

●平成 30 年度秋期

午前問題 解答・解説

問 1 エ

16 進小数の 10 進分数変換 (H30 秋・FE 問 1)

16 進数の小数 $0.x_1x_2x_3 \dots$ ($x_1x_2x_3 \dots$ は 16 進数の 0~F, 10 進数で 0 から 15 を表す数) について, 小数第 1 位 x_1 , 小数第 2 位 x_2 , 小数第 3 位 x_3 は, それぞれ, 10 進数で言うところの 16 分の 1 の位, 16^2 分の 1 の位, 16^3 分の 1 の位の値である。

$$\begin{aligned} \text{したがって, } (0.248)_{16} &= 2 \times \frac{1}{16^1} + 4 \times \frac{1}{16^2} + 8 \times \frac{1}{16^3} \\ &= \frac{2}{16} + \frac{4}{256} + \frac{8}{4,096} \\ &= \frac{1}{8} + \frac{1}{64} + \frac{1}{512} = \frac{73}{512} \end{aligned}$$

と計算することができる。したがって, 答えは (エ) となる。

問 2 ウ

ビット操作のアルゴリズムに入る論理演算 (H30 秋・FE 問 2)

与えられたビット列 00101000 に対して, 最も右にある 1 を残し, 他のビットを全て 0 にした 00001000 を, 手順 1~3 のアルゴリズムに従って求める。そのとき, 手順 3 で必要な論理演算を考える。

①手順 1

$$\begin{array}{r} 00101000 \text{ (A)} \\ -) \quad 00000001 \\ \hline 00100111 \text{ (B)} \end{array}$$

②手順 2

$$\begin{array}{r} 00101000 \text{ (A)} \\ \text{XOR) } 00100111 \text{ (B)} \\ \hline 00001111 \text{ (C)} \end{array}$$

結果として, 最も右にある 1 を残し, 他のビットを全て 0 にした 00001000 を得るためには, A (00101000) と C (00001111) の論理積 (AND) を求めればよい。したがって, 空欄 a に入る論理演算は, (ウ) 論理積 (AND) である。

③手順 3

$$\begin{array}{r} 00101000 \text{ (A)} \\ \text{AND) } 00001111 \text{ (C)} \\ \hline 00001000 \end{array}$$

AI (Artificial Intelligence ; 人工知能) は提唱者であるジョン・マッカーシーによると「知的な機械、特に、知的なコンピュータプログラムを作る科学と技術」とされている。人間の判断・識別・予測・作文などの知的活動をコンピュータによって実現するものである。機械学習はAIの歴史の中では2000年代から続いており、IoT (Internet of Things) の利用やSNSの情報などから数値、テキスト、画像、音声など多量のデータ (ビッグデータ) を用いることでAI自体が人間のように学習し、特定のパターン、ルールや知識を見つけ出すことである。したがって、(ア) が最も適切である。

イ：人工生命の説明である。コンピュータ上の仮想生命システムやロボットなどの機械を使って生命をシミュレーションすることで、生命現象や進化のプロセスを再現する。

ウ：エキスパートシステムの説明である。特定分野の専門家の知識 (規則や事例) を蓄積する知識ベースと、知識ベースを使用して推論し問題解決や処理を行う推論エンジンから構成される。医師の知識・経験から診断をする例などがある。

エ：適応学習 (アダプティブラーニング) の説明である。Webシステムを用いて自主学習を行うeラーニングの一種である。AIなどの技術を使用して、コンピュータが学習者個人の習熟度に応じて教材を提供し、進度などの管理を行う。学校教育や企業の人材育成での利用が始められている。

問4 エ

ハフマン符号化の符号表に入る符号 (H30 秋・FE 問4)

ハフマン符号化 (Huffman coding) は、1952年にDavid Huffmanによって提案された符号化方式で、文字列などの可逆圧縮に用いられる。出現頻度が高い文字には短いビット列を、出現頻度が低い文字には長いビット列を割り当て、メッセージ全体の符号化に使われるデータ量を削減することができる。JPEG、ZIPなどで使われている。

文字列を可変長のビット列 (符号) に対応させる場合、1文字分のビット列を受け取ったときに、復号するには、任意の文字に対応するビット列が、別の文字に対応するビット列の頭から何ビットか切り出した語頭とは一致しないことが条件となる。そのことを念頭に、各選択肢を見ていく。

A	B	C	D	E
00	01	10	xxx	111



001	⇒ A (00) と重なる。
010	⇒ B (01) と重なる。
101	⇒ C (10) と重なる。
110	⇒ どれとも重ならない。

ア：001 は、A (00) と語頭 2 ビットが一致しており、該当しない。

イ：010 は、B (01) と語頭 2 ビットが一致しており、該当しない。

ウ：101 は、C (10) と語頭 2 ビットが一致しており、該当しない。

エ：110 は、A, B, C, E (111) のどのビット列とも語頭が一致しておらず、この (エ) が適切となる。

本問では、A, B, C, D, E という 5 文字で構成されており、それぞれの文字を固定長のビット列で表す場合は、3 ビット ($2^2=4<5<2^3=8$) が必要となる。例えば、次のように 3 ビットを割り当てる。これを固定長符号という。

A: 000

B: 001

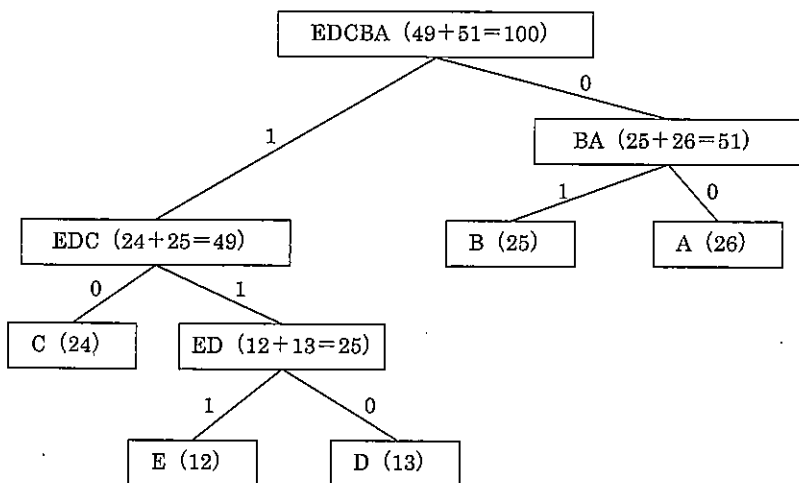
C: 010

D: 011

E: 100

ハフマン符号化では、各文字の出現頻度を基に、次のようにハフマン木 (2 分木) という木構造を作って符号を割り当てる。ここで各文字の後ろの括弧内の数値を出現頻度とする。

- ① 出現頻度の低い順に二つを木の葉にする。この場合は、E (12) と D (13) の二つが選ばれる。次に二つの葉を枝で結び接点を作る。
 - ② 既に関連 E, D は除いて、E と D の接点 ED (25) と残った A (26), B (25), C (24) から低い順に二つを選ぶ。接点 ED (25) と B (25) は同じ頻度であるからどちらを先に選んでもよい。C (24) と接点 ED (25) を選ぶ。
 - ③ A (26), B (25), 接点 EDC (49) から低い順に二つを選ぶ。A (26), B (25) が選ばれる。
 - ④ 接点 EDC (49) と接点 BA (51) を結ぶと完成である。
 - ⑤ 2 分木の枝には、左右に 0, 1 を割り振る。0, 1 は左右どちらでもよい。
 - ⑥ 枝に割り振った 0, 1 を上から順番に文字まで読むとハフマン符合になる。
- 例えば、A は 00, D は 110 となる。

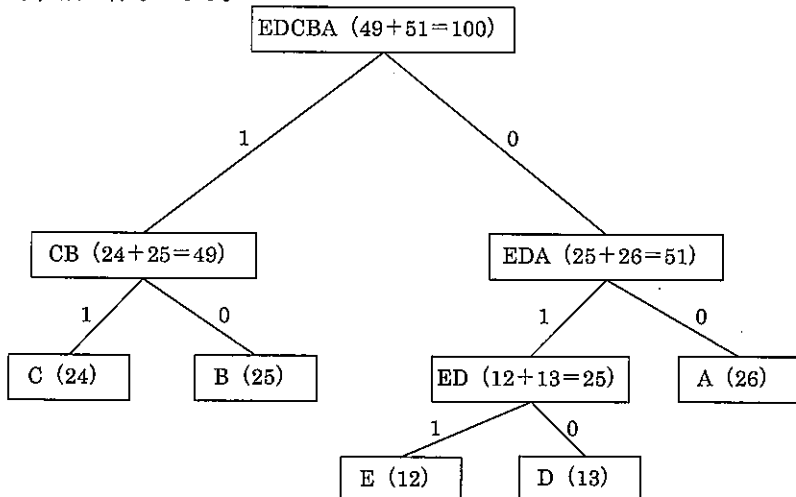


※カッコ内は出現頻度

念のために、出現頻度を基に A, B, C, D, E のハフマン符号を用いた場合の平均長を計算すると次のようになり、ハフマン符号の方が固定長 3 ビットより短くなっていることが分かる。

