平成 26 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：エ

カルノー図は，論理式を簡単化するために論理変数の組合せの結果を表で表す方式である。

カルノー図から論理式を導くには，次のルールに従って表中のすべての「1」のセルを囲ってグルーピングする。

・グルーピングするセルの中がすべて「1」であること
・グルーピングするセルの数が 2 のべき乗であること
・カルノー図の上下の端，および左右の端は連続していると考える
・同じセルが複数のグループに含まれてもよい

これに従って問題文のカルノー図をグルーピングすると次のようになる。

CD / AB	00	01	11	10
00	1	0	0	1
01	0	1	1	0
11	0	1	1	0
10	0	0	0	0

続いて，各グループの中から共通変数を取り出し，その論理積を作る。

上のグループの論理式は（ $\overline{ABCD}$ ）と（ $\overline{AB}C\overline{D}$ ）であるため，共通変数は（ $\overline{ABD}$ ），その論理積は $\bar{A}\cdot\bar{B}\cdot\bar{D}$ となる。

一方，中央のグループの論理式は，（ $\bar{A}B\bar{C}D$),($\bar{A}BCD$),($AB\bar{C}D$),($ABCD$)であるため，共通変数は BD，その論理積は B・D となる。

そして，次のようにそれらの論理積の論理和をとることでカルノー図の論理式が導き出せる。

$\bar{A}\cdot\bar{B}\cdot\bar{D}$ ＋B・D

したがって**エ**が正解。

●問 2　正解：イ

M/M/1 の待ち行列における窓口の平均待ち時間は，平均サービス時間（1 件の伝票データの処理時間），窓口の利用率（ρ）により，次の公式で表される。

平均待ち時間 ＝ $\frac{\rho}{(1-\rho)}$ × 平均サービス時間

「1 件の伝票データの処理時間は，平均 T 秒の指数分布に従う」とあることから，平均サービス時間はTとなり，これが平均待ち時間T秒以上となる利用率は次の式で求められる。

$$\frac{\rho \times T}{(1-\rho)} \geqq T$$

$$\frac{\rho}{(1-\rho)} \geqq 1$$

$$\rho \geqq 1-\rho$$

$$2\rho \geqq 1$$

$$\rho \geqq 0.5$$

したがって**イ**が正解。

●問３　正解：イ

V4 への最短所要時間：V1 → V3 → V2 → V4（1 ＋ 1 ＋ 1 ＝ 3）
V5 への最短所要時間：V1 → V3 → V2 → V4 → V5（1 ＋ 1 ＋ 1 ＋ 2 ＝ 5）
V6 への最短所要時間：V1 → V3 → V2 → V4 → V6（1 ＋ 1 ＋ 1 ＋ 1 ＝ 4）

これらを所要時間の短い順に並べると，V4, V6, V5 となる。
したがって**イ**が正解。

●問４　正解：エ

ライトバック方式とは，キャッシュメモリにだけデータを書き込み，キャッシュメモリからデータが追い出されるときに主記憶の更新を行う。プロセッサから主記憶への書込み頻度を減らすことで，アクセスの高速化を図る技術である。したがって**エ**が正解。
一方**ライトスルー方式**では，キャッシュメモリと主記憶の両方に同時に書き込む。

ア　ライトスルー方式に関する記述である。
イ　ライトスルー方式に関する記述である。
ウ　ライトスルー方式と比較した場合，ライトバック方式の方が回路構成は複雑になる。

●問５　正解：エ

2 台のプリンタのうち，いずれか一方が稼働していて，他方が故障している確率を求めるには，2 台とも稼働している確率と，2 台とも故障している確率を求め，それらを全体（100%）から除けばよい。

まず，2 台とも稼働している確率は 2 台の稼働率の積となるため，次のようになる。

$0.7 \times 0.6 = 0.42$

続いて，2 台とも故障している確率は 2 台の非稼働率の積となるため，次のようになる。

$(1 - 0.7) \times (1 - 0.6) = 0.12$

これらの合計を全体から除くと次のようになる。

$1 - (0.42 + 0.12) = 0.46$

したがって**エ**が正解。

●問６　正解：エ

Linux に限らず，**カーネル**は OS の中核となる部分であり，プロセス管理やメモリ管理，ハードウェアの制御等を行う。したがって**エ**が正解。

●問７　正解：ウ

左側が論理積，右側が否定を表すため，図の論理回路を論理式で表すと次のようになる。

X = ($\overline{S\ AND\ Y}$) , Y = ($\overline{R\ AND\ X}$)

