平成 29 年度 春期 情報処理安全確保支援士

＜午前 I 解答・解説＞

●問 1　正解：ア

$(1+\alpha)^n$ の式に，いくつかの値を入れて展開してみると次のようになる。

n=2 のとき
$1 + 2\alpha + \alpha^2$
n=3 のとき
$1 + 3\alpha + 3\alpha^2 + \alpha^3$
n=4 のとき
$1 + 4\alpha + 6\alpha^2 + 4\alpha^3 + \alpha^4$

ここで，α が 1 に比べて非常に小さい値（例：0.01）とすれば，α のべき乗は次のようになり，ゼロに近い値となる。

$\alpha^2 = 0.0001$
$\alpha^3 = 0.000001$
$\alpha^4 = 0.00000001$

つまり，|α|が 1 に比べて非常に小さい場合には，$(1+\alpha)^n$ は，$1+n\times\alpha$ で近似値計算ができることになる。したがってアが正解。

●問 2　正解：エ

BNF（Backus-Naur Form：バッカス・ナウア記法）は，ジョン・バッカスとピーター・ナウアによって考案された構文規則の記法であり，プログラミング言語の ALGOL60 で用いられている。BNF では，" ::= " は左辺と右辺の区切り，" | " は " or "の意味であり，文字の繰り返しは再帰的定義によって表す。

ア，イ　2 つ目の" ＜digit＞ "により，先頭が数字で始まってもよいことになってしまう。
ウ　" ＜identifier＞＜letter＞ "の定義がないため，2 文字目以降は数字であることが必須となってしまう。
エ　正しい記述である。

●問３　正解：イ

問題文の関数は**ユークリッドの互助法**によって a, b の最大公約数（Greatest Common Divisor:gcd）を求めるものである。たとえば，a＝128, b＝40 として処理を実行すると次のようになる。

x ← 128
y ← 40

1 回目のループ
t ← mod(128, 40) ＝ 8
x ← 40
y ← 8

2 回目のループ
t ← mod(40, 8) ＝ 0
x ← 8
y ← 0

ループ終了
x ＝ 8

8 は a と b の最大公約数であり，他の選択肢には該当しない。したがって**イ**が正解。

●問４　正解：ア

15M バイトのプログラムを 40%に圧縮すると，15 × 0.4 ＝ 6M バイトである。

これを 20M バイト／秒で転送すると，6 ／ 20 ＝ 0.3 秒を要する。
主記憶上で 6M バイトを展開するには，0.03 × 6 ＝ 0.18 秒を要する。

合計すると，0.48 秒となる。したがって**ア**が正解。

●問５　正解：エ

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。

稼働率 ＝ MTBF ／ (MTBF ＋ MTTR)

稼働率 α の装置が n 台直列している場合の稼働率は，α^n，n 台並列している場合の稼働率は，$1 - (1 - \alpha)^n$ となる。

装置 A, B は，MTBF＝450，MTTR＝50 なので，その稼働率 α は次のようになる。

$\alpha = 450/(450+50) = 450/500 = 0.9$

続いて，稼働率 0.9 の装置 2 台並列している場合の稼働率を求めると，次のようになる。

$1 - (1 - 0.9)^2 = 1 - 0.1^2 = 1 - 0.01 = 0.99$

したがって**エ**が正解。

●問 6　正解：エ

ア　FIFO（First In First Out）は，最初にロードされたものが置換え対象となるため，ロード時刻が 0:00 の" C0 "が対象となる。

イ　LFU（Least Frequently Used）は，最も使用されていないものが対象となるため，参照回数が 1 回の" C1 "が対象となる。

ウ　LIFO（Last In First Out）は，最後にロードされたものが置換え対象となるため，ロード時刻が 0:05 の" C3 "が対象となる。

エ　LRU（Least Frequently Used）は，最後に参照されてからの経過時間が最長のものが置換え対象となるため，最終参照時刻が 0:05 の" C2 "が対象となる。

