平成28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

問題文の式に実際に値を代入してみると次のようになる。

$x_0 = 0,\ x_1 = 1$

$x = \frac{0+1}{2} = 0.5$

$x_1 = 0.5$ として(2)を繰り返す。

$x = \frac{0+0.5}{2} = 0.25$

$x_1 = 0.25$ として(2)を繰り返す。

$x = \frac{0+0.25}{2} = 0.125$

$x_1 = 0.125$ として(2)を繰り返す。

このように，(2)を n 回実行した際の x の値は次の式で表すことができる。

$x = \frac{1}{2^n}$

n ＝ 10 のとき，xは次の式で表すことができる。

$x = \frac{1}{2^{10}} = \frac{1}{1{,}024} < 0.001$

したがって**ア**が正解。

●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 しかないことがわかる。

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：エ

ヒープソートとは，未整列の部分を順序木とし，その最小値を取り出して整列後の部分に移す，という操作を繰り返すことでデータを整列させる方式である。したがって**エ**が正解。

ア　シェルソートの説明である。
イ　クイックソートの説明である。
ウ　バブルソートの説明である。

●問４　正解：エ

メモリインタリーブは，次のような方式によって，連続したメモリへのアクセスを高速化する技法である。

・主記憶装置を並行してアクセス可能な幾つかの区画（バンク）に分割する
・連続したアドレスが異なるバンクになるようにアドレスを割り当てる
・複数のバンクに対して並行アクセスすることで，連続したアドレスに対する処理を同時

に行う

したがって**エ**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)

稼働率は MTBF，MTTR の比率によって決定するため，両者がともに 1.5 倍になったとしてもその比率は変わらず，したがって稼働率も変わらない。したがって**エ**が正解。

●問６　正解：イ

ア　メモリコンパクションの説明である。
イ　正しい記述である。
ウ　動的再配置の説明である。
エ　動的リンキングの説明である。

ガーベジコレクションは，不要になったメモリ領域を自動的に解放する機能であり，Java などで採用されている。これにより，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**イ**が正解。

●問７　正解：エ

一方のスイッチの状態（0, 1）にかかわらず，スイッチを押す（1）ことにより，出力を反転できるのであるから，XOR（排他的論理和）が該当する。したがって**エ**が正解。

A のスイッチの状態（0, 1）と B のスイッチの状態（0, 1）の組合せによる出力（照明）は次のようになる。

A＝0，B＝0 のとき：出力=0（消灯）
A＝1，B＝0 のとき：出力=1（点灯）
A＝0，B＝1 のとき：出力=1（点灯）
A＝1，B＝1 のとき：出力=0（消灯）

●問８　正解：ウ

問題文に該当するのは**SMIL**（Synchronized Multimedia Integration Language）である。したがって**ウ**が正解。なお，SMIL は「スマイル」と発音される。

ア　Ajax（Asynchronous JavaScript + XML）は，JavaScript などのスクリプト言語を使ってサーバと非同期通信を行うことで，Web ページ全体を再描画することなく，ページの必要な箇所だけを部分的に更新することを可能にする技術である。

イ　CSS（Cascading Style Sheets）は，Web ページの構成要素をどのように装飾するかを指定するための言語である。

エ　SVG（Scalable Vector Graphics）は，XML で記述されたベクターグラフィックス言語のスタンダードである。

●問９　正解：イ

B+木は，B 木から派生した木構造の一種であり，挿入・検索・更新が効率的に行える特徴を持つ。B+木では，木の深さが一定となっており，全てのデータは最下層ノードの葉に格納され，中間ノードの各節にはインデックスと下位層のノードへのポインタが格納される。

B+木におけるデータ総件数 X は，各節の数である次数 b と深さ h で次のように表すことができる。

$$X = b^h$$

木の深さが一定であるため，アクセス回数は h となり，次のように X の対数で表すことができる。

$$h = \log_b x$$

したがって**イ**が正解。

●問 10　正解：ア

ロールフォワード（前進復帰）によって処理が復旧できるのは，システム障害発生前にコミットされたトランザクションであるため，T2 と T5 が該当する。一方，障害発生時に実行中であったトランザクションはロールバック（後退復帰）によって復旧する必要があるが，Read 処理のみの T3 は復旧させる必要はないため，T6 のみが該当する。したがって**ア**が正解。