ハフマン符号： $2 \times 0.26 + 2 \times 0.25 + 2 \times 0.24 + 3 \times 0.13 + 3 \times 0.12 = 2.25$ ビット
 < 3 ビット

②で B の代わりに接点 ED (25) を選んだが、B (25) を選ぶと次のようになり、別の符号となる。



問5 ウ

待ち行列へのデータ入力と取出し (H30 秋・FE 問 5)

待ち行列は、FIFO (First In First Out) のデータ構造で、先に待ち行列に挿入 (ENQ) されたデータから順に取り出される (DEQ) ことになる。

① ENQ 1	待ち行列に 1 が挿入される。
② ENQ 2	待ち行列に 2 が挿入される。待ち行列の内容は、1・2 である。
③ ENQ 3	待ち行列に 3 が挿入される。待ち行列の内容は、1・2・3 である。
④ DEQ	待ち行列から 1 が取り出される。待ち行列の内容は、2・3 である。
⑤ ENQ 4	待ち行列に 4 が挿入される。待ち行列の内容は、2・3・4 である。
⑥ ENQ 5	待ち行列に 5 が挿入される。待ち行列の内容は、2・3・4・5 である。
⑦ DEQ	待ち行列から 2 が取り出される。待ち行列の内容は、3・4・5 である。
⑧ ENQ 6	待ち行列に 6 が挿入される。待ち行列の内容は、3・4・5・6 である。
⑨ DEQ	待ち行列から 3 が取り出される。待ち行列の内容は、4・5・6 である。
⑩ DEQ	待ち行列から 4 が取り出される。待ち行列の内容は、5・6 である。

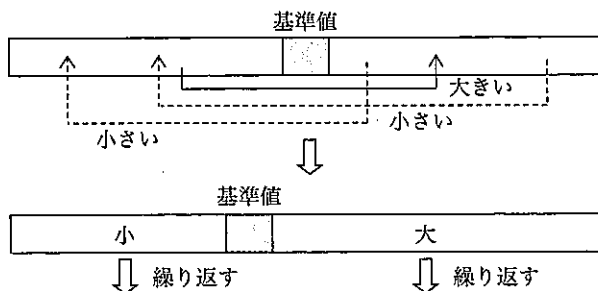
以上の操作から、待ち行列の内容は 5 と 6 になっており、次の DEQ で取り出される値は 5 となる。したがって、(ウ) が正解である。

ただし、FIFO の場合、スタック構造とは違い、待ち行列中の要素数以上の DEQ が続いているかという条件をチェックさえすれば、より単純に考えることができる。本問の場合、ENQ1~ENQ6 の順に六つの要素が挿入され、DEQ は 4 回行われ、次の 5 回目の DEQ が問題となっている。FIFO なので、5 番目に ENQ されたデータが取り出されるので、“5” であることが分かる。

問6 ウ

クイックソートの処理方法 (H30 秋・FE 問 6)

クイックソートの基本的な考え方は、基準値 (ピボットという) を選んで、データをそれより値の大きいグループと小さいグループの二つに分割して、それぞれのグループごとに、同じ操作を再帰的に繰り返していくものである。



- その名のとおり、高速な整列方法で、(ウ)がクイックソートの説明である。
- ア：既に整列済みのデータ列にデータを追加するということから、挿入法に関する記述である。
- イ：データ中の最小値を求めていくことから、選択法（最小値選択法）に関する記述である。最大値を求めていく方法は最大値選択法と呼ばれる。
- エ：隣り合ったデータの比較を繰り返し、小さな値のデータを端の方に移していくのは交換法である。バブルソートとも呼ばれる。

問7 エ

プログラムのコーディング規約に規定する事項 (H30 秋・FE 問7)

コーディング規約は、プログラムコードの書き方に関する決まり事で、標準化してまとめておくことによって、チームで開発する場合や、開発後もソフトウェアの保守を行う上で担当者の変更にも対応しやすくなる。したがって、生産性の向上、品質の安定化に貢献する。

領域割付け関数はプログラム実行時に動的に記憶域を確保する関数であり、割付けができなかった場合は処理が中断するため、割付けができなかったときのエラー処理は決めておく必要がある。したがって、(エ)が適切である。

ア：プログラムの一部で使われる局所変数は、用途が異なる場合は分かりやすくするためにデータ型が同じでも別の変数を使う方がよい。

イ：処理性能を向上させるためには、浮動小数点型変数を使用するより整数型変数を使用する方が命令実行性能がよい。

ウ：関数の再帰呼出しとは、関数の中からさらに自分自身の関数を呼び出す処理である。再帰処理の場合は、呼び出されるたびに新たに呼び出された関数用にメモリ領域が動的に確保され、戻るときには解放を繰り返すため、メモリの使用や実行の効率が悪くなる。同様の計算を何度も繰り返すときは関数の再帰呼出しではなく繰返し処理を使用する。

問8 エ

Java の特徴 (H30 秋・FE 問8)

C 言語や C++ 言語では、プログラムがメモリ領域を確保した場合、そのプログラムの責任で使わなくなったメモリ領域を解放しなくてはならない。しかし、Java ではメモリの状況を常に監視し、利用されなくなったメモリ領域を自動的に整理して空き領域にまとめる機能がある。この機能をガーベジコレクション (garbage collection) と呼ぶ。したがって、(エ) の説明が適切である。

ア：オブジェクト指向言語で複数のスーパークラスから継承を行うことを多重継承と呼ぶ。C++ 言語では多重継承がサポートされているが、Java では多重継承はサポートされていない。

イ：共通する変数とメソッドをもつオブジェクトをまとめ、その特徴を記述したものがクラスである。一方、基本データ型は変数の属性を表すものなので、クラスとして扱うことができない。整数を表す int と、文字を表す char は、Java における基本データ型なので、クラスではない。

ウ：C 言語の変数の型のうち、ポインタ、構造体、共用体の三つの型は、Java ではサポートされていない。

問9 エ

CPU の性能計算 (H30 秋・FE 問9)

コンピュータで実行される命令は、命令の種類によって実行時間が異なるため、命令実行時間は基本動作時間 (クロック時間、クロック周波数の逆数) の何倍かで示されることが多い。問題には、命令の種類ごとに命令実行に必要なクロック数と出現率が示されているので、それを掛け合わせて合計することで、平均命令クロックサイクル数 (クロック/命令) が得られる。

命令の種類	命令実行に必要なクロック数	出現率 (%)
レジスタ間演算	4	30
メモリ・レジスタ間演算	8	60
無条件分岐	10	10

$$\begin{aligned}\text{平均命令クロックサイクル数} &= 4 \times 0.3 + 8 \times 0.6 + 10 \times 0.1 \\ &= 1.2 + 4.8 + 1 = 7 \text{ (クロック/命令)}\end{aligned}$$

クロック周波数が 700MHz の CPU は 1 秒間に 700×100 万クロック発生する。また、MIPS は 1 秒あたりに実行できる命令数を百万単位で表した値である。

1 命令につき 7 クロックサイクルかかるとすると、1 秒間に実行できる命令は、次のようになる。

$$\begin{aligned}&700 \times 1,000,000 \text{ (クロック/秒)} \div 7 \text{ (クロック/命令)} \\ &= 100 \times 1,000,000 \text{ (命令/秒)} = 100\text{MIPS}\end{aligned}$$

よって、求める MIPS 値は (エ) の 100 となる。

問 10 ウ

割込み発生時にプロセッサが保存するもの (H30 秋・FE 問 10)

割込み処理はプログラムの実行中に OS やハードウェア、プログラム自身からの要求によって処理を中断して行う処理である。中断したプログラムは割込み処理終了後いつでも再開できるように、プログラムカウンタ (命令アドレスレジスタ)、汎用レジスタ、命令実行結果の情報などの割込み時のプログラム状況を退避させておく必要がある。プログラムが次に実行する命令のアドレスを記憶するレジスタはプログラムカウンタである。したがって、(ウ) プログラムカウンタが正解である。参考までに、プログラムカウンタ、汎用レジスタの内容などを、タスクのコンテキストという。

ア：インデックスレジスタ (指標レジスタ) は、データのアドレスを示すときに基準となるアドレスに定数を増減するためのレジスタである。汎用レジスタをインデックスレジスタとして利用する場合が多い。

