

平成 27 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：エ

M/M/1 の待ち行列モデルにおける統合前の各支店の ATM の平均待ち時間は、平均サービス時間 (T_s)、ATM の利用率 (ρ) により、次の公式で表される。

$$\text{平均待ち時間} = \frac{\rho}{(1-\rho)} \times T_s$$

統合後は 1 台の ATM を 2 倍の利用者が利用することになるので、利用率 (ρ) が 2 倍となり、平均待ち時間は次の式で表すことができる。

$$\text{平均待ち時間} = \frac{2\rho}{(1-2\rho)} \times T_s$$

したがってエが正解。

●問 2 正解：イ

サンプル 3 個がすべて良品であればロット全体を合格とするのであるから、100 個中に 10 個の不良品を含む（すなわち 90 個の良品を含む）ロットが合格と判定されるのは、100 個から 3 個を抽出する組合せ数における、90 個から 3 個を抽出する組合せ数の割合となり、次の式で表すことができる。

$$\frac{\text{90 個から 3 個を抽出する組合せ数}}{\text{100 個から 3 個を抽出する組合せ数}} = \text{100 個中 10 個の不良品を含むロットが合格する確率}$$

100 個から 3 個を抽出する組合せ数は次の式で求められる。

$${}_{100}C_3 = \frac{(100 \times 99 \times 98)}{(3 \times 2 \times 1)}$$

同様に、90 個から 3 個を抽出する組合せ数は次の式で求められる。

$${}_{90}C_3 = \frac{(90 \times 89 \times 88)}{(3 \times 2 \times 1)}$$

これらから、100 個中 10 個の不良品を含むロットが合格する確率は、次のようになる。

$$\frac{90 \times 89 \times 88 \times 6}{100 \times 99 \times 98 \times 6} = \frac{9 \times 89 \times 8}{10 \times 9 \times 98} = \frac{89 \times 4}{5 \times 98} = \frac{89 \times 2}{5 \times 49} = \frac{178}{245}$$

したがってイが正解。

●問3 正解：イ

キーaをnで割ったときの商をx, 余り（ハッシュ値）をrとすると, 次の式で表すことができる。

$$r = a - nx$$

キーbをnで割ったときの商をy, 余りをr'とすると, 次の式で表すことができる。

$$r' = b - ny$$

キーaとbが衝突するのは, rとr'が等しい場合なので, 次の式が成り立つ。

$$a - nx = b - ny$$

$$a - b = nx - ny$$

$$a - b = n(x - y)$$

上記の式より, $a - b$ がnの倍数となっていることが分かる。したがってイが正解。

●問4 正解：ウ

スーパスカラは, 命令を実行するためのパイプラインを複数用意して並行動作させることにより, 同時に複数の命令を実行可能にし, 高速化を図る方式である。したがってウが正解。

ア ベクトル処理方式に関する説明である。

イ スーパパイプラインに関する説明である。

エ VLIW (Very Long Instruction Word) に関する説明である。

●問5 正解：ウ

スケールアウトとは, サーバの台数を増やすことによってサーバ群としての処理能力や信頼性, 可用性等を向上させようとするアプローチである。これに対し, サーバのCPUを高性能なものに交換したり, メモリ, ストレージ等のシステムリソースを増設したりすることによってサーバ単体としての処理能力や信頼性, 可用性等を向上させようとするアプローチをスケールアップという。したがってウが正解。ア, イ, エはいずれもスケールアップに関する記述である。

●問 6 正解：エ

ラウンドロビン方式とは、物事や処理をあるルールに従って順番に実行したり、資源を均等に割り当てたりする方式である。ラウンドロビン方式のプロセススケジューリングでは、各プロセスを待ち行列の順に一定の CPU 時間（タイムクォンタム）を割り当てて実行し、終了しないときは待ち行列の最後尾につなぐ。したがってエが正解。

●問 7 正解：ア

3 入力多数決回路なので、真理値表に示すように、入力値 A, B, C のうち、0 が二つ以上あれば出力値 Y は 0 に、1 が二つ以上あれば Y は 1 となる。

これを回路で表すと、まず A と B, B と C, A と C の論理積を求め、その結果いずれかに 1 があれば 1 が二つ以上あるということなので Y が 1、いずれも 0 の場合には 1 が一つ以下（0 が二つ以上）ということなので Y が 0 となるよう、最初の三つの論理積の出力結果の論理和を求めればよい。したがってアが正解。

