平成 29 年度 秋期 情報処理安全確保支援士

＜午前Ⅰ解答・解説＞

●問 1　正解：ア

相関係数とは，2 つの変量間の相関の度合いを表したものであり，－1～1 までの値をとる。相関係数が 1 に近いときは 2 つの変量間に正の相関があるといい，標本点は正の傾きをもつ直線付近に分布する。一方，相関係数が－1 に近いときは負の相関があるといい，標本点は負の傾きをもつ直線付近に分布する。また，相関係数が 0 に近いときは 2 つの変量間には相関がないこと（無相関）を表す。したがって**ア**が正解。

●問 2　正解：エ

表より，各アルファベットの変換後のビット列の長さは次のとおりである。

a：1 ビット
b：2 ビット
c：3 ビット
d：3 ビット

これに各アルファベットの出現確率を乗じて，変換後のアルファベットのビット長の平均値を求める。

a：1 × 0.4 ＝ 0.4 ビット
b：2 × 0.3 ＝ 0.6 ビット
c：3 × 0.2 ＝ 0.6 ビット
d：3 × 0.1 ＝ 0.3 ビット

a ＋ b ＋ c ＋ d ＝ 0.4 ＋ 0.6 ＋ 0.6 ＋ 0.3 ＝ 1.9 ビット

変換前の各アルファベットのビット列の長さは 2 ビットの固定長であるから，変換後のビット列の長さの比は次のようになる。

1.9 ÷ 2 ＝ 0.95

したがって**エ**が正解。

●問 3　正解：ウ

非負の整数 n の階乗を計算する式に該当するのは"n×fact(n－1)"であるが，0 の階乗は 1 であるため，"if n＝0"が真の場合には 1 を返す必要がある。したがって**ウ**が正解。

●問 4　正解：イ

主記憶装置，キャッシュメモリを合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

MTBF（Mean Time Between Failure：平均故障間隔）と **MTTR（Mean Time To Repair：平均修理時間）**は，次の式でシステム等の稼働率を算出する際に用いられる。

$$\text{稼働率} = \frac{\text{MTBF}}{\text{MTBF} + \text{MTTR}}$$

ア　エラーログを取得することで，障害の発生箇所や内容を特定することが可能となるため，MTTR を短くするのに役立つ。正しい記述である。
イ～エ　これらはいずれも MTBF を長くするのに役立つものである。

●問 6　正解：イ

自分より優先順位の高い他のタスクが実行可能状態になると，実行状態のタスクは**プリエンプション**（Preemption：**先取り**，**差替え**）によって CPU 使用権を奪われ，実行可能状態となる。その後，プリエンプションが解消されると再び実行状態となる。

したがって**イ**が正解。

●問 7　正解：ウ

問題文の回路を真理値表で表すと次のようになる。

G：0 0 1 1
A：0 1 0 1
X：0 1 1 0

G：0 0 1 1
B：0 1 0 1
Y：0 1 1 0

X, Y ともに排他的論理和（XOR）の出力結果であるため，これを図で表すと**ウ**の回路となる。

●問 8　正解：イ

JIS X 8341-1 の目的は，情報通信機器及びサービスを最も幅広い層の人々が，その能力，障害，制限及び文化にかかわらず利用できるようにすることである。様々な能力をもつ最も幅広い層の人々に対する製品，サービス，環境又は施設のユーザビリティを「アクセシビリティ」としている。また，アクセシビリティについて，利用者の能力の全範囲に十分に注意を払うと同時に利用の特定の状況を考慮し，できるだけ高い水準の有効さ，効率及び満足度を達成することを目指す，としている。

ア　全ての個人に対して等しい水準のアクセシビリティを達成するわけではない。
イ　適切な記述である。
ウ　一般的な人間工学の原則に従うことをアクセシビリティの原則としている。
エ　平均的能力をもった人々ではなく，高齢者や障害者をはじめ，様々な能力をもつ人々を対象としている。

●問 9　正解：イ

射影（projection）とは，表から必要な列だけを取り出すことである。関係 R の A, C へ

の射影の結果は，A 列，C 列だけが取り出されるとともに，集合の特性により，重複した行は除かれ，次のようになる。

A	C
a1	c1
a1	c2
a2	c2

このような結果を得るためには，SQL 文に「DISTINCT」を指定する必要がある。したがって**イ**が正解。

●問 10　正解：エ

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**エ**が正解。

●問 11　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 12　正解：エ

利用者が Web サイトを閲覧した際に，気付かないうちに利用者の PC にマルウェア等の不正プログラムをダウンロードする手法を**ドライブバイダウンロード**（drive-by-download）と呼ぶ。攻撃者はこの攻撃を成立させるため，利用者が日常的に閲覧する Web サイトを改ざんし，閲覧時に攻撃コードが実行されるようにしておくなどの手法を用いる。したがって**エ**が正解。