したがって**エ**が正解。

●問 7　正解：イ

図を論理式で表すと次のようになる。

$F = (\overline{A} \cdot B) + (A \cdot B)$

これを論理演算すると次のようになる。

$F = B \cdot (\overline{A} + A)$

$F = B \cdot 1$

F ＝ B

したがって**イ**が正解。

●問８　正解：エ

デッドロックとは，たとえば，テーブル a にロックをかけてからテーブル b にロックをかけようとしているトランザクションと，その逆にテーブル b にロックをかけてからテーブル a にロックをかけようとしているトランザクションが同時に実行された場合に，互いに必要なデータをロックしあっているため，待ち状態になってしまうことをいう。

表では，③でトランザクション A がテーブル a にロックをかけ，④でトランザクション B がテーブル b にロックをかけた後，⑤でトランザクション A がテーブル b のアンロック待ち，⑥でトランザクション B がテーブル a のアンロック待ち，すなわちデッドロックとなっている。したがって**エ**が正解。

●問９　正解：ア

データマイニングとは，データベース等に蓄積された大量のデータに対して様々な統計処理を施すことによって，その関連性や規則性を見つけることをいう。したがって**ア**が正解。

●問 10　正解：ア

CSMA/CD（Carrier Sense Multiple Access with Collision Detection）**方式**とは，イーサネットに代表されるバス型ネットワーク（各ノードが 1 本のケーブルに接続されるネットワーク形態）において用いられているアクセス制御方式である。

この方式では，通信を行う際に，まずそれぞれのステーションがキャリア（通信路）の信号を検出し，空いていれば通信を開始する。通信データの衝突を検出した場合は，ランダムな時間を待ってから再送する。したがって**ア**が正解。

イ　TDMA（Time Division Multiple Access）の説明である。
ウ　無線 LAN で用いられる CSMA/CA（Carrier Sense Multiple Access/Collision Avoidance）の説明である。
エ　トークンパッシングの説明である。

●問 11　正解：イ

OpenFlow は，制御機能と転送機能が共存する従来のネットワーク機器と異なり，制御機能を「OpenFlow コントローラ」，転送機能を「OpenFlow スイッチ」として分離したアーキテクチャである。

SDN とは，ソフトウェアによって柔軟かつ動的にネットワークを構成，制御する技術であり，それを実現するための技術の一つが OpenFlow である。したがって**イ**が正解。

●問 12　正解：ウ

Web サーバのサーバ証明書には，その証明書を発行した認証局のディジタル署名が付されている。Web サーバへの TLS を用いたアクセスにおいて，サーバ証明書を入手した PC は，あらかじめブラウザに格納されている認証局の公開鍵を用いて当該ディジタル証明書を検証することで，サーバ証明書の正当性を確認する。したがって**ウ**が正解。

●問 13　正解：ア

共通鍵暗号方式では，n 人の送受信者がそれぞれ秘密に暗号を使って通信を行うときに必要な鍵の数は次の式で求められる。

$$ {}_{n}C_{2} = \frac{n(n-1)}{2} $$

したがって，仮に 100 人が共通鍵暗号方式を用いて通信を暗号化する場合には，100×99 / 2 ＝ 4,950 個の鍵が必要となる。

一方，**公開鍵暗号方式**では，送受信者がそれぞれ秘密鍵と公開鍵の二つの鍵を持てばよいため，必要な鍵の数は，2n 個（100 人の場合には 200 個）となる。

ア　正しい記述である。
イ　共通鍵暗号方式では，送信者と受信者が共通の鍵を用いる。
ウ　公開鍵暗号方式で暗号化通信を行う場合は，暗号化に用いる鍵を公開する。
エ　署名に用いる鍵（秘密鍵）は決して公開せず，厳重に管理する必要がある。

したがって**ア**が正解。

●問 14　正解：ア

サイバーセキュリティ経営ガイドラインは，IT に関するシステムやサービス等を供給する企業及び経営戦略上 IT の利活用が不可欠である企業の経営者を対象に，経営者のリーダ

ーシップの下で，サイバーセキュリティ対策を推進するため，経産省と IPA が策定したガイドラインである。（2016 年 12 月 8 日に Ver1.1 を公表）