イ：データレジスタは命令を実行するときに必要なメモリから読み込んだデータを格納、又はメモリに書き込むデータを格納しているレジスタである。

エ：命令レジスタはメモリから読み込んだ命令そのものを一時的に保持しているレジスタである。

問 11 ウ

ECC を利用したエラー検出に必要な冗長ビットの数 (H30 秋・FE 問 11)

ECC (Error Correcting Code 又は Error Check and Correct) とは、エラー検出と訂正を行うための仕組みである。データバス幅 2^n ビットに対して $n+2$ ビットの冗長ビットが必要なので、まず 128 ビットを 2^n ビットの形式に変換する。 $128=2^7$ なので、 n は 7 となる。よって、必要な冗長ビットの数は、 $7+2=9$ ビットとなり、(ウ) が正解である。

問 12 エ

USB3.0 の説明 (H30 秋・FE 問 12)

USB 3.0 は、USB 2.0 の最大転送速度 480M ビット/秒に対して、スーパースピードと呼ばれる 5G ビット/秒を実現したものである。したがって、(エ) が正解である。その他、従来の USB 2.0 との違いは、USB 2.0 の四つの転送モード (注) (コントロール転送、インタラプト転送、アイソクロナス転送、バルク転送) に加えて、バルクストリーム転送と呼ばれるバルク転送より更に大容量の転送モードがある。また、給電容量が、USB 2.0 の最大 500mA から 900mA に増加している。

ア：LAN の規格 IEEE 802.3ab として標準化されている 1000BASE-T の説明である。カテゴリ 5e 以上の UTP ケーブル内の 4 対 8 線のより対線を使用し、各対に 250M ビット/秒の性能をもたせている。

イ：シリアル ATA (SATA) の説明である。従来のパラレル ATA をシリアル化す

ることによって、高速転送を可能にしたものであり、現在では、パラレル ATA、SCSI（スカジー）に代わるコンピュータにハードディスク、SSD や光学ドライブを接続する主流のインタフェース規格である。

ウ：IEEE1394 シリアルインタフェースの説明で、アップル社が提唱した FireWire 規格を標準化したものである。主としてビデオ・オーディオ分野で使われてきた。i.LINK、DV 端子などの別の名称が使われることもある。

(注)・コントロール転送モード…USB デバイスの初期情報の転送などに用いられる。

- ・インタラプト転送…デバイスからホストへ周期的にデータを転送する場合に用いられる。
- ・アイソクロナス転送…音声データやリアルタイム性を要求される場合に用いられる。
- ・バルク転送…大量のデータを転送する場合に用いられる。

問 13 エ

Web サーバと AP サーバを異なる物理サーバに配置するメリット (H30 秋・FE 問 13)

Web システムにおいては、Web サーバとアプリケーション (AP) サーバを異なる物理サーバに配置する構成にすることがある。この目的は Web サーバと AP サーバの役割を分離し処理にかかる負荷を分散することによって多くのリクエストを効率よく処理することである。Web サーバは主にクライアントとの通信を受け持ち、クライアントからのリクエストやデータを受け取って AP サーバに渡し、AP サーバの処理結果をクライアントに返す役割を果たす。静的コンテンツはリクエスト内容によらず常に同じ内容を返すコンテンツであり、動的コンテンツはクライアントから送られるパラメタの内容によって処理を実行しリクエストごとに異なる結果を返すコンテンツである。負荷が軽い静的なコンテンツへのリクエストについては Web サーバだけで処理を行い、負荷が重い動的コンテンツへのリクエストは AP サーバで処理を行う。したがって、(エ) が適切である。

ア：Web サーバにクライアントの実行環境は実装されていないため、クライアントと AP サーバの間で画面データのやり取りは必要である。

イ：Web サーバは AP サーバが生成した HTML の受渡しを行うだけでコード変換は行わない。コード体系はアプリケーション側で決定する必要がある。

ウ：データへのアクセスを伴う業務ロジックは AP サーバのプログラムに実装されるため、業務ロジックの変更に伴って AP サーバのプログラムを変更する必要がある。

問 14 イ

キャパシティプランニングの作業項目の順序 (H30 秋・FE 問 14)

キャパシティプランニングとは、情報システムの開発、改修を行う際に、システムに求められるサービスを分析し、必要となる資源の能力や数を見積もり、最適なシステム構成を計画することである。具体的な手順としては、まず、トランザクション数、応答時間、CPU 使用率、メモリ使用率、ディスク使用量、ネットワーク使用率といったシステムやシステム資源の稼働状況から性能状況やシステム固有の環境を把握する。利用者などに新規業務をヒアリングし、想定される処理件数や時間といったシステムに求められる要件を把握する。要件を満たすために、サーバの台数、並列分散処理の実施の有無など、必要なシステム構成の案を検討する。その後、システム構成の案に則って資源を増設し、決定した構成が適正なものかどうかを評価、必要があれば見直しを行うというサイクルを継続して行う。これに①～④の作業項目を当てはめると、最初に③の現状把握、次に④のシステムに求められる要件の把握、その後②の必要なシステム構成案の検討、最後に①のシステム構成案が適正かどうかの評価となる。したがって、(イ)が正解である。

問 15 ウ

迂回回線を追加したネットワークの稼働率 (H30 秋・FE 問 15)

東京～大阪～福岡の迂回回線は直列型なので、その稼働率 (A_1 とする) は各回線の稼働率を掛けることで求めることができ、次のようになる。

$$A_1 = 0.9 \times 0.9 = 0.81$$

東京～福岡の稼働率 (A_2 とする) は、 $A_2 = 0.9$ である。

東京～福岡の全体の稼働率を A とすると、 A_1 と A_2 の並列接続になるので、両方が故障する確率を 1 から引いて、求める。

$$A = 1 - (1 - A_1)(1 - A_2) = 1 - (1 - 0.81)(1 - 0.9) = 1 - 0.019 = 0.981$$

したがって、(ウ)が正解である。

問 16 イ

CPU 遊休時間の計算 (H30 秋・FE 問 16)

三つのタスク高、中、低について、CPU と I/O の専有状況のタイムチャートを次の図のように書いていく。CPU が使われていない時間の合計が、求める遊休時間 (アイドルタイム) である。CPU は 1 個であり、1CPU は 1 コアで構成され、CPU の実行は同時に一つであるが、I/O は競合しないので、I/O 動作の並列実行は自由に行えると考え。ここでは CPU の優先度だけを考慮して、CPU の実行が重ならないように、高い優先度のタスクから順番に CPU(3)→I/O(5)→CPU(2)→……の順番に記入していけばよい。結果は、7, 8 ミリ秒目と 11 ミリ秒目で CPU の遊休時間がある。したがって、(イ)の 3 ミリ秒が正解である。

	1	2	3	4	5	6	7	8	9	10	11	12	13	14
高														
中														
低														

凡例

— CPU を使用

--- I/O 動作

... CPU 空き待ち

午前解答

問 17 ウ

スプーリング機能の説明 (H30 秋・FE 問 17)

スプーリング (Simultaneous Peripheral Operation On-Line ; スプール) 機能とは、スプール領域を使った入出力のことである。スプール領域とは、低速な機器の入出力動作から CPU を解放するためのバッファの役目をもつ補助記憶装置の記憶領域のことである。例えば、プリンタへの出力データをいったん高速の磁気ディスク装置 (スプール領域) に格納しておき、その後に出力データを目的のプリンタに出力する。こうすることによって、プログラムはデータをスプール領域に出力した時点で終了でき、他の処理を開始することができる。プリンタなどの低速な入出力機器からプログラムを早く切り離すことで、並行実行できるプログラムが増え、低速な入出力機器と CPU を有効利用でき、システム全体のスループット (システム全体の処理能力) が向上する。したがって、(ウ) が適切である。

ア：タスクのスケジューリングに関する記述である。

イ：割込みに関する記述である。

エ：ディスクアクセス時に用いられるバッファリングに関する記述である。ディスクキャッシュも同等の機能を実現する。

問 18 ア

ラウンドロビン方式のタスクスケジューリング (H30 秋・FE 問 18)

ラウンドロビンとは、マルチプログラミングにおいてタスクを一定時間 (クォンタム) だけ実行させ、一定時間が過ぎれば、そのタスクの実行を中断し、同一優先順位の待ち行列の先頭のタスクに切り替えて実行する方式である。このとき、実行を中断されたタスクはその待ち行列の最後に回される。

したがって、(ア) の「各タスクに、均等に CPU 時間を割り当てて実行させる方式である」という記述は適切である。

イ：タスクのターンアラウンドタイム（処理時間）は予想できないので、基本的にこのようなスケジューリングは行われない。ジョブという単位であれば、パラメタとしてユーザが指定した実行時間を基に、処理時間が短いジョブの実行を優先する SJF（Shortest Job First；処理時間順）というスケジューリング方式がある。

