平成 25 年度 秋期 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：ア

桁落ちとは，値がほぼ等しい二つの数値の差を求めた場合に，有効桁数が減少することによって発生する誤差であり，コンピュータの有効桁数の制限によって発生する誤差の一つである。したがって**ア**が正解。

イ　丸め誤差の説明である。
ウ　情報落ちの説明である。
エ　打ち切り誤差の説明である。

●問 2　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わかる。したがって，**イ**が正解。

●問 3　正解：ウ

問題文で示された配列 a を**流れ図のアルゴリズム**で処理すると次のようになる。

配列 a：21，5，53，71，3，17（初期値）
ループ 1：i＝1
ループ 2：j＝6 のとき，3＞17＝No のため，入替えなし
ループ 2：j＝5 のとき，71＞3＝Yes のため，入替え（1 回目）
配列 a：21，5，53，3，71，17

ループ 2：j＝4 のとき，53＞3＝Yes のため，入替え（2 回目）
配列 a：21，5，3，53，71，17
ループ 2：j＝3 のとき，5＞3＝Yes のため，入替え（3 回目）
配列 a：21，3，5，53，71，17
ループ 2：j＝2 のとき，21＞3＝Yes のため，入替え（4 回目）
配列 a：3，21，5，53，71，17
ループ 1：i＝2
ループ 2：j＝6 のとき，71＞17＝Yes のため，入替え（5 回目）
配列 a：3，21，5，53，17，71
ループ 2：j＝5 のとき，53＞17＝Yes のため，入替え（6 回目）
配列 a：3，21，5，17，53，71
ループ 2：j＝4 のとき，5＞17＝No のため，入替えなし
ループ 2：j＝3 のとき，21＞5＝Yes のため，入替え（7 回目）
配列 a：3，5，21，17，53，71
ループ 1：i＝3
ループ 2：j＝6 のとき，53＞71＝No のため，入替えなし
ループ 2：j＝5 のとき，17＞53＝No のため，入替えなし
ループ 2：j＝4 のとき，21＞17＝Yes のため，入替え（8 回目）
配列 a：3，5，17，21，53，71

この時点で配列 a が昇順に整列したので以降の処理は省略する。したがって**ウ**が正解。

●問４　正解：イ

主記憶装置とキャッシュメモリをあわせた**平均アクセス時間**は次の式により求められる。

平均アクセス時間＝（データがキャッシュメモリに存在する確率×キャッシュメモリのアクセス時間）＋（データが主記憶装置に存在する確率×主記憶装置のアクセス時間）

″データがキャッシュメモリに存在しない確率γ″は，裏を返せば，″データが主記憶装置に存在する確率（ヒット率）″である。また，″データがキャッシュメモリに存在する確率（ヒット率）″は，″1－γ″で表すことができる。

このことから上記の式を問題文中の文字を使って表すと下記のようになる。

平均アクセス時間＝（1－γ）・ｘ＋γ・ｙ

なお，平均アクセス時間を計算するうえで，主記憶装置，キャッシュメモリの容量は特に関

係ない。

したがって**イ**が正解。

●問５　正解：ア

フェールセーフとは，システムに障害が発生した場合に，常に安全な方向に向かうように制御することである。したがって**ア**が正解。

イ　フェールソフトの説明である。
ウ　フォールトトレラントの説明である。
エ　フールプルーフの説明である。

●問６　正解：イ

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。

稼働率αを仮に0.9として，A，B，C の稼働率を求めると次のようになる。

A：$1-(1-0.9)^3=1-0.1^3=1-0.001=0.999$

B：$0.9\times(1-(1-0.9)^2)=0.9\times(1-0.01)=0.9\times0.99=0.891$

C：$1-(1-0.9)\times(1-0.9^2)=1-0.1\times0.19=0.981$

このように，システムの稼働率が装置単体の稼働率を上回るのはAとCである。したがって，**イ**が正解。

●問７　正解：ア

問題文に該当するのは**ガーベジコレクション**である。ガーベジコレクションにより，プログラマがメモリを管理する負担を軽減しているが，実行時にはシステムリソースを消費するため，同機能の実行による応答性への影響等を考慮する必要がある。したがって**ア**が正解。