サイバー攻撃から企業を守る観点で，経営者が認識する必要のある「3 原則」，及び経営者が情報セキュリティ対策を実施する上での責任者となる担当幹部（CISO 等）に指示すべき「重要 10 項目」をまとめている。したがって**ア**が正解。

イ　情報セキュリティポリシの説明である。
ウ　**COBIT**（Control Objectives for Information and related Technology）の説明である。
エ　サイバーセキュリティ基本法の説明である。

●問 15　正解：イ

WPA2-PSK（Wi-Fi Protected Access 2 Pre-Shared Key）は，一般家庭や小規模なオフィスなどで無線 LAN を使用する場合に用いられる方式である。同方式では，アクセスポイントと端末で，事前に SSID とパスワード（8～63 文字）を共有しておき，それらが正しく設定された端末だけを接続させる。したがって**イ**が正解。

ア　SSID は通信の暗号化には用いられない。
ウ　事前に設定したパスワードによって端末を認証する。
エ　SSID は利用者ごとに付与されることはなく，アクセスポイントごとに設定する。

●問 16　正解：ア

汎化（generalization）とは，オブジェクト指向において，子クラスに共通する性質を持つ親クラスを定義すること，またはその関係のことをいい，" is-a "（汎化－特化）関係とも呼ばれる。**特化**（specialization）は，汎化とは逆に，親クラスの性質を継承して具体化することである。

一方，「アクセル」「ブレーキ」「ハンドル」が「自動車」の一部であるように，「○○は，○○の一部である」ということを表す，" part-of "（集約－分解）関係がある。

ア　「哺乳類」は，「人」「犬」「猫」に共通する性質であるため，適切である。
イ　" part-of "（集約－分解）関係である。
ウ　「受注」「在庫」「出荷」は「商品」に対する処理や手続きである。
エ　「会社名」「住所」「電話番号」は「取引先」の属性である。

したがって**ア**が正解。

●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

アローダイアグラムは，関連性のある複数の作業からなるプロジェクト等において工程管理を行うために用いられる。関連性のある作業とは，「ある作業が終了しないと次の作業が始められない」という関係のことを意味する。アローダイアグラムでは，この関係を矢印（アロー）で表しており，各矢印が一つの作業単位を，各矢印上の数字が作業日数を表す。また，ダミー作業の矢印がある場合には，ダミー作業が完了するまではその次の作業を開始することはできない。

図から各作業経路の必要日数を求めると次のようになる。

A→C→G→H ＝ 10＋20＋20＋10 ＝ 60 日
A→D→H　＝ 10＋30＋10　＝ 50 日
A→E→H　＝ 10＋30＋10　＝ 50 日
B→F→H　＝ 10＋10＋10　＝ 30 日

このことから，クリティカルパス（最も日数を要する経路）は，A→C→G→H であることがわかる。

ア　作業 C を開始するには，作業 A と作業 B が完了している必要があるため，最も早く開始できるのは 10 日目である。
イ　作業 D はクリティカルパス上の作業ではない。
ウ　C→G で 40 日必要であるため，作業 E の余裕日数は 30 日である。
エ　A→C→G で 50 日必要であり，それまでに B→F の作業が完了していればよい。作業 F に 10 日間を要するため，最も遅く開始できるのは 40 日目である。

したがってウが正解。

●問 19　正解：ア

PMBOK（Project Management Body of Knowledge）は，プロジェクトマネジメント団体である **PMI**（Project Management Institute）が発行しているプロジェクトマネジメントに関する知識体系である。

定量的リスク分析は，特定したリスクがプロジェクト目標全体に与える影響を数量的に分析するプロセスである。したがってアが正解。

イ　定性的リスク分析で実施することである。
ウ　リスク対応計画で実施することである。
エ　リスク特定で実施することである。

●問 20　正解：ア

KPI（Key Performance Indicators：重要業績評価指標）とは，目標を達成するために設定した重要な業績評価の指標である。可用性管理プロセスでは，IT サービスの提供に必要な IT インフラや要員等の可用性を適切に維持管理することが主な活動となる。IT サービスの可用性と信頼性を適切に維持するには，サービスの中断回数とそのインパクトをいかに少なくするかが重要であるため，KPI となる。したがってアが正解。