ウ：「各タスクの実行イベント発生に応じて」という記述から、イベントドリブンスケジューリングのことを指しているといえる。

エ：マルチプログラミングにおける基本的なスケジューリング方式である、優先度スケジューリングの説明である。

問 19 エ

手続型言語のコンパイラが行う最初の処理 (H30 秋・FE 問 19)

手続型言語のコンパイラが行う処理は、次のような順番で行われる。

① 字句解析

ソースプログラムのファイルに記載された文字列から字句（英文でいうところの単語に当たる部分）を見つけ、切り分ける。予約語とは、言語ごとにあらかじめ決まっている文字列のことである。

② 構文解析

切り分けた字句それぞれを、変数、予約語、定数、記号、改行文字と判別するとともに複数の字句から成る構文として成立しているかどうかを解析する。算術式の構造も調べる。

③ 意味解析

それぞれの字句が相互に正しい関係になっているかを調べる。例えば、算術式の場合には、数値を扱うデータ型の変数、定数、算術記号、カッコだけが使われているかなどを調べる。

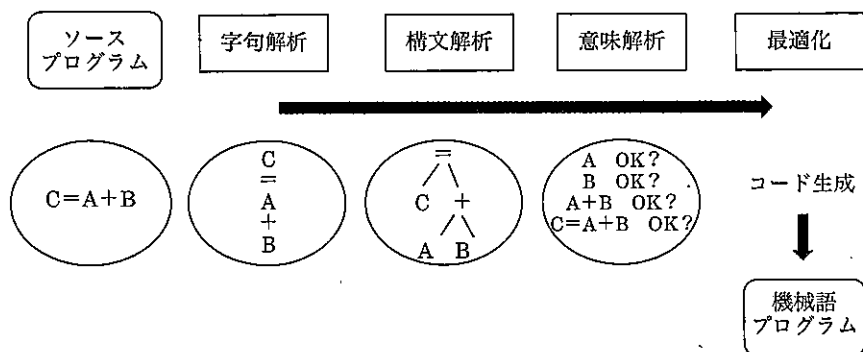
④ 最適化

目的プログラムの実行時間や大きさが小さくなるように、プログラムを変更する。例えば、式を簡略化したり、定数をあらかじめ計算したりしておく。

⑤ コード生成

機械後の目的プログラムを生成する。

上記から、最初に行う処理は、(エ) の字句解析となる。



午前解答

問 20 ウ

リンカの機能 (H30 秋・FE 問 20)

リンカは、リンケージエディタ、連係編集プログラムともいう。アセンブラやコンパイラが原始プログラムを翻訳して作った幾つかの目的プログラム（オブジェクトモジュール）を結合して、実行形式プログラム（ロードモジュール）を作る（連係編集する）プログラムである。したがって、(ウ) が適切である。

ア：ライブラリプログラム（ライブラリアン）に関する記述である。

イ：プログラムを実行させるために、主記憶に読み込む役割のロードに関する記述である。

エ：トレサ（追跡プログラム）に関する記述である。プログラムのデバッグの際に、どこの命令でプログラムの実行がおかしくなったかなどを見つけるのに役立つ。

問 21 エ

DRAM の説明 (H30 秋・FE 問 21)

DRAM (Dynamic Random Access Memory) は、各構成素子が電荷を蓄えた状態か否かによって 1 ビットを記憶するメモリである。構成素子として微小なコンデンサ（キャパシタ）が利用され、蓄えた電荷の量は時間の経過とともに放電によって減少する。このため、数ミリ秒ごとに内容を書き直す“リフレッシュ”と呼ばれる動作が必要となる。アクセス速度は後述の SRAM (Static RAM) に比べて遅いが、回路が簡単のため 1 ビット当たりの単価が安く、大容量のものを作りやすい。このため、PC やスマートフォンをはじめとする多くのコンピュータの主記憶は DRAM で構成されている。したがって、(エ) が適切である。

ア：バイト単位でデータの消去と書き込みが可能な不揮発性メモリであることから、EEPROM (Electrically Erasable Programmable ROM) の説明である。

イ：フラッシュ ROM (メモリ) の説明である。書き込みはブロック単位で行う。

なお、SSD (Solid State Drive) はフラッシュメモリを使った記憶装置で、大

容量化が進み、ハードディスクの代わりに使用されるようになってきている。
 ウ：SRAM の説明である。DRAM と比べてデータを速く読み出せるが、構造が複雑なため集積度が低く、ビット当たりのコストも高くなる。

問 22 イ

4 入力 NAND 回路の構成 (H30 秋・FE 問 22)

2 入力 NAND 素子は、2 入力を A , B として、出力を O とすると、ブール代数の式で表現すると、 A と B の AND の否定であるから

$$O = \text{NOT } (A \text{ AND } B)$$

と表現される。

4 入力を A , B , C , D とすると

$$O = \text{NOT } (A \text{ AND } B \text{ AND } C \text{ AND } D)$$

と表現される。これを図中にあるように 2 入力の素子しか存在しない前提を踏まえて、展開すると、

$$= \text{NOT } ((A \text{ AND } B) \text{ AND } (C \text{ AND } D))$$

と表現される。この式は、 A と B の AND と C と D の AND をとり、さらに AND をとるということを意味している。これを基に、各選択肢の NAND 回路をブール代数で表現したものにすると、次のようになる。

$$\text{ア：} O = \text{NOT } (\text{NOT } (A \text{ AND } B) \text{ AND } \text{NOT } (C \text{ AND } D))$$

$$= (A \text{ AND } B) \text{ OR } (C \text{ AND } D)$$

$$\text{イ：} O = \text{NOT } (\text{NOT } (\text{NOT } (A \text{ AND } B) \text{ AND } \text{NOT } (\text{NOT } (C \text{ AND } D))))$$

$$= \text{NOT } ((A \text{ AND } B) \text{ AND } (C \text{ AND } D))$$

ウ：左側の上部 A , B の部分は

$$O_{\text{上部}} = \text{NOT } (\text{NOT } (A) \text{ AND } \text{NOT } (B)) = A \text{ OR } B$$

下部の C , D も同様であり、

$$O_{\text{下部}} = \text{NOT } (\text{NOT } (C) \text{ AND } \text{NOT } (D)) = C \text{ OR } D$$

上部と下部を右側の入力とすると

$$O = \text{NOT } (\text{NOT } ((A \text{ OR } B) \text{ AND } (C \text{ OR } D)))$$

$$= (A \text{ OR } B) \text{ AND } (C \text{ OR } D)$$

エ：左側の上部 A , B の部分は

$$O_{\text{上部}} = \text{NOT } (\text{NOT } (\text{NOT } (A) \text{ AND } \text{NOT } (B)))$$

$$= \text{NOT } (A) \text{ AND } \text{NOT } (B) = \text{NOT } (A \text{ OR } B)$$

上部と同様に C , D の下部を右側の入力とすると

$$O = \text{NOT } (\text{NOT } (\text{NOT } (A \text{ OR } B) \text{ AND } \text{NOT } (C \text{ OR } D)))$$

$$= \text{NOT } ((A \text{ AND } B) \text{ AND } (C \text{ AND } D))$$

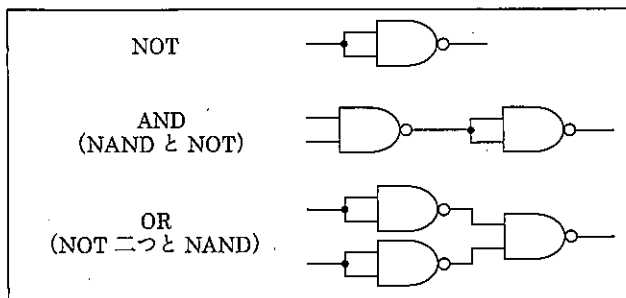
$$= \text{NOT } (A \text{ AND } B) \text{ OR } \text{NOT } (C \text{ AND } D)$$

となる。

以上から、4 入力の NAND 回路となるのは、(イ) が正解である。

(注) 上記の展開では、ド・モルガンの定理： $\text{NOT } (A \text{ OR } B) = \text{NOT } (A) \text{ AND } \text{NOT } (B)$

NOT (B) を適用している。なお、論理演算では、AND、OR、NOT の三つが基本演算であるが、実際に論理演算を実行する集積回路では、三つの基本演算機能を個別に実装すると複雑になるため、集積回路では、NAND (又は NOR) の 1 種類で論理回路を構成する手法をとっている。



問 23 エ

二次電池 (充電式電池) (H30 秋・FE 問 23)

電池は、放電してしまうと使用できない使い切りの一次電池と、充電すると繰り返し使用できる二次電池に分類できる。二次電池は蓄電池 (充電式電池) ともいう。選択肢の中で二次電池は (エ) の「リチウムイオン電池」である。

