平成28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：ウ

123 ÷ 26 ＝ 4 余り 19
であるから，一桁目が 19 で，二桁目が 4 となる英字の組合せとなる。

A＝0, Z＝25 とすると，E＝4, T＝19 となる。したがってウが正解。

●問２　正解：ウ

ア　この方法では，“aa”を符号化すると“00”，“c”を符号化しても"00"となるため，一意に復号することができない。

イ　この方法では，“ac”を符号化すると“010”，“ba”を符号化しても“010”となるため，一意に復号することができない。

ウ　この方法であれば符号化されたビット列から元のメッセージが一意に復号可能である。a，b，c，d の出現頻度からビット列の長さを計算すると次のようになる。

a : 0.5 × 1 ビット ＝ 0.5
b : 0.3 × 2 ビット ＝ 0.6
c : 0.1 × 3 ビット ＝ 0.3
d : 0.1 × 3 ビット ＝ 0.3

a + b + c + d ＝ 1.7

エ　ウと同じく，この方法であれば符号化されたビット列から元のメッセージが一意に復号可能である。a，b，c，d の出現頻度からビット列の長さを計算すると次のようになる。

a : 0.5 × 2 ビット ＝ 1.0
b : 0.3 × 2 ビット ＝ 0.6
c : 0.1 × 2 ビット ＝ 0.2
d : 0.1 × 2 ビット ＝ 0.2

a + b + c + d ＝ 2.0

このように，符号化されたビット列から元のメッセージが一意に復号可能であって，ビット列の長さが最も短くなるのは**ウ**である。

●問３　正解：ウ

並列処理の同期があると，一方の処理が終了しても先には進まず，もう一方の処理が終了するのを待ってから次の処理に進む。そのため，問題文の流れ図では，まず A の処理が実行された後，B と C がほぼ同時に実行される。B が先に終了した場合には C の終了を待ち，C が先に終了した場合には B の終了を待って同期をとり，再び B と C がほぼ同時に実行され，以降もそれを繰り返すことになる。したがって**ウ**が正解。

●問４　正解：イ

SIMD とは，単一の命令（Single Instruction）で，複数のデータ（Multiple Data）を処理する方式である。したがってイが正解。

ア　SISD（Single Instruction Single Data）の説明である。
ウ　MISD（Multiple Instruction Single Data）の説明である。
エ　MIMD（Multiple Instruction Multiple Data）の説明である。

●問５　正解：ア

ライブマイグレーション（Live Migration）とは，ある仮想サーバ上で稼働している OS やソフトウェアを停止させることなく，別の物理サーバへ移し替える技術である。元の環境で実行していた処理やネットワーク接続も停止させることなくそのままの状態で移すことが可能である。したがって**ア**が正解。

●問６　正解：ア

LRU（Least Recently Used）**アルゴリズム**は，ページフォールトが発生した際に，使用後の経過時間が最長のページを置換対象として除去（ページアウト）し，必要なページを読み込む（ページイン）ページ置換アルゴリズムである。したがってアが正解。

イ　必要最低限のページテーブルでよい。
ウ　ガーベジコレクションではなく，ページアウトとページインを行う。
エ　ページのサイズは固定であるため，フラグメンテーション（断片化）は発生しない。

●問７　正解：エ

DRAM（Dynamic Random Access Memory）は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，消費電力も多いという特徴がある。したがって**エ**が正解。

ア，イ　フラッシュメモリの説明である。
ウ　SRAM（Static Random Access Memory）の説明である。

●問８　正解：ア

利用者の満足度を評価するには，実際に使用した利用者に**インタビュー**を行うのが適切である。したがって**ア**が正解。

イ　**ヒューリスティック評価**とは，専門家の知見に基づいて評価する手法である。
ウ　**ユーザビリティテスト**は，複数の利用者が製品を使用する過程を観察し，評価する手法である。
エ　製品を使用した際のログデータから評価する手法である。

●問９　正解：ウ

参照制約とは，データの追加，更新，削除などを行うときに，関連するテーブル間の整合性を保つようにする制約である。“在庫”表への行追加を行った場合，“製品”表に存在しない製品番号が指定されるとテーブル間の整合性が保てなくなるため，参照制約が働く。したがって**ウ**が正解。

●問 10　正解：エ

データベースの回復処理は，**バックアップ**と**トランザクションログ**（「ジャーナルファイル」とも呼ばれる）を用いて行う。バックアップには，ある時点でのデータベースの内容そのものが記録されており，トランザクションログにはデータベースの更新処理に関する履歴情報が記録されている。