●問 8 正解：ウ

拡張現実とは、現実世界の情報に対し、コンピュータによって処理された情報を付加することにより、人間が知覚する現実世界の情報を拡張する技術である。

仮想現実（VR : Virtual Reality）は、コンピュータによって人工的に作り出された現実感を人間に知覚させる技術だが、拡張現実とは現実の一部を改変する技術である。

衣料品を仮想的に試着したり、実際の画像上に過去の建築物を 3 次元 CG で再現したりするのは、現実世界の情報にコンピュータによって処理された情報を付加し、現実世界を拡張する例である。したがってウが正解。

●問 9 正解：ウ

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）の四つがあり、頭文字をとって ACID 特性と呼ばれる。ACID 特性の内容は次のとおり。

- ・原子性：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

したがってウが正解。

ア 一貫性の説明である。

- イ 耐久性の説明である。
- エ 独立性の説明である。

●問 10 正解：ア

CSMA/CD (Carrier Sense Multiple Access with Collision Detection) 方式とは, Ethernet 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, ネットワークの利用率が高くなればなるほどパケット同士の衝突が発生する頻度が高くなるため, スループットが低下する傾向にある。一般に利用率が 20~30% に達すると衝突が増加し, 再送が繰り返されることによってスループットが低下する。したがってアが正解。

●問 11 正解：イ

100 秒で受信するデータは, $64\text{k ビット} \times 100 \text{ 秒} = 64 \times 10^5 \text{ ビット}$ である。

この中で 1 ビットの誤りが発生するのであるから, ビット誤り率は次のように求められる。

$$\frac{1}{64 \times 10^5} = \frac{100}{64} \times 10^{-7} \div 1.56 \times 10^{-7}$$

したがってイが正解。

●問 12 正解：ア

同じパスワード文字列中に同じ文字を複数回使用することについて制限はないため, 設定できるパスワードの総数は, 単純に "文字の種類 (M) " の "文字数 (n) " 乗 (M^n) で求めることができる。したがってアが正解。

●問 13 正解：エ

残留リスクとは, リスクコントロールやリスクファイナンスを行っても対処しきれずに残るリスクのことである。したがってエが正解。

- ア 統制リスクの説明である。
- イ 固有リスクの説明である。
- ウ 投機的リスクの説明である。

●問 14 正解：ウ

NIST (National Institute of Standards and Technology : 米国国立標準技術研究所) では, クラウドコンピューティングのサービスモデルについて概ね次のように定義している。

・ **SaaS (Software as a Service)**

利用者に提供される機能はクラウドのインフラ上で稼動しているアプリケーションであり、利用者が OS などのインフラを管理したりコントロールしたり、アプリケーションの設定をしたりすることはできない。

・ **PaaS (Platform as a Service)**

利用者に提供される機能はクラウドのインフラ上に利用者が開発もしくは購入したアプリケーションを実装することである。利用者は OS などのインフラを管理したり、ミドルウェアの設定等を行ったりすることはないが、自分が実装したアプリケーションに対する各種設定、セキュリティ対策等を行う。

・ **IaaS (Infrastructure as a Service), HaaS (Hardware as a Service)**

利用者に提供される機能は CPU、ストレージ等のインフラである。利用者は OS やミドルウェア、ストレージ容量等を選択してサーバ環境を構築したり、OS やミドルウェアに対する各種設定等を行ったりする。

したがってウが正解。

●問 15 正解：エ

ディレクトリトラバーサル攻撃とは、ファイル名の入力に伴うアプリケーションに対して、ファイル名の先頭に“..”や“..¥”などを用いることにより、通常はアクセスできない上位のディレクトリにある非公開のファイルにアクセスする攻撃手法である。対策としては、入力されたファイル名をチェックし、不正な文字列を取り除くことであるが、意図的にエンコードされた文字列が使われることなども多く、注意が必要である。したがってエが正解。

●問 16 正解：ウ

JIS X 25010 : 2013（システム及びソフトウェア品質モデル）では、製品品質を八つの特性（機能適合性、信頼性、性能効率性、使用性、セキュリティ、互換性、保守性及び移植性）に分類しており、各特性は、関係する副特性の集合から構成される。