ア　"autorun.inf"を悪用してマルウェアを実行する攻撃手法の説明である。
イ　ランサムウェアの説明である。
ウ　ウォードライビングの説明である。

●問 13　正解：イ

ア　AES（Advanced Encryption Standard）は，米国標準の共通鍵暗号方式であり，RSA（Rivest Shamir Adleman）は公開鍵暗号方式の一種である。
イ　正しい記述である。
ウ　公開鍵暗号方式では，復号に使用する鍵を秘密にして，暗号化に使用する鍵を公開する。
エ　ディジタル署名では，公開鍵暗号方式を使用する。

●問 14　正解：エ

サイバーレスキュー隊 J-CRAT（Cyber Rescue and Advice Team against targeted attack of Japan）は，標的型サイバー攻撃の被害拡大防止のため，IPA が 2014 年 7 月に発足させた組織である。

標的型サイバー攻撃の被害の発生が予見され，その対策の対応遅延が社会や産業に重大な影響を及ぼすと判断される組織や，標的型サイバー攻撃の連鎖の元となっていると推測される組織などに対しては，レスキュー活動にエスカレーションして支援を行う。したがって**エ**が正解。

ア　内閣サイバーセキュリティセンター（NISC）の役割である。
イ　サイバー情報共有イニシアティブ（J-CISP）の役割である。
ウ　日本セキュリティオペレーション事業者協議会（ISOG-J）の役割である。

●問 15　正解：ア

WAF（Web Application Firewall）は，クロスサイトスクリプティング，SQL インジェクション，OS コマンドインジェクション等，Web アプリケーションに対する攻撃を検出・排除することでセキュアな Web アプリケーション運用を実現する製品である。したがって**ア**が正解。

●問 16　正解：ア

モジュール強度とは，モジュールに含まれる機能の結びつきの強さであり，次の 7 種類がある。上のものほどモジュール強度が高く，再利用や拡張がしやすくなる。

機能的強度：一つの機能だけを提供するモジュール
情報的強度：特定のデータ構造や資源を扱う機能をまとめたモジュール
連絡的強度：関連のある逐次的な機能で要素が連絡し合うモジュール

手順的強度：関連のある逐次的な機能をまとめたモジュール
時間的強度：時間的に連続した複数の機能をまとめたモジュール
論理的強度：関連する複数の機能をまとめたモジュール
暗号的強度：関連性を考慮せずに複数の機能をまとめたモジュール

ア　情報的強度に該当する。
イ　時間的強度に該当する。
ウ　論理的強度に該当する。
エ　連絡的強度に該当する。

これらの中でモジュール強度が最も高いのは**ア**である。

●問 17　正解：ア

CMMI（Capability Maturity Model Integration）は，ソフトウェア開発の品質向上，生産性向上，リスクの軽減等を目的として，米国カーネギメロン大学ソフトウェア工学研究所によって開発された。CMMI では，次の 5 段階でソフトウェア開発組織及びプロジェクトのプロセスの成熟度を評価・判定する。

レベル 1：プロセスの管理が行われていない状態
レベル 2：基本的なプロジェクト管理が行われている状態
レベル 3：プロセスの標準化が行われている状態
レベル 4：定量的な管理が行われている状態
レベル 5：継続的なプロセス改善が行われている状態

したがって**ア**が正解。

●問 18　正解：ア

EVM（Earned Value Management）は，プロジェクトに進捗や作業のパフォーマンスを定量化（金額換算）し，プロジェクトの現状及び将来の状況を評価する進捗管理手法であり，コストとスケジュールが管理対象となる。したがって**ア**が正解。

●問 19　正解：イ

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 8 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。