S = 1, R = 1, X = 0, Y = 1 のとき，S をいったん 0 にすると，次のようになる。

X = ($\overline{0\ AND\ 1}$) = 1 , Y = ($\overline{1\ AND\ 1}$) = 0

続いて，S を再び 1 に戻すと，次のようになる。
X = ($\overline{1\ AND\ 0}$) = 1 , Y = ($\overline{1\ AND\ 1}$) = 0

したがって**ウ**が正解。

●問８　正解：ア

新規顧客が毎年 2 割ずつ増えていくので，3 年後の顧客総数は次のようになる。

8,000 × 1.2 × 1.2 × 1.2 ＝ 13,824

一方，A～Z の英大文字を用いた顧客コードは，3 桁（26^3）で 17,576 種類となる。
したがって**ア**が正解。

●問 9　正解：ウ

A が決まると B が特定され，C が決まると D と E が特定される。また，A と C が決まると F が特定される。

つまり，A と C が決まれば，関係 R（A,B,C,D,E,F）を特定できることになるため，候補キーは{A,C}である。したがって**ウ**が正解。

●問 10　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として，**TCP**（Transmission Control Protocol）と **UDP**（User Datagram Protocol）がある。UDP はコネクションレスのデータグラム通信を行うプロトコルであり，TCP は信頼性のための確認応答や順序制御などの機能をもつプロトコルである。したがって**エ**が正解。

ア　**ICMP**（Internet Control Message Protocol）は，IP 通信において発生したエラー関連の情報や制御メッセージを通知するためのプロトコルである。
イ　**PPP**（Point to Point Protocol）は，2 点間のデータ通信に用いるデータリンク層のネットワークプロトコルである。

●問 11　正解：イ

255.255.252.0 のサブネットマスクは 2 進数では次のようになる。

11111111.11111111.11111100.00000000

第 3 オクテットでは，上位 6 ビットがネットワークアドレスとして用いられるので，サブネットワークアドレスの第 3 オクテットの値は，すべて末尾 2 ビットが"00"となるものとなる。具体的には，次のように，最小値 : 0，最大値 : 252，最小値と最大値の間はすべて 4 の倍数となる。

第 3 オクテットの値	サブネットワークアドレス	属する IP アドレスの範囲
00000000	x.x.0.0	x.x.0.1 ～ x.x.3.254
00000100	x.x.4.0	x.x.4.1 ～ x.x.7.254
00001000	x.x.8.0	x.x.8.1 ～ x.x.11.254
00001100	x.x.12.0	x.x.12.1 ～ x.x.15.254
:	:	: :
01111000	x.x.120.0	x.x.120.1 ～ x.x.123.254

01111100	x.x.124.0	x.x.124.1 ～ x.x.127.254
:	:	: :
11111100	x.x.252.0	x.x.252.1 ～ x.x.255.254

上記より，IP アドレスが 172.30.123.45 のホストが属するサブネットワークのアドレスは 172.30.120.0 となる。したがって**イ**が正解。

●問 12　正解：ア

SMTP-AUTH は, SMTP にユーザ認証機能を追加した方式であり, クライアントが SMTP サーバにアクセスしたときに利用者認証を行うことで，許可された利用者だけから電子メールの送信を受け付ける。したがって**ア**が正解。

イ　SSL/TLS におけるクライアント認証の説明である。
ウ　POP before SMTP の説明である。
エ　APOP の説明である。

●問 13　正解：ウ

DNS キャッシュポイズニング（汚染）とは，DNS サーバからの名前解決要求に対し，正常な応答に加えて悪意あるサイトに誘導するための不正な名前解決情報も付加して返すことで，当該 DNS サーバのキャッシュに（不正な名前解決情報を）登録させる攻撃である。このようにしてキャッシュが汚染されてしまうと，社内の利用者がインターネット上の Web サーバ等を参照する場合に，本来とは異なるサーバに誘導される可能性がある。したがって**ウ**が正解。