信頼性とは、「明示された時間帯で、明示された条件下に、システム、製品又は構成要素が明示された機能を実行する度合い」であり、その副特性を次のように定義している。

・ **成熟性**

通常の運用操作の下で、システム、製品又は構成要素が信頼性に対するニーズに合致している度合い。

・ **可用性**

使用することを要求されたとき、システム、製品又は構成要素が運用操作可能及びアクセ

可能な度合い。

・障害許容性（耐故障性）

ハードウェア又はソフトウェア障害にもかかわらず、システム、製品又は構成要素が意図したように運用操作できる度合い。

・回復性

中断時又は故障時に、製品又はシステムが直接的に影響を受けたデータを回復し、システムを希望する状態に復元することができる度合い。

ア 使用性の副特性である運用操作性の説明である。

イ 保守性の副特性である解析性の説明である。

ウ 信頼性の副特性である回復性の説明である。

エ 互換性の副特性である相互運用性の説明である。

したがってウが正解。

●問 17 正解：ウ

エクストリームプログラミング（XP：eXtreme Programming）とは、Kent Beck 氏らが考案・提唱しているソフトウェア開発手法であり、「アジャイルソフトウェア開発手法」と総称される、ソフトウェアを迅速かつ柔軟に開発する一連の手法を代表するものである。

XP では、開発チームが行うべきプラクティス（手法、慣行）が定められている。

ア XP では「40 時間労働」が提唱されている。

イ XP では「ソースコードの共同所有」が提唱されている。

ウ 正しい記述である。

エ XP では「ペアプログラミング」（常に二人一組でプログラミングを行うこと）が提唱されている。

したがってウが正解。

●問 18 正解：エ

PERT 図（Program Evaluation and Review Technique）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。

図の中で最も日数を要する経路を「クリティカルパス」と呼び、この経路上にある作業を短縮することで、プロジェクト全体の所要日数を短縮することができる。

問題文の PERT 図には次の四つの経路があり、クリティカルパスは「A → C → G → J」である。

$A \rightarrow B \rightarrow E \rightarrow I: 4 + 6 + 1 + 3 = 14$ (日)

$A \rightarrow C \rightarrow F \rightarrow I: 4 + 5 + 2 + 3 = 14$ (日)

$A \rightarrow C \rightarrow G \rightarrow J: 4 + 5 + 1 + 6 = 16$ (日)

$A \rightarrow D \rightarrow H \rightarrow J: 4 + 2 + 1 + 6 = 13$ (日)

作業 B, F, I はいずれもクリティカルパス上にないため、プロジェクト全体の所要日数を短縮することはできない。一方、作業 J はクリティカルパス上にあるため、1 日短縮することでプロジェクト全体の所要日数を 1 日短縮することができる。したがってエが正解。

●問 19 正解：ウ

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。

PMBOK では、リスク対応戦略を次のように分類している。

- ・回避：リスクの影響を避けること
- ・転嫁：リスクの影響を第三者に移転すること
- ・軽減：リスクの発生確率と影響度を受容できるレベルまで低減すること
- ・受容：リスクの影響を受け入れること

ア 受容に該当する。

イ 軽減に該当する。

ウ 転嫁に該当する。

エ 回避に該当する。

したがってウが正解。

●問 20 正解：ア

ITIL (Information Technology Infrastructure Library) とは、英国商務局 (Office of Government Commerce : OGC) が、IT サービスマネジメントにおける業務プロセスや手法を体系的に整理したものである。

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。IT サービスマネジメントの可用性と信頼性の管理では、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と信頼性を適切に維持・管理することが主な活動となる。そのためには、サービスの中断回数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 として用いる。

ウ キャパシティ管理の KPI として用いる。

エ サービスレベル管理の KPI として用いる。

●問 21 正解：イ

エディットバリデーションチェックとは、入力された値が正常な範囲に収まっているか、数値や文字などの種別や書式が正しいか、論理的に正しいか、といったことを確認し、問題がある場合には当該データをエラーとして処理する機能である。

これが正しく機能しているかどうかを検証するには、実際に例外データや異常データの入力を行い、それらがエラーとして適切に処理されているかを確認するとよい。したがってイが正解。

●問 22 正解：イ

日次バックアップデータが継続的に取得されているかどうかを検証するには、バックアップジョブの設定内容とジョブの実行結果ログを閲覧し、ジョブの設定内容と実行結果が適切であるかをチェックするのが有効である。したがってイが正解。

●問 23 正解：エ

問題文に該当するのは **ROI** (Return on Investment : 投下資本利益率) である。ROI は、企業全体や特定の事業部、個別のプロジェクト等において、投下した資本がどれだけの利益を生んでいるかを測るための指標であり、売上増やコスト削減などによって創出された利益額を分子に、投資額を分母にして算出する。したがってエが正解。