リチウムイオン電池は、軽量で高電圧を維持できる特徴があるため携帯電話、スマートフォン、タブレット、PC などのバッテリーとして利用されている。リチウムイオンで電子を運び充放電を繰り返す。使い切る前に充電すると容量が少なくなるメモリ効果が少なく、頻繁な充放電の繰返しや自然放電が少ない点もモバイルバッテリーとして適している。

ア：アルカリマンガン乾電池は一般によく使われている一次電池である。二酸化マンガンと亜鉛を極に持ち、アルカリ濃度の高い電解液を使用する。電気容量が大きく長持ちするため、大容量を必要とし長時間使用する強力ライト、リモコン、モータを使用する機器などに向いている。

イ：酸化銀電池はボタン型の一次電池である。酸化銀と亜鉛を両極に持つ。電池の寿命が来る直前まで安定した電圧を維持するため、時計や電子体温計などの精密さを要する機器に使用される。

ウ：燃料電池は水素と酸素の化学反応によって電気を発電する。放電や充放電する電池と異なり、水素と酸素を燃料として供給することで継続的に発電する仕組みである。発電と同時に発熱もするため、利用効率の良い環境にやさしい発電装置とされている。宇宙開発、発電所から、家庭用、自動車の駆動まで様々な用途に利用されている。

問題の人間とコンピュータのやり取りを見ると、音声だけのインタフェースであたかも人と人が話しているようにコンピュータが受け答えをしている。これは自然言語インタフェースである。自然言語とは人間が使う言語のことを指す。自然言語処理では統計的手法を使用して、形態素解析→構文解析→文脈解析→意味解析と進み、その逆をたどって返答などを返す方法で進められてきた。また、文字でなく音声だけのやり取りでは、この問題の列車の予約システムのように不特定多数の人が利用する場合には発音の個人差、単語と単語の間隔が短い際の単語の結合、意味の複数の解釈、内容自身の曖昧さなど解決する課題は様々である。AI の技術が進んだ現在では、自然言語の解析や返答に AI を利用し、スマートフォンやスピーカ型の音声だけの自然言語インタフェースなどが実現されている。したがって、(イ)「自然言語インタフェース」が正解である。

ア：感性インタフェースは人とコンピュータが表情や身振りなどを双方でやり取りし、人の意思を的確にくみ取り使いやすくしたインタフェースで、ロボットへの実装の取組みが始まっている。

ウ：バーバルコミュニケーション (verbal communication) は会話や文字などの言葉を使ったコミュニケーションのことで、ノンバーバルコミュニケーションは言葉以外の身振り手振り、表情、視線、態度、声のトーンなどの情報でコミュニケーションをとることである。人間とコンピュータとのノンバーバルインタフェースには、会話できない場合の視線による入力や、表情変化の画像解析、センサや映像を使用した身振りの解析がある。

エ：マルチモーダル (multimodal) とは、複数の様式の意味である。マルチモーダルインタフェースは文字や音声言語だけでなく、表情、身振り・手振り、視線など複数の方法でコンピュータとやり取りするインタフェースである。擬人化されたキャラクタとのやり取りで処理を進める方法などがある。(ウ) のノンバーバルインタフェースはマルチモーダルインタフェースの一種と考えられる。

問 25 ア

直線の境界を滑らかに表示する技術 (H30 秋・FE 問 25)

液晶ディスプレイなどの表示装置を用いたコンピュータグラフィックスで、例えば傾いた直線の境界を滑らかに表示するには、境界に生じるギザギザ (ジャギーという) を目立たなくする必要がある。この技術をアンチエイリアシング (anti-aliasing) という。具体的に言うと、画像は、画面を構成する画素の色を変えることで表示している。このとき、画素は与えられた数値に相当する色しか表示できないので、色の境界は階段状になってしまい、それを目立たなくするためには色彩の中間色を割り当てる必要がある。例えば、白地に黒文字を表示する場合には、中間色の灰色を利用してジャギーを目立たなくする。したがって、(ア)

が正解である。

イ：シェーディング (shading) とは、3次元コンピュータグラフィックスの 3D モデル表面に明暗のコントラストを付けて立体感を与えることである。

ウ：テクスチャマッピング (texture mapping) とは、3次元コンピュータグラフィックスの 3D モデル表面に 2D の画像を貼り付けることで質感を与えることである。

エ：バンプマッピング (bump mapping) とは、3次元コンピュータグラフィックスの 3D モデル表面に凹凸があるかのように見せることである。

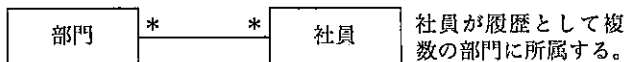
問 26 エ

UML を用いて表した図のデータモデルの多重度 (H30 秋・FE 問 26)

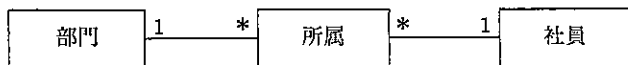
UML クラス図の多重度の表記は、関連の線の近くに「最小値..最大値」の形式で記述する。最小値は、対応するがインスタンス (実現値) が存在しないことが許される場合は 0、一つ以上の場合は 1 である。最大値に制限がない場合、* と表記する。

空欄 a は、条件(1)に「部門には 1 人以上の社員が所属する」とあるので、部門から見た多重度は 1..* である。空欄 b は、条件(3)に「社員が部門に所属した履歴を所属履歴として記録する」とあり、社員には最低一つの所属履歴があり、一般には n 個の所属履歴があるので、社員から見た多重度は 1..* である。したがって、(エ) が正解である。なお、部門と社員は、一般に多対多の関連があるが、その関連を 1 対多と多対 1 の二つの関連に分解する。多対多の関連は、データモデル (E-R 図) を関係データベースで実装する場合、第 3 正規形を満たす形で展開できないので、1 対多と多対 1 の二つの関連に分解 (正規化) する。

部門には複数の社員が所属する。



↓ 多対多を排除 (関係データベースでの正規化と等価)



問 27 イ

データ項目の命名規約だけでは回避できない事象 (H30 秋・FE 問 27)

データ項目の命名規約は、システム開発において標準化が必要とされる事柄の一つで、開発メンバが一意にデータ項目を識別するために設ける。開発メンバが命名規約に基づいてデータ項目名を決めることで曖昧さや重複がなくなり、データ項目名を命名した開発メンバ以外も、データ項目名からどのデータを指すかを

一意に特定することができるようになる。しかし、データの取り得る値は仕様によって異なり、データ項目名やデータ型から一意に決められるものではなく、命名規約に定義できるものではない。したがって、(イ)が正解である。参考までに、データ項目の取り得る値の範囲を定めることを、関係データベースでは、定義域(ドメイン)制約という。

ア：命名規約(1)によって、データ項目名が決まればデータ型も定まる。また、命名規約(2)によって、同音異義語は発生しないので、“受信年月日”という同音のデータ項目名で日付型と文字列型が混在することはない。

ウ：命名規約(2)によって、“賞与金額”と“ボーナス金額”という異音同義語が発生することはない。

エ：命名規約(1)によって、“取引先”の末尾には必ず“コード”や“名”などの区分語が付与されるので、判別できる。

問 28 ウ

関係代数演算 (H30 秋・FE 問 28)

関係 X と Y を自然結合した後とあるので、共通属性の学部コードで結合すると、次の表(結合結果)となる。その後、実行結果として Z を得るためには、その表のうち必要部分を取り出す操作が必要で、図のように、選択(横方向に組(タプル、行)を選ぶ演算)と射影(縦方向に属性を選ぶ演算)の二つの演算を行う。したがって、(ウ)が正解である。

X

学生番号	氏名	学部コード
1	山田太郎	A
2	情報一郎	B
3	鈴木花子	A
4	技術五郎	B
5	小林次郎	A
6	試験桃子	A

Y

学部コード	学部名
A	工学部
B	情報学部
C	文学部

結合結果（網掛け部分が実行結果 Z）

学生番号	氏名	学部コード	学部名
1	山田太郎	A	工学部
2	情報一郎	B	情報学部
3	鈴木花子	A	工学部
4	技術五郎	B	情報学部
5	小林次郎	A	工学部
6	試験桃子	A	工学部

選択

射影

午前解答

問 29 ア

ロックの粒度 (H30 秋・FE 問 29)