イ　メモリ領域の一種であり，最後に書き込んだデータが最初に読み出される**後入れ先出し**（Last In First Out：LIFO）となっている。プログラムが一時的に使用するデータを格納するために用いられる。
ウ　メモリ領域の一種であり，プログラムが永続的に使用するデータを格納するために用いられる。C++言語の場合，new 演算子によって動的に確保され，不要になった場合には，delete 演算子を用いて明示的に解放する必要がある。

エ　記憶領域に書き込みと削除を繰り返すことによって,使用されない小さな領域の断片が多数存在する状態になることである。

●問８　正解：ウ

SRAM（Static Random Access Memory）は DRAM（Dynamic Random Access Memory）に比べアクセス速度が高速であり，通電している間はデータが失われることがない。その反面，構造が複雑でビット当たりの価格が高いため，主にキャッシュメモリとして使用されている。

DRAM は，SRAM に比べると構造が単純でビット当たりの価格が安く，高集積化に適しているため，主に主記憶装置やグラフィックスメモリとして使用されている。その反面，データを保持するためには一定時間ごとにコンデンサに充電する（これを「リフレッシュ」という）必要があるため，アクセス速度が遅く，消費電力も多い。したがって**ウ**が正解。

●問９　正解：ウ

ストアドプロシージャは，データベースへのアクセスにおいて，利用頻度の高い命令群をあらかじめサーバ側に用意しておく機能である。データベースへの命令群を大きな単位でまとめてプロシージャ化することにより，クライアントとサーバ間の通信量を削減し，処理性能を向上させることができる。一方，データベースへのアクセスを細かい単位でプロシージャ化した場合には，クライアントとサーバ間の通信が頻繁に発生するため，処理性能の向上にはつながらない。したがって**ウ**が正解。

●問 10　正解：イ

ア　ボイス・コッド正規形（Boyce/Codd normal form：BCNF）に変換する手順である。
イ　第３正規形に変換する手順である。
ウ　第２正規形に変換する手順である。
エ　第１正規形に変換する手順である。

したがって**イ**が正解。

●問 11　正解：エ

サブネットマスクとは，IP アドレスのうち，上位何ビットまでがネットワークアドレスであるかを示すものである。可変長サブネットマスクは，同一ネットワーク内で長さの異なるサブネットマスクを用いることで，柔軟にサブネットを構成し，集約する技術である。

固定長，可変長に関係なく，サブネットマスクは上位ビットからの連続した"1"によって表される。解答群を２進数に変換すると，上位ビットからの連続した"1"になるのは"255.255.255.128"のみである。したがって**エ**が正解。

●問 12　正解：エ

TCP/IP において，**OSI 基本参照モデルのトランスポート層**に位置するものには，TCP（Transmission Control Protocol）と UDP（User Datagram Protocol）がある。UDP はコネクションレス型の通信を行うプロトコルである。したがって**エ**が正解。

ア　HTTP はアプリケーション層のプロトコルである。
イ　ICMP はネットワーク層のプロトコルである。
ウ　SMTP はアプリケーション層のプロトコルである。

●問 13　正解：エ

ディジタル署名は，発信者（文書作成者）が，自分の秘密鍵を用いて文書のハッシュ値を暗号化してディジタル署名を生成し，元の文書とともに送信する。受信者は，発信者の公開鍵を用いてディジタル署名を復号するとともに，送られてきた文書のハッシュ値を求め，両者を比較することによって,発信者の正当性と文書が送信途中で改ざんされていないことを確認する。したがって**エ**が正解。