ア **EVA** (Economic Value Added) は、企業の経済的付加価値を表す指標であり、株主に対する収益還元に重点を置いている。

イ **IRR** (Internal Rate of Return) は、内部収益率を表す。

ウ **NPV** (Net Present Value) は、正味現在価値を表す。

●問 24 正解：ウ

エンタープライズアーキテクチャ (**EA**) とは、企業や政府機関など、大規模な組織 (enterprise) の機能や業務内容等を体系化して分析することで、IT ガバナンスを強化し、業務や情報システムの標準化や最適化を図るための活動や方法論を意味する。

EA の構成要素は、一般的に「ビジネスアーキテクチャ」「データアーキテクチャ」「アプリケーションアーキテクチャ」「テクノロジーアーキテクチャ」の四つとされている。したがってウが正解。

ア UML (Unified Modeling Language) の説明である。

イ E-R 図 (Entity-Relationship Diagram : 実体関係図) の説明である。

エ DFD (Data Flow Diagram) の説明である。

●問 25 正解：エ

IT 投資ポートフォリオとは、主に金融分野などで用いられるポートフォリオの考え方を情報化投資戦略に応用したものである。情報化投資をリスクや投資価値の類似性から幾つかのカテゴリに整理することで、ビジネス戦略実現のための最適な資源配分を管理する手法である。

なお、経済産業省発行の「業績評価参照モデル（PRM）を用いた IT ポートフォリオモデルの活用ガイド」では、プロジェクトを投資目的に応じて、戦略目標達成型、業務効率化型、インフラ構築型の三つのカテゴリに分類し、その上でカテゴリごとに用意した評価項目を用い、戦略適合性、実現性の二軸からプロジェクト間の相対評価を行う IT ポートフォリオモデルが示されている。したがってエが正解。

●問 26 正解：ウ

コモディティ化とは、技術の成熟などにより、メーカーや販売会社による製品の機能や品質などの差異がごくわずかとなり、均質化している状態をいう。したがってウが正解。

●問 27 正解：イ

イノベーション（innovation）は、革新、新機軸などの意味であり、プロセスイノベーションとは、製品の製造方法や物流、管理手法等の工程（プロセス）を刷新することにより、コストを大幅に削減したり、製品の品質を飛躍的に向上させたりすることをいう。一方、既存の製品とは明らかに異なる革新的、画期的な新製品を開発することをプロダクトイノベーションという。したがってイが正解。

●問 28 正解：エ

EDI（Electronic Data Interchange：電子データ交換）とは、B to B 取引の一種であり、特定企業間において、標準的なデータレコードフォーマットを用いて受発注等の取引業務を電子化する仕組みである。

EDI の国際標準として EDIFACT（Electronic Data Interchange For Administration, Commerce and Transportation）がある。日本では、1992 年に「財団法人 日本情報処理開発協会（JIPDEC※）」の産業情報化推進センター（CII）により、CII 標準が国内標準としてリリースされた。同標準において、EDI の規約は次の四つのレベルからなっている。

- ・レベル 1（情報伝達規約）：回線の種類や伝送手順等に関する事項
- ・レベル 2（情報表現規約）：標準的なメッセージの形式等に関する事項
- ・レベル 3（業務運用規約）：業務やシステムの運用に関する事項
- ・レベル 4（取引基本規約）：取引の法的有効性を確立するための事項

したがってエが正解。

※現在は「一般財団法人 日本情報経済社会推進協会」に改称されている。

●問 29 正解：ア

OC 曲線 (Operating Characteristic curve) は、ロットの不良率と合格率の関係を表した図である。OC 曲線により、抜取検査において、ある不良率をもったロットがどの程度の確率で合格するかを確認することなどができる。したがって**ア**が正解。

イ **バスタブ曲線**は、時間経過に伴う機械や装置等の故障率の変化を示したものである。

ウ **ポアソン分布**は、一定の区間や時間間隔の中で発生する事象の分布を示したものである。

エ **ワイブル分布**は、物体の形状と強度の関係を統計的に表したものである。

●問 30 正解：ウ

このようなケースにおいて、著作権の帰属に関する特段の取決めがない場合、開発したプログラム著作権の原始的帰属は実際に開発を行った C 社となる。なお、会社の業務にて開発したプログラムの著作権は、個人ではなく会社に帰属する。したがって**ウ**が正解。