●問 14　正解：イ

ア　**OS コマンドインジェクション**を防ぐには，OS コマンドの呼出しが可能な関数を極力使用せず, 外部からの入力データに OS コマンドとして使用可能な文字列が含まれていないかをチェックするのが有効である。
イ　適切な対策である。
ウ　**クロスサイトスクリプティング**を防ぐには，外部からの入力データに"<", ">", "&"などのメタキャラクタが存在しないかをチェックし，存在した場合にはエスケープ処理を行うのが有効である。
エ　**セッションハイジャック**を防ぐためには，Web アプリケーションが発行するセッション ID を推測困難なものにするのが有効である。

●問 15　正解：ア

WPA（Wi-Fi Protected Access）は無線 LAN のセキュリティを強化することを目的とした技術であり，無線 LAN の業界団体である Wi-Fi Alliance が 2002 年 10 月に発表した。**WPA2** は WPA の後継となる規格であり, Wi-Fi Alliance が 2004 年 9 月に発表した。WPA2

では暗号化アルゴリズムに **AES**（Advanced Encryption Standard）を採用した CCMP を使用する。したがって**ア**が正解。

●問 16　正解：イ

ソフトウェア開発における代表的なテスト手法として，**ブラックボックステスト**とホワイトボックステストがある。ブラックボックステストとは，プログラムの外部仕様（入出力仕様）に基づいてテストを行う手法であり，同値クラスや限界値を識別し，テストデータを作成する。一方ホワイトボックステストは，プログラムの内部仕様に基づいてテストを行う手法であり，分岐条件に基づいたテストデータを作成し，ロジックを検証する。したがって**イ**が正解。

●問 17　正解：ア

著作権法の第 15 条第 2 項（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委託先に帰属することになり，委託元で開発する別のソフトウェアに適用できなくなる。したがって**ア**が正解。

●問 18　正解：ウ

ITIL における構成管理とは，IT サービスの構成アイテム（Configuration Item：CI）を正しく認識し，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。CI には，機器やソフトウェアの情報のみでなく，IT サービスの提供に必要な規程，手順書，設備等も含まれる。ソフトウェア開発プロジェクトで行う構成管理においては，個々のプログラムのバージョン情報等が対象項目となる。したがって**ウ**が正解。

●問 19　正解：ウ

ファストトラッキングとは，本来の計画では順番に実施する予定だった作業を，前工程の終了を待たずに並行して実施することで期間短縮を図る手法である。例えば，全体の設計が完了する前に，仕様が固まっているモジュールの開発を開始することなどがこれに該当する。したがって**ウ**が正解。

●問 20　正解：ア

SLA（Service Level Agreement）とは，サービスの提供者と顧客との間の契約における，サービス及びサービス目標値に関する合意である。ISP（Internet Services Provider）や IDC（Internet Data Center）が，回線の最低通信速度やネットワーク内の平均遅延時間，利用不能時間の上限など，サービス品質の保証項目や，それらを実現できなかった場合の利用料金の減額に関する規定などをサービス契約に含めているのが一般的である。したがっ

てアが正解。

●問 21　正解：ウ

目標復旧時点（Recovery Point Objective：**RPO**）とは，業務中断からさかのぼって，いつの時点の状態まで戻すのかを示す指標である。これに対し，目標復旧時間（Recovery Time Objective：RTO）とは，業務中断後，いつまでに業務を復旧させるのかを示す指標である。解答群のア，イ，エはいずれも RTO であり，RPO に該当するのは**ウ**である。

●問 22　正解：エ

在庫データの網羅性を確保するためには，在庫データに抜け漏れや重複がなく，すべ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：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，の四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。したがって**ウ**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

「**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（平成 19 年 1 月実施）を集約し，提示したものである。

本書では，「モデル契約書雛形における個別業務と契約類型」として，次のように「システム方式設計（システム内部設計）」から「システム結合」までのフェーズについては請負型の契約が適切としている。したがって**エ**が正解。