データベースの媒体障害時には，媒体交換後，最新のバックアップでデータベースを復元し，更新後のトランザクションログを用いてバックアップ取得以降にコミットした全てのトランザクションを**ロールフォワード**する。したがって**エ**が正解。

●問 11　正解：イ

スイッチングハブと同様に，OSI 参照モデルの第 2 層であるデータリンク層のレベルで動作し，同様の機能をもつ装置として**ブリッジ**がある。したがって**イ**が正解。

●問 12　正解：ア

ア　**AES**（Advanced Encryption Standard）は，米国標準の共通鍵暗号方式である。

イ　**ElGamal 暗号**は，離散対数問題を応用した公開鍵暗号方式の一つである。

ウ　**RSA**（Rivest Shamir Adleman）は代表的な公開鍵暗号方式であり，桁数の大きな整数の素因数分解が困難であることを安全性の根拠にしている。

エ　**楕円曲線暗号**（Elliptic Curve Cryptosystem）は，楕円曲線上の離散対数問題の難しさを安全性の根拠にする公開鍵暗号方式の一つである。

したがって**ア**が正解。

●問 13　正解：エ

WAF 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。

WAF のブラックリストには, Web アプリケーションに対する攻撃の特徴を示す通信データのパターンを定義しておくことで，攻撃を検出し，該当する通信を遮断する。

一方, WAF のホワイトリストには, 正常な通信データのパターンを定義しておくことで，それに合致しない通信データを攻撃として検出する。したがって**エ**が正解。

●問 14　正解：エ

問題文の攻撃手法は，Web アプリケーションのユーザ認証やセッション管理の不備を突いて，サイトの利用者に Web アプリケーションに対する不正な処理要求を行わせる手法であり，**クロスサイトリクエストフォージェリ**（Cross-Site Request Forgeries : **CSRF**）と呼ばれる。CSRF による被害を防ぐためには，Web アプリケーションのユーザ認証機能やセッション管理機能を強化し，不正なリクエストを受け付けないようにする必要がある。具体的には，次のようなものがある。

・POST メソッドを使用し，hidden フィールドに秘密情報をセットする
・確定処理の直前で再度パスワードを入力させる
・Referrer を用いてリンク元の正当性を確認する
・重要な操作を行った後で，その内容を登録アドレスにメール送信する

したがって**エ**が正解。

●問 15　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働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 16　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。

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，効率性の度合である。

ア　使用性に影響するものである。
イ　保守性に影響するものである。
ウ　信頼性に影響するものである。
エ　性能効率性に影響するものである。

したがって**イ**が正解。

●問 17　正解：イ

モジュールの結合度とは，モジュール間の結びつきの強さを表し，モジュールの結合度が低いほどモジュールの保守性は高まる。

モジュールの結合度は 6 種類に分類され，低い順に並べると次のようになる。

・データ結合
　単一のデータ項目を引数で受け渡す。
・スタンプ結合
　データ構造を引数で受け渡す。
・制御結合
　フラグなどの制御要素を受け渡す。
・外部結合
　単一のデータ項目を大域的データで受け渡す。
・共通結合
　データ構造を大域的データで受け渡す。
・内容結合
　他のモジュールの内部を直接参照する。

したがって**イ**が正解。

●問 18　正解：ア

COCOMO（Constructive Cost Model）は，予想されるソースコードの行数にエンジニアの能力などの補正係数を掛け合わせてソフトウェアの開発工数，期間等を算出する手法である。COCOMO では，自社における生産性に関する蓄積されたデータが必要である。したがって**ア**が正解。

イ　過去の開発における工数も見積りの参考になる。
ウ　工数の見積りはソフトウェアの品質管理においても有効なデータとなる。
エ　**ファンクションポイント法**はソフトウェアの機能に着目し，その複雑さなどから見積もる手法であり，プログラムのステップ数は不要である。

●問 19　正解：ア

IT サービスマネジメントにおけるサービスレベル管理は，IT サービスを利用する顧客とそれを提供する組織との間で，SLA（Service Level Agreement）として合意したサービスレベルの目標値の達成度を監視し，改善するためのプロセスである。したがって**ア**が正解。