●問 11　正解：ア

ARP（Address Resolution Protocol）とは，IP アドレスから MAC アドレス（Ethernet の物理アドレス）を得るために使われるプロトコルである。ARP とは逆に，MAC アドレスから IP アドレスを得るために使われるプロトコルが RARP（Reverse Address Resolution Protocol）である。したがって**ア**が正解。

●問 12　正解：イ

IPv6 では，VPN で広く用いられているパケット暗号化プロトコルである IPsec を標準機能として装備しており，それに関する情報等が拡張ヘッダに格納される。したがって**イ**が正解。

●問 13　正解：エ

チャレンジレスポンス認証方式とは，次のような仕組みで利用者を認証する方式である。

・サーバが「チャレンジ」と呼ばれる乱数文字列をクライアントに送る
・クライアントは，「チャレンジ」と，利用者があらかじめ入力しておいたパスワードを組み合わせたものをハッシュ関数に通して出力した文字列（レスポンス）をサーバに返す
・サーバはあらかじめ登録されている利用者のパスワードを用いて同様の計算を行った結果と，クライアントから返されたレスポンスとを比較することによって利用者を認証する（つまり，両者が同じであれば認証可と判断する）

したがって**エ**が正解。

●問 14　正解：イ

ア　そのような必要はない。
イ　正しい記述である。
ウ　指紋認証に室内の照明は影響しない。
エ　非接触型 IC カードに関する説明である。

したがって**イ**が正解。

●問 15　正解：イ

ハイブリッド暗号方式は，共通鍵暗号方式と公開鍵暗号方式を組み合わせた方式である。
ハイブリッド暗号方式では，データの暗号化に処理の速い共通鍵暗号方式を用いる。データの暗号化に用いた共通鍵暗号方式の鍵を安全に相手に渡すために，鍵自体を公開鍵暗号

方式（通信相手の公開鍵）を用いて暗号化する。

ハイブリッド暗号方式は，共通鍵暗号方式，公開鍵暗号方式各々の短所を，各々の長所により互いに補い合うことで，鍵管理コストと処理性能の両立を図る。したがって**イ**が正解。

●問 16　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 17　正解：ア

ア　正しい記述である。特許で保護された技術を使っているか否かに関係なく，使用許諾することが可能である。

イ　販売されている製品に組み込まれていたとしても，ソフトウェア単体で使用許諾対象にすることが可能である。

ウ　ソフトウェア単体で使用許諾対象にすることが可能である。

エ　ソースコードの無償での使用許諾のみでオープンソースソフトウェアになるわけではない。なお，OSI（Open Source Initiative）では，OSD（The Open Source Definition）において，オープンソースソフトウェアを次ように定義している。

1.再配布の自由（有償／無償配布の自由）
2.ソースコードの入手が可能
3.派生ソフトウェアの同ライセンス条件による配布
4.パッチファイルの配布を認める場合には，同一性保持のため，派生物に対して元のソフトウェアとは異なる名称やバージョン番号を持つよう要求可能
5.特定の個人やグループに対する差別の禁止
6.特定の利用分野に対する差別の禁止

7.再配布における追加ライセンス要求の禁止
8.特定製品でのみ有効なライセンスの禁止
9.同じ媒体で配布される他のソフトウェアを制限するライセンスの禁止
10.技術的中立の保持

したがって**ア**が正解。

●問 18　正解：イ

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。問題文に該当するのはコンフィギュレーション・マネジメント（構成管理）である。したがって**イ**が正解。

ア　アーンド・バリュー・マネジメントとは，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）することにより，進捗管理を行う手法である。
ウ　コンフリクトとは衝突・対立を意味する言葉であり，コンフリクト・マネジメントとは，それらを組織の成長や活性化の機会と捉え，積極的に受け入れて問題解決を図ろうとする活動である。
エ　ポートフォリオマネジメントとは，企業が自社の事業の市場競争力を分析し，最適な資金配分や事業構成を決定するための管理手法である。

●問 19　正解：エ

問題で示されている図はアローダイヤグラムもしくは PERT 図（Program Evaluation and Review Technique）とも呼ばれ，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と，プロジェクト全体の所要日数を短縮することができる。なお，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。

問題文の PERT 図には次の 4 つの経路があり，クリティカルパスは「A→D→G」（最短完了日は 30 日）である。

A→F：8＋8＝16（日）
A→D→G：8＋10＋12＝30（日）
B→E→G：5＋9＋12＝26（日）
C→H→I：12＋6（ダミー作業による待ち）＋5＋4＝27（日）