<table>
<tr><th>共通フレーム
（基本プロセス群）</th><th>取引・契約モデルにおける
フェーズ分け</th><th colspan="2">モデル契約書雛形における
個別業務と契約類型</th></tr>
<tr><td>1.4 企画プロセス</td><td>システム化の方向性
システム化計画</td><td colspan="2">（対象外）</td></tr>
<tr><td>1.5 要件定義プロセス</td><td>要件定義</td><td rowspan="6">ソフトウェア開発委託基本モデル契約書</td><td>要件定義作成支援業務
【準委任型】</td></tr>
<tr><td rowspan="5">1.6 開発プロセス</td><td>システム設計（システム外部設計）</td><td>外部設計書作成（支援）業務
【準委任型】【請負型】の選択</td></tr>
<tr><td>システム方式設計（システム内部設計）
ソフトウェア設計
プログラミング
ソフトウェアテスト
システム統合</td><td>ソフトウェア開発業務
*ハードウェア等の調達の留意点は別途整理。
【請負型】</td></tr>
<tr><td>システムテスト</td><td>【準委任型】【請負型】の選択</td></tr>
<tr><td>導入・受入支援</td><td rowspan="2">ソフトウェア運用準備・移行支援業務
【準委任型】</td></tr>
<tr><td rowspan="2">1.7 運用プロセス</td><td>運用テスト</td></tr>
<tr><td>運用</td><td>情報システム保守運用委託基本モデル契約書</td><td>システム運用業務
システム保守業務</td></tr>
<tr><td>1.8 保守プロセス</td><td>保守</td><td colspan="2"></td></tr>
</table>

出典：経済産業省「情報システム・モデル取引・契約書＜第一版＞」

http://www.meti.go.jp/policy/it_policy/keiyaku/model_keiyakusyo.pdf

●問 26　正解：エ

問題文は**SCM**（Supply Chain Management）についての説明である。したがって**エ**が正解。

ア　**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マーケティング活動に反映させる手法。既存の顧客をマーケティング対象の中心に考えた手法であり，新規顧客獲得に重点を置いたものではない。

イ　**ERP**（Enterprise Resource Planning）とは，管理業務，生産業務，営業，販売業務，商品調達，研究開発など企業活動の様々な業務における経営資源を統合的に管理し，経営の効率化を図るための手法。この手法を実現するための統合的なソフトウェアは ERP パッケージと呼ばれている。

ウ　**MRP**（Material Resource Planning）とは，予想される需要によって発注量と発注時期をコントロールすることで在庫の圧縮と不足の解消を同時に実現する生産管理手法。

●問 27　正解：イ

コア技術とは，競合他社との競争において優位に立つための核となるものであり，他社が容易に真似できないような技術のことである。したがって**イ**が正解。

●問 28　正解：エ

CE（コンカレントエンジニアリング）とは，製品の企画から製造までの工程を同時並行で進めることにより，作業を効率化し，全体のリードタイムを短縮する手法である。したがって**エ**が正解。

ア　CAM（Computer Aided Manufacturing）の説明である。
イ　POP（Point of Production）の説明である。
ウ　PDM（Product Data Management）の説明である。

●問 29　正解：エ

問題文に該当するのは連関図であり，**エ**が正解。

ア　**アローダイアグラム**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図である。
イ　**パレート図**は，測定値データの項目別出現頻度を求め，度数の高い順に並べ替えたグラフであり，データ項目の重点ポイントを探る際に用いられる。
ウ　**マトリックス図**は，表の縦軸と横軸に複数の項目を置き，それらの交点に"○"，"×"等を表記することで，各項目間の関連性や関係等を表した図である。

●問 30　正解：ウ

企業の顧客情報や技術的なノウハウ等は，次に示す要件を満たすことで，「営業秘密」として不正競争防止法によって保護される。

＜情報が「営業秘密」として扱われるための要件＞
・秘密として管理されていること（秘密性）
・事業活動に有用な技術上又は営業上の情報であること（有用性）
・公然と知られていないこと（非公知性）

したがって**ウ**が正解。