イ　可用性管理の説明である。

ウ　インシデント管理の説明である。
エ　サービスの予算業務及び会計業務の説明である。

●問 20　正解：ウ

IT サービスマネジメントにおける構成管理は，IT サービスの構成品目を正確に把握し，それを常に最新の状態に維持管理するとともに，確認・監査することを目的としたプロセスである。これにより，他のプロセスの確実な実施を支援できる。したがって**ウ**が正解。

ア　キャパシティ管理を導入することによって得られるメリットである。
イ　サービス継続及び可用性管理を導入することによって得られるメリットである。
エ　サービスレベル管理を導入することによって得られるメリットである。

●問 21　正解：ウ

クラウドサービスを提供する事業者が突然サービスを停止したとすれば，サービス上に保存されている情報が消失してしまう可能性がある。クラウドサービスを提供する事業者に信頼が置け，かつ，事業やサービスが継続性について検討することは，情報の消失の予防に関するチェックポイントとして適切である。したがって**ウ**が正解。

ア　完全性に関するチェックポイントである。
イ　可用性に関するチェックポイントである。
エ　機密性に関するチェックポイントである。

●問 22　正解：イ

予備調査は，本調査に先立ち，監査人が監査対象を明確に把握するため，被監査部門から事前に入手した資料の閲覧やアンケート等によって行う調査活動である。したがって**イ**が正解。

ア　監査報告書の作成における実施事項である。
ウ　本調査での実施事項である。
エ　本調査での実施事項である。

●問 23　正解：エ

ア　達成状況を評価し，必要に応じて改善策を検討するのは中間評価である。
イ　投資額や効果目標の変更が必要かどうかを検討するのは中間評価である。
ウ　投資効果の実現時期に合わせて行うのは事後評価である。
エ　効果目標を設定し，実施可否判断に必要な情報を提供するのは事前評価である。

したがってエが正解。

●問 24　正解：エ

SOA（Service Oriented Architecture：サービス指向アーキテクチャ）とは，ビジネスの構成要素とそれを支援する IT 基盤をソフトウェア部品である「サービス」として提供するシステムアーキテクチャである。「サービス」は，一つ又は複数のアプリケーションをコンポーネント化したものであり，外部から呼び出すためのインターフェイスをもっている必要がある。したがってエが正解。

ア　BPR（Business Process Reengineering）の説明である。
イ　ERP（Enterprise Resource Planning）パッケージの説明である。
ウ　SLA（Service Level Agreement）の説明である。

●問 25　正解：エ

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。

ア　**クラス図**は，モデル要素の属性，他のモデル要素との関連を記述するものであり，表の“a”に該当する。
イ　**コラボレーション図**は，オブジェクト間のメッセージ交換と相互作用を記述するものであり，表の“d”に該当する。
ウ　**ステートチャート図**は，オブジェクトの状態遷移を記述するものであり，表の“c”に該当する。
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記述するものであり，表の“b”に該当する。

したがってエが正解。

●問 26　正解：ア

チャレンジャ戦略（マーケットチャレンジャ戦略）とは，上位企業のシェアを奪うことを目標として，競争相手や攻撃戦略を明確にし，製品，サービス，販促等のあらゆる面で差別化を図ることである。したがってアが正解。

イ　ニッチ戦略の説明である。
ウ　フォロワー戦略の説明である。

エ　フルライン戦略の説明である。

●問 27　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される。

・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 28　正解：ウ

ア　既に一部利用しているツールの活用であるから，組織内からの技術的アプローチである“a”に相当する。
イ　外部の市場調査会社を活用しての消費者ニーズの調査であるから，組織外からの組織的アプローチである“d”に相当する。
ウ　組織内の部門の作業工程見直しによる作業の効率化であるから，組織内からの組織的アプローチである“b”に相当する。
エ　外部の組織との共同研究開発や技術導入であるから，組織外からの技術的アプローチである“c”に相当する。

したがって**ウ**が正解。

●問 29　正解：エ

在宅型テレワーカの数，短時間勤務を選択できる事業所の割合，男性の育児休業取得率などは，「多様な働き方・生き方が選択できる社会の実現に向けた指標」に該当する。したがって**エ**が正解。

一方，“a”の例は「就労による経済的自立が可能な社会の実現に向けた指標」，“b”の例は「健康で豊かな生活のための時間が確保できる社会の実現に向けた指標」に該当する。

●問 30　正解：ウ

個人情報の保護に関する法律（個人情報保護法）では，個人情報を，生存する個人に関する情報に限定している。したがって**ウ**が正解。