イ　IT サービス継続性管理の KPI となる。
ウ　キャパシティ管理の KPI となる。
エ　サービスレベル管理の KPI となる。

●問 21　正解：ア

IT サービスマネジメントの問題管理プロセスは，インシデントをはじめ，IT サービスにおける問題の根本原因を追究して解決するとともに，再発防止策を策定することを目的としている。インシデントにつながる可能性のある事象や予兆について管理し，問題の発生を未然に防ぐことも重要な役割である。したがってアが正解。

●問 22　正解：エ

ア　システム監査人は，改善の実現可能性を考慮する必要がある。
イ　改善勧告の内容は監査証拠に裏付けられたものでなければならない。
ウ　被監査部門の承認を受ける必要はない。
エ　適切な記述である。

したがって**エ**が正解。

●問 23　正解：ア

プログラムマネジメントは，関連する複数のプロジェクトを可視化するとともに一元管理することで，それらの連携，統合，相互作用等を通じて価値を高め，組織全体の戦略の実現を図ることを目的とした活動である。したがって**ア**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

問題文に該当するのはアクティビティ図であり，**ア**が正解。**アクティビティ図**は，処理の流れや分岐を記述するのに用いられるフローチャートに似た図であり，並行処理や処理の同期なども表現することができる。

イ　クラス図は，クラス間の関係を表す図である。
ウ　状態遷移図は，システムの状態がどのように推移していくかを視覚的に表現した図である。
エ　ユースケース図は，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図である。

●問 26　正解：エ

浸透価格戦略とは，新製品のマーケットシェアの確保を目的として，発売初期の価格を低く設定するとともに，積極的なプロモーション活動などを行うことである。したがって**エ**が正解。

●問 27　正解：エ

問題文に該当するのは**デルファイ法**であり，**エ**が正解。デルファイ法は，社会情勢や技術動向等のテーマに関する未来予測を行う場合等に用いられる意見収束技法であり，対象となるテーマについて複数の専門家へのアンケートを実施し，その結果をフィードバックした後で再びアンケートを実施する，という作業を何度か繰り返すことによって意見を収束させていく。

●問 28　正解：エ

セル生産方式とは，作業員を取り囲んだセルと呼ばれる作業台を用いて，1 人または数名程度の作業員が，部品の組み立て，加工，検査等の全ての工程を担当する生産方式である。セル生産方式は，セル数の増減やセル内の作業員の人数調整等によって製品の種類や生産量の調整が行い易いため，多種類かつフレキシブルな生産が求められる場合に適している。したがって**エ**が正解。

●問 29　正解：ウ

損益分岐点（売上高）は次の式で求められる。

$$\text{損益分岐点} = \frac{\text{固定費}}{1 - \dfrac{\text{変動費}}{\text{売上高}}} = \frac{\text{固定費}}{1 - \text{変動費率}}$$

ア　変動費率が低くなると損益分岐点は低くなる。
イ　変動費率の変化と損益分岐点の変化は正比例しない。
ウ　正しい記述である。
エ　変動費率が変わらないとき，固定費が小さくなると損益分岐点は低くなる。

したがって**ウ**が正解。

●問 30　正解：エ

ア　個人の趣味のページであっても，Web というパブリックなスペースに他人の著作物を無断で掲載することは著作権の侵害にあたる。
イ　例えフリーウェアであってもプログラム自体は著作物であり，著作権法によって保護される。
ウ　シェアウェアを用いて作成したデータは，シェアウェアの開発者ではなく，データ作成者の著作物となる。したがってシェアウェアの試用期間とは無関係である。
エ　URL のリンク集であっても，作成者による分類がなされていたり，コメントが付加

されていたりするなど創作性がある場合には著作物として保護される。

したがって**エ**が正解。