●問 14　正解：ウ

ISMS 適合性評価制度における規格文書である ISO/IEC 27001（JIS Q 27001）の「附属書Ａ：管理目的及び管理策」では，情報セキュリティ基本方針の管理目的を「情報セキュリティのための経営陣の方向性及び支持を，事業上の要求事項，関連する法令及び規制に従って規定するため」としており，その管理策として，主に次のように記述している。

・情報セキュリティ基本方針は経営陣によって承認され，全従業員及び外部関係者に公表し，通知すること
・情報セキュリティ基本方針の有効性や適切性を維持するため，定期的に，または重大な変化が発生した場合にレビューすること

したがって**ウ**が正解。

●問 15　正解：ア

クロスサイトスクリプティング（Cross-Site Scripting：XSS）とは，クライアント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不正なスクリプトを実行させることで，クッキーを盗んだり，存在しない入力欄を表示して個人情報を盗むなどする行為である。

クロスサイトスクリプティングの脆弱性が存在する Web サイトでは，JavaScript 等を用いた悪意あるコードを Web サーバに送り付け，実行させることができる。したがって**ア**が正解。

●問 16　正解：ア

親組織と子組織が**多対多の関連**であるため，親組織の数が子組織の数より多い可能性がある。なお，多対多の関連とは，0 以上対 0 以上の関係であることを表す。したがって**ア**が正解。

イ　0 以上であるため，子組織が存在しない場合もある。
ウ　子組織がある組織の親となり，３段階以上の階層となる場合もある。
エ　親組織は複数の子組織をもち，子組織もまた複数の親組織をもつことができるため，組織はネットワーク構造になっている。

●問 17　正解：エ

分岐網羅とは，判定条件が最低１回は真と偽になるデータを用いてテストを行うことである。**条件網羅**とは，判定条件が複数ある場合に，各々の条件が真と偽になるデータの組み合わせでテストを行うことである。判定条件が複数ある一つ目の分岐で条件網羅を満たすには，下記のテストデータが必要となる。

x≧1 かつ y≠1
x＜1 かつ y＝1

ア　分岐網羅，条件網羅ともに満たしていない。
イ　分岐網羅は満たしているが，条件網羅を満たしていない。
ウ　条件網羅は満たしているが，一つ目の分岐において分岐網羅を満たしていない。
エ　分岐網羅，条件網羅ともに満たしている。

したがって**エ**が正解。

●問 18　正解：イ

要件定義からシステム内部設計までの期間比は，0.25＋0.21＋0.11＝0.57 であり，これを 228 日で完了しているのであるから，プロジェクト全体の期間は 228÷0.57＝400 日 である。現在プログラム開発の 50%を完了しているため，残りの期間比は，(0.11×0.5)＋0.11＋0.21＝0.375 であり，日数に換算すると 400×0.375＝150 日 となる。したがって**イ**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：ウ

ミッションクリティカルシステムとは，障害の発生等によって中断・停止すると，企業活動や一般利用者の生活，社会等に重大な影響を及ぼすシステムである。したがって**ウ**が正解。

●問 21　正解：ウ

ア　例外取引データに対する処理の正当性の確認にはなるが，起票された受注伝票が漏れなく，重複することなく入力されていることの確認にはならない。
イ　入力された受注伝票データの正確性の確認にはなるが，起票された受注伝票が漏れなく，重複することなく入力されていることの確認にはならない。
ウ　プルーフリストとは，入力データをそのまま出力したものである。プルーフリストと受注伝票との照合が適切に行われているかどうかを監査することにより，起票された受注伝票が漏れなく，重複することなく入力されていることを確認することができる。
エ　並行シミュレーション法とは，監査人が用意した検証用プログラムと監査対象プログラムに同一のデータを入力して，両者の実行結果を比較する方法である。これによって受注伝票を処理するプログラムの論理の正当性を確認することはできるが，起票された受注伝票が漏れなく，重複することなく入力されていることの確認にはならない。