保守性とは，製品やシステムが保守担当により修正するにあたっての効果性，効率性の

度合いである。したがって**イ**が正解。

ア　信頼性の評価指標である。
ウ　移植性の評価指標である。
エ　機能適合性の評価指標である。

●問 20　正解：ウ

1 日のサービス提供時間が 14 時間,1 か月の稼働日数が 30 日であるから,可用性が 100%の場合の 1 か月のサービス提供時間は次のようになる。

14 × 30 ＝ 420 時間

サービス提供時間内の停止時間は 7 時間であるから，この月のサービス提供時間は 413 時間であり，可用性は次のようになる。

413 ÷ 420 ≒ 0.983

したがって**ウ**が正解。

●問 21　正解：ウ

経済産業省発行の**「システム監査基準」**において，システム監査の目的は次のように記載されている。

> システム監査の目的は，組織体の情報システムにまつわるリスクに対するコントロールがリスクアセスメントに基づいて適切に整備・運用されているかを，独立かつ専門的な立場のシステム監査人が検証又は評価することによって，保証を与えあるいは助言を行い，もって IT ガバナンスの実現に寄与することにある。

問題のような状況となった場合，システム監査人は被監査部門から独立した立場で必要な助言を行うべきである。

ア　システム監査人は対策の実施を指示する立場にない。
イ　システム監査人は被監査部門の活動に参加することはできない。
ウ　システム監査人はとして適切な行動である。
エ　システム監査人は要員の追加を要求する立場にない。

したがって**ウ**が正解。

●問 22　正解：エ

在庫データの網羅性を確保するためには，在庫データに抜けもれや重複がなく，全ての入庫及び出庫を正しく把握できていることが求められる。入庫及び出庫記録に対して，自動的に連番を付与していることは，在庫データの網羅性のチェックポイントとして適切である。したがって**エ**が正解。

●問 23　正解：イ

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。

エンタープライズアーキテクチャにおいて，業務や情報システムの理想を表すのは「To-Be モデル」である。したがって**イ**が正解。

●問 24　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。多段階契約を採用した場合，契約作業の手間は増加するが，開発途中で発生する仕様変更の影響を極力抑えることができる。また，工程ごとに異なるベンダに分割発注することも可能となる。
イ　SLA（(Service Level Agreement）導入の目的である。
ウ　仮発注合意書のプロセスを設けることの目的である。
エ　基本契約書を締結する目的である。

したがって**ア**が正解。

●問 25　正解：エ

ファブ（fab）は"fabrication facility"（工場）の略語であり，**ファブレス**（fabless）**企業**とは，工場などの生産設備を自社で所有せずに製造業として活動する企業である。

ア　委託による生産を専門に行うファウンドリ企業の説明である。

イ　OEM（Original Equipment Manufacturer）による生産を行う企業の説明である。
ウ　自社内で開発・生産を行う企業の説明である。
エ　半導体ファブレス企業の説明である。

したがって**エ**が正解。

●問 26　正解：ウ

CRM（Customer Relationship Management）とは，多様化する顧客ニーズに対応するため，顧客に関するあらゆるデータをデータベース化して共有し，マーケティング活動に反映させる手法である。

ア　リテールサポートの説明である。
イ　ERP（Enterprise Resource Planning）の説明である。
ウ　CRM の説明である。
エ　SCM（Supply Chain Management）の説明である。

したがって**ウ**が正解。

●問 27　正解：ア

ア　正しい記述である。WTO の「政府調達に関する協定」（Agreement on Government Procurement : GPA）の加盟国では，政府調達は国際標準の仕様に従って行われる。
イ　技術的な優位性が保証されるわけではない。
ウ　特許のライセンス料が無償になることはない。
エ　国際標準に適合していても輸出先国で規制されている場合は輸出できない。

●問 28　正解：ア

エッジコンピューティングとは，端末の近くにサーバを分散配置することにより，負荷分散や低遅延化を図る技術である。したがって**ア**が正解。

ア　適切な説明である。
イ　機械学習の説明である。
ウ　グリッドコンピューティングの説明である。
エ　エネルギーハーベスティングの説明である。

●問 29　正解：エ

デルファイ法とは，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。したがって**エ**が正解。

●問 30　正解：ア

著作権法の第十五条の 2「職務上作成する著作物の著作者」において，「法人等の発意に基づきその法人等の業務に従事する者が職務上作成するプログラムの著作物の著作者は，その作成の時における契約，勤務規則その他に別段の定めがない限り，その法人等とする。」と定められている。そのため，開発成果物の著作権の帰属先が記載されていない場合，その著作権は実際に開発を行った側に帰属することになり，請負の場合は発注先に帰属し，派遣の場合は派遣先に帰属する。したがって**ア**が正解。