 正解：ア

ア 正しい記述である。

イ サンプルングリスクとは、抽出されたサンプルが母集団の特性を正確に反映しないために、監査人が誤った結論を形成するリスクである。

ウ 統計的サンプルングとは、母集団から無作為にサンプルを抽出し、そのサンプルを分析して母集団の特性を推測する方法である。

エ 母集団とは、サンプルを抽出し、その特性等を導き出そうとしている集合全体である。

●問 22 正解：ア

可監査性とは、監査がどの程度可能であることを示すものである。情報システムの可監査性とは、コントロールや監査証跡によって、当該システムの安全性や処理の正当性を効果的に監査できるように設計・運用されていることの度合いである。したがって**ア**が正解。

●問 23 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。
ステートチャート図：	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（アクター）とシステムの相互作用を表す。

したがって**ウ**が正解。

●問 24 正解：エ

バランススコアカードとは、設定した戦略を遂行するために、財務、顧客、内部ビジネスプロセス、学習と成長、の 4 つの視点に基づいて、相互の適切な関係を考慮しながら業績評価の指標を設定し、経営戦略との適合性を評価することによって IT 投資の効果を多面的に把握する経営管理手法である。

- ア 財務の視点である。
- イ 顧客の視点である。
- ウ 学習と成長の視点である。
- エ 内部ビジネスプロセスの視点である。

したがって**エ**が正解。



●問 25 正解：ア

システム化構想の立案プロセスにおいては、経営上のニーズ、課題等を確認するとともに、情報技術動向を調査し、企業目標を達成するため、競争優位または事業機会を生み出す情報技術の利用方法等について分析する。したがって**ア**が正解。

●問 26 正解：ア

問題文に該当するのはクラスタ分析法である。クラスタ分析法は、観測データを類似性によっていくつかの集団や群（クラスタ）に分類し、そのクラスタの特徴となる要因を分析する。したがって**ア**が正解。

- イ 指数平滑法は、時系列データに対してウェイトを付け、平滑化することで将来値を予測する方式である。新しいデータに大きなウェイトを置き、過去のデータになるほどウェイトを小さくする。
- ウ デルファイ法は、複数人がそれぞれ独自に意見を出し合い、その結果をフィードバックした後で再び意見を出し合う、という作業を繰り返すことで意見を収束させていく手法である。
- エ モンテカルロ法は、乱数によるシミュレーションを何度も繰り返すことにより、問題の近似値を求める計算手法である。

●問 27 正解：ウ

- ア インターネットを経由して機器の電源のオン・オフなどの操作命令を送信するのであるから、“制御”の段階である。
- イ 機械の温度や振動データをインターネットを経由してサーバに蓄積するのであるから、“監視”の段階である。
- ウ 機械同士が互いの状態を常時監視・分析し、人手を介すことなく目標に合わせた協調動作を自動で行うのであるから、“自律化”の段階である。
- エ 機械の稼働情報を基に、機械の故障検知時に保守員が故障部位を分析して特定するのであるから、“最適化”の段階である。

したがって**ウ**が正解。

**●問 28 正解：イ**

製品 A を 1 個製造するのに、部品 D はユニット B で 12 個、ユニット C で 1 個必要であるため、製品 A を 10 個製造するには合計 130 個必要である。しかし、ユニット B の在庫残 5 個（部品 D の在庫残 15 個）と、部品 D 単体の在庫残が 25 個あるため、正味所要量は  $130 - 40 = 90$  となる。したがって**イ**が正解。

**●問 29 正解：ウ**

売上高、変動費、損益、変動費率は次の式で表すことができる。

$$\text{売上高} - (\text{固定費} + \text{変動費}) = \text{損益}$$

$$\text{変動費} = \text{売上高} \times \text{変動費率}$$

問題文の 2 つの条件を式で表すと次のようになる。

$$7,000 - \text{固定費} + 7,000 \times \text{変動費率} = -200$$

$$9,000 - \text{固定費} + 9,000 \times \text{変動費率} = 600$$

2 つ目の式から 1 つ目の式を引くことで、変動費率が求められる。

$$2,000 - 2,000 \times \text{変動費率} = 800$$

$$2,000 \times \text{変動費率} = 1,200$$

$$\text{変動費率} = 0.6$$

これにより、売上高が 8,000 万円のと時の変動費は 4,800 万円となる。したがって**ウ**が正解。

**●問 30 正解：イ**

下請代金支払遅延等防止法は、下請事業者の利益を保護し、取引の適正化を推進することを目的としている。同法では、第 3 条において、「親事業者は、下請事業者に対し製造委託等をした場合は、直ちに、公正取引委員会規則で定めるところにより下請事業者の給付の内容、下請代金の額、支払期日及び支払方法その他の事項を記載した書面を下請事業者に交付しなければならない。」としている。

解答群の中で、同法で禁止されている行為に該当するのは**イ**である。