したがって**ウ**が正解。

●問 22　正解：ウ

経済産業省発行の「システム管理基準」の「Ⅱ.企画業務」「1.開発計画」において，次の 9 項目が記載されている。

（1）開発計画は，組織体の長が承認すること。
（2）開発計画は，全体最適化計画との整合性を考慮して策定すること。
（3）開発計画は，目的，対象業務，費用，スケジュール，開発体制，投資効果等を明確にす

こと。
（4）開発計画は，関係者の教育及び訓練計画を明確にすること。
（5）開発計画は，ユーザ部門及び情報システム部門の役割分担を明確にすること。
（6）開発計画は，開発，運用及び保守の費用の算出基礎を明確にすること。
（7）開発計画はシステムライフを設定する条件を明確にすること。
（8）開発計画の策定に当たっては，システム特性及び開発の規模を考慮して形態及び開発方法を決定すること。
（9）開発計画の策定に当たっては，情報システムの目的を達成する実現可能な代替案を作成し，検討すること。

ア　業務上の利便性よりも全体最適を優先する必要がある。
イ　開発作業に着手する前に策定する必要がある。
ウ　上記の（9）に合致しており，正しい記述である。
エ　利用部門とシステム部門の役割分担を明確にする必要がある。

したがって**ウ**が正解。

●問 23　正解：エ

IT 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いく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。

ア　**ABC**（Activity Based Costing：活動基準原価計算）の説明である。
イ　**バランススコアカード**の説明である。
ウ　**ベンチマーキング**の説明である。

●問 24　正解：イ

DFD（Data Flow Diagram）などを用いた業務の構造化分析においては，業務やシステムにおけるデータの流れに着目し，次の流れで新システムのモデル化を行う。

① 現行システムの物理モデル（現物理モデル）を作成

② ①を抽象化して現論理モデルを作成
③ ②をもとに新システムにおける論理モデル（新論理モデル）を作成
④ ③を実装する新物理モデルを作成する

ア　現論理モデルの説明である。
イ　新論理モデルの説明である。
ウ　現物理モデルの説明である。
エ　新物理モデルの説明である。

問題文の「業務のあるべき姿を表す論理モデル」とは，新論理モデルのことである。したがってイが正解。

●問 25　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などのテーマに関する未来予測を行う場合など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。

ア　複数データ間の因果関係を分析することで,目的とする解を導き出す手法である。
イ　時間の経過によって変化する事象について,ある一時点で横断的に取得したデータを分析する方法である。
ウ　時間の経過によって得られたデータを回帰分析する手法である。

●問 26　正解：ウ

売り手側でのマーケティング要素４Ｐとは，次の通りである。

・製品（Product）
・価格（Price）
・流通（Place）
・プロモーション（Promotion）

一方，回答群に示されているのが買い手側での要素４Ｃであり，これらは各々次のように対応付けられる。

・製品（Product）：顧客価値（Customer Value）
・価格（Price）：顧客コスト（Customer Cost）
・流通（Place）：利便性（Convenience）

・プロモーション（Promotion）：コミュニケーション（Communication）

したがって**ウ**が正解。

●問 27　正解：エ

イノベーション（innovation）は，革新，新機軸などの意味であり，**プロダクトイノベーション**とは，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である。一方，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ることを**プロセスイノベーション**という。

解答群のア～ウはいずれもプロセスに関するものであり，プロダクトイノベーションに該当するのは**エ**である。

●問 28　正解：エ

EDI（Electronic　Data Interchange：電子データ交換）とは，BtoB 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など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）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などに関する事項
レベル 2（情報表現規約）：標準的なメッセージの形式などに関する事項
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。

●問 29　正解：ア

定額法による減価償却額は，次の式で求められる。

(取得価額－残存価額)÷耐用年数
＝(800－0)÷5＝160 千円

年間の減価償却額が 160 千円であるから，３年後の残存簿価は次のようになる。

800－(160×3)＝ 320 千円

これを 115 千円で売却するので，固定資産売却損は 205 千円となる。
したがって**ア**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当たる。

イ　たと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。