ロックは DBMS (DataBase Management System ; データベース管理システム) が同一データに複数のトランザクションがアクセスし不整合が起こらないようにする排他制御で用いられる。アクセスするデータにロックをかけると、他のトランザクションからのアクセスを制限することができる。アクセスが終了するとロックを解放し他のトランザクションからのアクセスが可能になる。データを更新する場合は、他のトランザクションからの参照も更新も許可しない専有ロックをかけ、参照だけの場合は他のトランザクションからの更新は許可しないが参照だけは許可する共有ロックをかける。共有ロックの場合は他のトランザクションからの共有ロックも可能である。ロックをかける範囲には、行（レコード）単位、表（ブロック）単位、データベース単位、などがありこれをロックの粒度と呼ぶ。更新処理の場合、行単位のようにロックの粒度が小さければ別のデータを利用する他のトランザクションと競合する可能性は少なくなり待ち時間は短くなる。表全体のように粒度を大きくするとアクセスする対象のデータ以外に多くのデータを専有ロックするため他のトランザクションがロック解除されるまでの待ちが長くなり、全体のスループットが低下する。したがって、(ア) が正解である。

イ：同一のデータを更新するトランザクションの数が多いときには、粒度の大きさに関係なくそのトランザクションの更新処理中は専有ロックをかけるため、他のトランザクションからの更新はできない。更新対象以外のデータをアクセスするトランザクションは粒度が大きい場合は実行を待たされる。したがって同時実行できるトランザクションの数は少なくなる。

ウ：参照の場合は共有ロックをかけるので、ロックの粒度に関係なく他のトランザクションからのデータ参照は可能である。

エ：一つのトランザクションが一つの表の三つのデータを処理する場合を考えると、粒度の小さい行単位でロックをかけると3個のロックをかけることになり、粒度の大きい表全体にロックをかけた場合は1個のロックで済む。したがって、粒度を大きくすると一つのトランザクションでかけるロックの個数は少なくなる。

問 30 エ

データベースを回復する操作 (H30 秋・FE 問 30)

問題文にあるような媒体障害など物理的な障害に対処するために、バックアップデータ（退避データ）とログ（更新履歴）を用いて行われる回復操作を、ロールフォワード処理という。したがって、(エ)が正解である。記憶媒体に障害が発生した場合には、まず、記憶媒体自体を修理あるいは交換などして使えるようにし、失われたデータを回復する。このとき、障害発生前に採った最も新しいバックアップデータを用いて、バックアップ時点のデータベース内容に回復する。次に、その退避時点から障害発生直前まで行われた更新処理をログファイルの更新後ログを使って回復する。

データベースに発生する障害には、デッドロックの解除処理など論理的な障害もある。このような障害に対処するには、ロールバック処理が行われる。例えば、更新処理の直後に異常終了したような場合を考える。その更新を無効にするために、更新履歴の更新前ログを使って更新前の状態に戻す処理を行う。

ア：アーカイブ……幾つかのファイルをまとめた保管用のファイルのことで、圧縮した書庫ファイルとするのが普通である。インターネットでは、公開されているファイルの保管庫のことをいう。もともとは、公文書の保管庫などを意味する英語である。

イ：コミット……トランザクションによる処理が正常終了した場合に、データベースの更新を確定することをいう。コミット後は更新結果が保持されて他のトランザクション処理でも参照可能となる。

ウ：チェックポイントダンプ……チェックポイントはプログラムの中断点で、このときのコンピュータの状態を保存するために必要な情報を書き出すことがダンプである。ダンプに基づいてリスタート（再開）することもできる。なお、データベースへの更新データ書出しは、通常、一定時間隔ごとのタイミングで行われ、この時点で実行中のトランザクション情報やデータベース更新履歴などのログ情報も書き出される。障害発生後のデータベース回復はこの書出し時点の一つの目印として行うことになるが、この時点のことをトランザクション処理のチェックポイントという。

問 31 エ

伝送時間の計算 (H30 秋・FE 問 31)

伝送時間の計算に必要となる情報は、転送するデータ量と回線速度である。転送するデータ量は、問題文から 12M バイトと分かる。一方、回線速度であるが、「伝送路の伝送効率を 50% とする」とあるため、 $1.5\text{M ビット/秒} \times 50\% = 750\text{k ビット/秒}$ となる。ここで単位を統一するため、データ量の単位を k ビットに変換すると、 $12\text{M バイト} \times 8 \text{ ビット/バイト} = 96,000\text{k ビット}$ となる。よって、

$$96,000\text{k (ビット)} \div 750\text{k (ビット/秒)} = 128 \text{ (秒)}$$
 となる。したがって、(エ) が正解である。

問 32 ウ

LAN 間接続装置 (H30 秋・FE 問 32)

LAN と LAN を接続することで、更に広範囲をカバーする LAN が構築できる。その際、OSI 基本参照モデルのどの層の機能レベルで接続するかによって、必要な装置が異なる。

リピータは、物理層でのセグメント間の接続に使い、信号を増幅し中継を行う。特にデータを識別することなく単に伝送路を延長することになる。したがって、(ウ) が適切である。

ア：ゲートウェイは、OSI 第 4～7 層についてプロトコルが異なるネットワークの相互接続を行う。

イ：ブリッジは、データリンク層 (OSI 第 2 層) が使用するアドレス (MAC アドレス) を用いて、そのフレームを通過させるべきかどうかを判断 (フィルタリング) し、中継を行う。

エ：ルータは、ネットワーク層 (OSI 第 3 層) が使用するアドレス (IP アドレス) を用いて、データを中継する経路の選択 (ルーティング) を行う。

問 33 エ

DNS が果たす役割 (H30 秋・FE 問 33)

現在のインターネット上で使用されている IP アドレスは、32 桁の 2 進数 (便宜上 10 進数 3 桁で四つに分けて表記する。IPv6 では 128 桁) であり、人間にとっては覚えにくい。このため、文字列を用いたドメイン名というアドレスが用いられる。そして、このドメイン名から IP アドレスを探す仕組みを DNS (Domain Name System) といい、例えば、www.abcdef.co.jp というドメイン名から、その IP アドレスを探し出す。DNS サーバは、このドメイン名から IP アドレスへの変換機能をもつサーバのことで、(エ) が正解である。

ア：この機能をもつものに、DHCP (Dynamic Host Configuration Protocol) サーバがある。これは、それぞれのコンピュータにあらかじめ IP アドレスを割り当ててではなく、クライアントのコンピュータからの要求の都度、DHCP サーバが IP アドレスを自動的に設定するものである。

イ：ネットワーク上の資源を管理するディレクトリサービスに関する記述である。

ウ：NAT (Network Address Translation) や, NAPT (Network Address Port Translation) (IP マスカレードともいう) に関する説明である。特に NAPT は、限られたグローバル IP アドレスを有効に利用するための技法として重要である。

問 34 ウ

インターネットにおける電子メールの規約 (H30 秋・FE 問 34)

インターネットを利用した電子メールの規約で、メッセージヘッダの拡張 (電子メールのタイトルに日本語が使用できることなど) のほか、テキスト文書だけではなく、ワープロ文書・音声・画像データなどを扱えるようにした規格が MIME (Multipurpose Internet Mail Extensions) である。したがって、(ウ) が正解である。

ア：HTML (HyperText Markup Language) ……Web サーバによって配信されるコンテンツを記述するための言語である。

イ：MHS (Message Handling System) ……ITU-T が標準化した電子メールシステムである。企業間の EDI を行う国内標準の H 手順は、MHS を採用している。

エ：SMTP (Simple Mail Transfer Protocol) ……TCP/IP ネットワークにおいて、メールクライアントからメールサーバへのメール送信や、メールサーバ間でメールの送受信を行うためのプロトコルである。

問 35 ア

携帯電話機で使用される通信規格の名称 (H30 秋・FE 問 35)

LTE (Long Term Evolution) は、第 4 世代 (4G) の移動体通信規格である。携帯電話網は、携帯電話やスマートフォンなどの移動体通信機器を使って相互間通信を行うための通信網で、通信回線にはパケット交換機を使って接続している。そのため、全ての通信をパケット交換方式で処理している。また、MIMO (Multiple Input Multiple Output) と呼ばれる複数のアンテナを使用する通信方式を利用することで、屋内外問わず、数十 M ビット/秒の無線通信を行うことができる。そして、これらの仕様は 3GPP (3rd Generation Partnership Project) によって標準化されている。3GPP は、第 3 世代 (3G) 以降の移動体通信に関して、標準仕様の検討や調整を行う国際標準化プロジェクトである。したがって、(ア) が正解である。

イ：MAC (Media Access Control) は、データリンク層の通信プロトコルである。

PC や通信機器がもつ MAC アドレスはこの通信プロトコル用の識別子である。

ウ：MDM (Mobile Device Management) は、モバイル端末が紛失、盗難にあった場合を想定した情報保護技術である。代表的な機能として、モバイル端末を