作業 H，作業 I で 9 日必要であるため，作業 H はプロジェクトの開始から遅くとも 21 日後（30－9＝21）に開始しなければならない。したがって**エ**が正解。

●問 20　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 21　正解：ウ

1 か月で使用する磁気テープは，毎月初日のフルバックアップ用で 1 本と，2 日から月末日までの差分バックアップ用で 1 本の計 2 本である。また，処理条件の(3)の例で，4 月 30 日以降のデータについて指定日の状態にファイルを復元するには，4 月から 10 月までの 7 か月分のバックアップが必要である。したがって，必要な磁気テープは 14 本である。**ウ**が正解。

●問 22　正解：イ

IT への対応は，IT 環境への対応と IT の利用及び統制からなっている。IT 環境への対応とは，組織の目標を達成するために，あらかじめ適切な方針と手続を定め，それを踏まえて組織内外の IT 環境に対して適切な対応を行うことである。

IT の利用及び統制とは，内部統制の他の基本的要素の有効性を確保するために IT を有効かつ効率的に利用すること，そして，内部統制の他の基本的要素を機能させることにより，IT が有効かつ適正に利用されるよう監視・統制することである。

IT の統制は，IT 業務処理統制と IT 全般統制からなる。

IT 業務処理統制

組織の業務プロセスに組み込まれた個々の情報システム（アプリケーションシステム）の処理工程（入力・編集・計算・送信・保存・削除等）において，データの欠落や重複，改ざんなどが発生することなく，その正当性・正確性・網羅性・一貫性等を確保するために行う各種のコントロール。

IT 全般統制

IT 業務処理統制が適正かつ有効に機能するために必要な組織全体の IT 基盤や施策，体制などからなる各種のコントロール。

したがってイが正解。

●問 23　正解：ウ

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，内部業務プロセス，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　顧客の KPI（Key Performance Indicators：重要業績評価指標）の目標例である。
イ　内部業務プロセスの KPI の目標例である。
ウ　学習と成長の KPI の目標例である。
エ　財務の目標例である。

したがってウが正解。

●問 24　正解：イ

BI（Business Intelligence）は，企業の業務システム等から蓄積された膨大なデータを分析・加工することにより，経営判断や意思決定に活用する手法である。したがってイが正解。

●問 25　正解：ア

「情報システム・モデル取引・契約書」は，経済産業省が設置した「情報システムの信頼性向上のための取引慣行・契約に関する研究会及びタスクフォース（研究会）」における，情報システムの信頼性向上・取引の可視化に向けた取引・契約のあり方等の議論及びパブリックコメントを集約し，提示したものである。

ア　正しい記述である。成果物が明確になっていない場合には準委任契約にすべきである。
イ　仕様の決定権はユーザ側にある。
ウ　成果物が具体的に想定できないのであれば請負契約にすべきではない。
エ　成果物が明確でないため，請負契約にすべきではない。

したがってアが正解。

●問 26　正解：ウ

ベンチマーキングとは，企業等が優れた業績を上げている競合企業等との比較分析を行

い，それを自社の経営改革に活用する活動である。したがってウが正解。

●問 27　正解：イ

アンゾフの成長マトリクスとは，縦軸に「市場」，横軸に「製品」を取り，それらに「既存」と「新規」の 2 区分を設けることにより，「市場浸透」「新製品開発」「新市場開拓」「多角化」の 4 象限のマトリクスとしたものである。したがってイが正解。

●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：イ

故障率曲線とは，機械や装置の使用時間と，それに伴う故障率の関係を示した曲線のことであり，その形からバスタブ曲線とも呼ばれる。時間の経過により，故障率が減少する「初期故障期」，故障率が安定する「偶発故障期」，故障率が増加する「摩耗故障期」の 3 つに分けられ，図中の A の期間は「偶発故障期」である。

ア　初期故障期に実施すべきことである。
イ　偶発故障期に実施すべきことである。
ウ　摩耗故障期に実施すべきことである。
エ　摩耗故障期に実施すべきことである。

したがってイが正解。

●問 30　正解：ア

産業財産権は，産業の発展を図ることを目的としており，意匠権，実用新案権，商標権，特許権が該当する。産業財産権は特許庁が所管している。

一方著作権は，音楽，絵画，映画，小節など人間の思想や感情を創作的に表現したもの保護する。著作権は文化の発展を図ることを目的としており，文化庁が所管している。

したがってアが正解。