遠隔操作でロックするリモートロックや、遠隔操作で内部の情報を消去するリモートワイプ、GPS による位置の特定などがある。

エ：VoIP (Voice over Internet Protocol) は、TCP/IP ネットワーク (インターネットやイントラネット) を使用して音声データを送受信する技術である。社内 LAN を利用した内線電話や、IP 電話、インターネット電話などに使われている。

問 36 ア

アプリケーションソフトウェアにデジタル署名を施す目的 (H30 秋-FE 問 36)

アプリケーションソフトウェアの入手や配布をインターネット上で行う場合、利用者からするとその安全性や信頼性は気になるところである。正規品と思って購入したのに、マルウェアが仕込まれた改ざんソフトウェアだったり、配布元をなりすましていた模造品だったりでは使えない。しかし、デジタル署名が施されていれば、署名鍵と対になる復号鍵でそれを検証することで、配布元の確認と改ざん有無を検出することができる。したがって、(ア) が正解である。

イ：ソフトウェアライセンスの目的である。デジタル署名が配布元を特定するために付されるのに対し、ソフトウェアライセンスは利用者を特定するために付されるものである。

ウ：著作権登録制度の目的である。例えば、著作権のある製造元とそれを配布する販売元が異なる場合では、販売元がデジタル署名を施すこともある。この場合、デジタル署名は著作権の保護や確認の意味をなさないの、著作権の証明に著作権登録制度を使用する。デジタル署名はソフトウェアの作成者だけでなく、販売者が付与することもあり得る。そしてこれは必ずしも著作権者と一致するわけではないため、著作権が作成者にあることの証明には使われない。

エ：デジタル署名を施しても利用者による修正や改変を防ぐことはできない。しかし、修正や改変をしたことによって、アプリケーションソフトウェアのハッシュ値も変わるので前述したように修正や改変したことを検出できる。

問 37 エ

ブルートフォース攻撃に必要な試行回数の最大値 (H30 秋-FE 問 37)

共通鍵暗号方式の暗号化鍵は、他者に公開せず、利用者が秘密にして使うものである。しかし、共通鍵暗号方式の代表例である AES (Advanced Encryption Standard) では、暗号化に用いているアルゴリズムを公開している。また、共通鍵暗号方式では、暗号化と復号に同じ鍵を使うので、暗号化鍵を入手できれば、暗号文を復号することができる。そして、AES-256 の 256 は、鍵長が 256 ビットであることを意味しているの、ブルートフォース攻撃、つまり総当りで暗号化鍵となり得るビット列を試せば、解読が可能である。よって、256 ビットの 2 進数で表現できるビット列は 2^{256} 種類なので、総当りの試行回数の最大も 2^{256} と

なる。したがって、(エ)が正解である。

問 38 ウ

共通鍵暗号方式の特徴 (H30 秋・FE 問 38)

共通鍵暗号方式は、暗号化と復号に同じ鍵を使用する暗号化方式である。同じ程度の暗号強度をもつ鍵長を選んだ場合、公開鍵暗号方式よりも暗号化、復号の速度が速い利点がある。したがって、(ウ)が正解である。

ア：共通鍵暗号化方式を用いて暗号化通信を行う場合、鍵を相手と共有する必要があるが、これが漏えいしてしまえば暗号化通信にならない。このため事前に相手に鍵を渡す必要があるが、平文で送ってしまうと通信を傍受した第三者に漏えいしてしまう。現実的には暗号化通信を共通鍵暗号方式で行う際に、先に公開鍵暗号方式による暗号化通信を行い、共通鍵の交換を行うハイブリッド暗号方式が一般的になっており、SSL/TLS もこのハイブリッド暗号方式の一種である。

イ：共通鍵暗号方式の場合、ある相手と暗号化通信を行う際に使用する鍵は、他の通信相手とは分けて置かないと、互いに解読可能になってしまう。このため、1人がN人と暗号化通信をする場合はN個の鍵が必要になる。しかし、相手が1人であれば、鍵も1個となり、公開鍵暗号方式で必要になる鍵の数より少なくなる。なお、公開鍵暗号方式の鍵のペア（秘密鍵と公開鍵）を2個と数える場合、公開鍵暗号方式でAさんとBさんという2人で暗号化通信を行うとすると、Aさんの秘密鍵、公開鍵、Bさんの秘密鍵、公開鍵の合計4個の鍵が必要になる。

エ：公開鍵暗号方式に関する説明である。公開鍵暗号方式の原理では公開鍵で暗号化した文書は秘密鍵で復号できる一方、秘密鍵で暗号化したデータは公開鍵で復号できる。前者は暗号化通信に、後者はデジタル署名として利用されている。

問 39 イ

真正性及び信頼性に対する定義 (H30 秋・FE 問 39)

JIS Q 27000:2014（情報セキュリティマネジメントシステム—用語）では、情報セキュリティマネジメントシステム（ISMS）における各種用語の定義をしている。その中で真正性、信頼性は次のように定義されている。

用語	意味
真正性 (authenticity)	エンティティは、それが主張するおりのものであるという特性
信頼性 (reliability)	意図する行動と結果とが一貫しているという特性
可用性 (availability)	認可されたエンティティが要求したときに、アクセス及び使用が可能である特性
機密性 (confidentiality)	認可されていない個人、エンティティ又はプロセスに対して、情報を使用させず、また、開示しない特性

したがって、(イ) が適切である。

なお、定義 c は可用性、定義 d は機密性を指している。

問 40 ア

JPCERT/CC が作成したもの (H30 秋・FE 問 40)

CSIRT (Computer Security Incident Response Team ; シーサート) は、セキュリティインシデント (セキュリティを損なう事象) への対応を専門に行う組織の総称である。セキュリティインシデントについて、単に技術的な支援を行うだけでなく、組織全体の視点から対応することを目的に編成されている。

JPCERT/CC (Japan Computer Emergency Response Team Coordination Center ; JPCERT コーディネーションセンター) は、国内のサイトに関するセキュリティインシデントの報告の受付、分析や対策の検討、対応の支援や助言などを技術的に行う組織で、これらの対策や対応内容を、CSIRT の構築を支援する目的で作成したものが CSIRT マテリアルである。したがって、(ア) が正解である。

イ : ISMS ユーザーズガイドは、JIS Q 27001 (ISO/IEC 27001) に対応したガイドラインで、ISMS の構築を支援する目的で JIPDEC (一般財団法人日本情報経済社会推進協会) が作成したものである。

ウ : 証拠保全ガイドラインは、インシデント発生時に最初に電磁的記録を保全する実務者を支援するために、デジタル・フォレンジック研究会が作成したものである。

エ : 組織における内部不正防止ガイドラインは、内部不正の防止を支援するために IPA (独立行政法人 情報処理推進機構) が作成したものである。

問 41 エ

ボットネットにおける C&C サーバの役割 (H30 秋・FE 問 41)

ボットは、コンピュータの中に潜み、ネットワークを経由して受け取った命令を実行する攻撃プログラムである。そのため、ボットに感染したコンピュータは遠隔操作されてしまう。ボットネットは、ボットに感染したコンピュータ群とこれらを遠隔操作する C&C サーバ (Command and Control server) で構成されるネットワークである。C&C サーバは、ボットに感染したコンピュータに攻撃命令

を出したり、その応答を受け取ったりする役割をもつ。したがって、(エ)が適切である。

ア：プロキシサーバの役割である。

イ、ウ：PPPサーバやRADIUSサーバの役割である。CHAP(Challenge-Handshake Authentication Protocol；チャレンジハンドシェイク認証プロトコル)は、チャレンジレスポンス方式を用いた認証プロトコルで、伝送路上にパスワードそのものを送信しないことでパスワードの盗聴を防止する。

問 42 ウ

IDSの機能 (H30 秋・FE 問 42)

IDS (Intrusion Detection System；侵入検知システム)は、サーバやネットワークに対する不正侵入を検知し、設定された方法で通知をする仕組みや装置のことである。不正侵入は「セキュリティポリシーを侵害するような挙動」ともいえる。したがって、(ウ)が正解である。

ア：各ソフトウェア製品の脆弱性をねらった攻撃を防ぐためには、ソフトウェア製品を常に最新版に保つことが重要である。最新版の有無を自らチェックし、バージョンアップを行うソフトウェア製品もある一方で、手動操作でのバージョンアップが必要になる製品、買替えが必要なソフトウェア製品もある。このため、PC内の各ソフトウェア製品のバージョンをリストアップする「バージョンチェッカ」と呼ばれるソフトウェアをPC上で実行することも有効である。

イ：実際の製品に対してテストデータを送り、応答や挙動から脆弱性を検査する手法をペネトレーションテスト(侵入テスト)と呼び、そのための機能をもつテスト用のソフトウェアをペネトレーションテストツールと呼ぶ。

エ：IPA(独立行政法人 情報処理推進機構)が公開している情報セキュリティ対策ベンチマーク(セルフチェック)の説明である。

問 43 ウ

セキュアブートの説明 (H30 秋・FE 問 43)

セキュアブートとは、安全に(セキュア)にPCを起動(ブート)することである。具体的には、PCの起動時にOSやドライバのデジタル署名を検証し、許可されていないものを実行しないようにすることで、OS起動中のマルウェアの実行を防ぐ技術である。ウイルス対策ソフトが起動しているとマルウェアの実行や感染は防御されてしまうので、マルウェアの中にはルートキットを使って、ウイルス対策ソフトが起動する前、更にはOSが起動する前に自らを実行させようとするものがある。これを防ぐには、PC起動時に実行するよう設定されているファイルであっても、許可されていないものは実行しないようにするほかなく、許可されているファイルかどうかの判定にはデジタル署名が有効である。したがって、(ウ)が正解である。

ア：BIOSパスワードは、パワーオンパスワードとも呼ばれ、PCの正当な利用者

以外の不正な起動を防ぐ技術である。

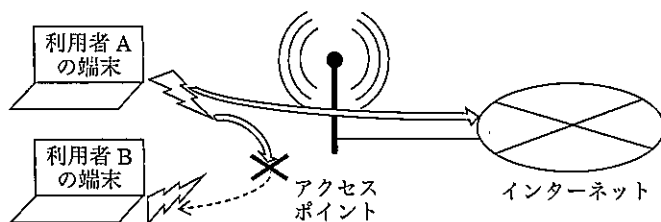
イ：HDD パスワードは、BIOS によってハードディスクに設定されるパスワードで、ハードディスクへの不正なアクセスを防ぐ技術である。HDD パスワードを設定した PC に限り、そのハードディスクにアクセス可能となる。

エ：マルウェア対策ソフト（ウイルス対策ソフト）の説明である。

問 44 エ

公衆無線 LAN のアクセスポイントのセキュリティ対策 (H30 秋・FE 問 44)

公衆無線 LAN のアクセスポイントを設置するときのセキュリティ対策なので、不特定多数の人が使うことを想定する。その場合、アクセスポイントに無線で接続し、そこを経由して使いたいサービスを利用するのが一般的な使い方である。しかし、アクセスポイントに接続している端末の情報を調べることもできるので、その情報を使えば、アクセスポイントを経由して他の端末に無断でアクセスすることも可能である。



不特定多数ということは悪意のある人がアクセスポイントを使う可能性もあり、これを防ぐには、同一のアクセスポイントに無線で接続している端末同士の通信を、アクセスポイントで遮断する対策が有効である。したがって、(エ)が適切である。

ア：MAC アドレスフィルタリングは、未登録の端末を接続させないための対策である。しかし、不特定多数が使う公衆無線 LAN では、全ての MAC アドレスをあらかじめ登録しておくことは不可能であり、フィルタリングを実施できない。そのため、なりすましを防止することはできない。

イ：SSID (Service Set Identification) は無線 LAN の識別子で、無線 LAN のアクセスポイントは、自身の SSID を定期的に発信して利用者に自身の存在を知らせている。これを行わず、自身の存在を隠すには SSID ステルス機能を使う。

ウ：ドメイン名も SSID もどこかに登録して使用するものではなく、同じドメイン名や SSID の使用を禁止することはできない。しかし、悪意のあるアクセスポイントでは、そこを利用してもらいやすくするためにパスワードを設定しないのが一般的である。そのため、悪意のあるアクセスポイントと区別するには、SSID とパスワードを組み合わせる、WPA2-PSK などが有効である。

メールの第三者中継とは、外部ネットワークから受信したメールの宛先が、メールサーバの管理するドメインとは異なるドメイン名をもったメールアドレスであった場合に、その異なるドメインにあるメールサーバに対してメールを中継することをいう。

具体的には、接続元 IP アドレス (又は、電子メールの送信者のドメイン名) が社外で、電子メールの受信者のドメイン名も社外であるメールが該当する。この条件で、表中の選択肢を確認していくと、送信者のドメイン名が他社 (a.b.d) で、かつ受信者のドメイン名も他社 (a.b.e) となっている (ウ) を見つけることができる。したがって、(ウ) が正しい。この問題では、IP アドレスとドメイン名は詐称されていないという条件があるので、ドメイン名だけに着目すればよい。

なお、(ア) は自社から他社、(イ) は自社から自社、(エ) は他社から自社へのメールなので、第三者中継には該当しない。

UML (Unified Modeling Language) は、モデリングに関する設計上の表現を標準化した統一モデリング言語である。UML2.0 には 13 種類の書式があり、構造に関するものと振舞い (動作) に関する書式に分かれており、シーケンス図もコミュニケーション図も振舞いに関する書式に分類される。シーケンス図は、オブジェクト間の相互作用を時間の経過に着目して記述する書式で、時間軸に沿って、状態遷移、時間制約、メッセージ送受信などを表現する。コミュニケーション図も、オブジェクト間の相互作用を記述する書式だが、時間ではなく、オブジェクト間の協調関係 (データリンク) に着目して、メッセージ送受信やデータの流れを表現する。よって、両者に共通して表現されるのは、オブジェクト間で送受信されるメッセージである。したがって、(エ) が正解である。

ア：ステートマシン図で表現されるものである。

イ：タイミング図で表現されるものである。

ウ：シーケンス図で表現されるものである。

オブジェクト指向において、クラスは定義であり、インスタンスは定義に基づき作成した実体である。逆の言い方をすると、クラスは、共通の属性とメソッドをもつオブジェクト (インスタンス) を集めたものである。

例えば、お菓子のクッキーを作る場合、生地を型枠で抜いて同じ形のクッキーを複数作ることができる。この場合、型枠が定義、複数作られたクッキーが複数の実体である。このように、一つのクラス定義に基づいて、複数のインスタンス

が生成される。インスタンスが生成されることは、メモリなどの資源が割り当てられることである。また、クッキーの型枠に様々な形があるように、クラスには、クラスごとに変数やメソッドが定義されている。したがって、(イ)が正解である。
 ア、ウ：インスタンスとクラスの関係が逆である。
 エ：一つのクラスに対して、複数のインスタンスが存在可能である。

問48 ウ

結合度が最も弱いモジュール結合 (H30 秋・FE 問48)

午前解答

モジュール結合度は、モジュール間の結び付き方に関する尺度である。モジュール間の情報の受渡し方を結び付き度合いとして、結合度を評価する。モジュール結合度が弱いほど良く、モジュールの独立性が高い、つまり他のモジュールからの影響が低いといえる。最も結合度が弱いのは、処理の実行に必要なデータ(変数)だけをパラメタ(引数)として受け渡すデータ結合である。したがって、(ウ)が正解である。

ア：共通結合は、複数のモジュールがグローバル変数など共有域にあるデータを共有しているので結合度は強い。他のモジュールがそのデータを更新するとその影響を受けることになる。

イ：制御結合は、他のモジュールの機能を選択する制御パラメタをもつので、データ結合より結合度が強い。他のモジュールの機能が変えると制御パラメタの受渡しも変更しなければならない。

エ：内容結合は、外部宣言していない他のモジュール内のデータを直接参照しているのが最も結合度が強い。他のモジュールがないと実行できないため、他のモジュールのインストールが必須となるだけでなく、他のモジュールに仕様変更があった場合、その影響を受けることになる。

問49 イ

オブジェクト指向における委譲の説明 (H30 秋・FE 問49)

オブジェクト指向における“委譲”とは、あるオブジェクトに対する操作を、他のオブジェクトに依頼する仕組みのことである。したがって、(イ)が適切である。具体的には、ある操作(メソッド)に対する処理を、他のオブジェクトに対するメッセージの送信(処理の依頼)として実装する。

委譲(デリゲーション)はオブジェクト指向における、再利用技術の一つとして位置付けられる。オブジェクト指向における再利用技術としては、継承が代表的であるが、継承ではスーパークラスで定義された全てのメソッドが利用可能となる。しかし、実際には、全てのメソッドを使用しないような場合でも、一部メソッドの再利用のためだけに継承関係を定義してしまい、クラス間の関係に混乱が発生するという問題が指摘されている。このため、他のクラスの一部の機能だけを利用する場合には、無理な継承を用いずに、委譲によって処理を依頼するようにすべきであるという提案がなされている。

ア：伝搬（プロパゲーション）のことである。

ウ：継承（インヘリタンス）のことである

エ：複合オブジェクトのことである。

問 50 イ

XP のプラクティスの説明 (H30 秋・FE 問 50)

XP (Extreme Programming) のプラクティスとしては、以下のようなものがある。

名称	手法
テスト駆動開発 (テストファースト)	テストケースを作成すること自体がソフトウェア設計であるという思想であり、ソフトウェア設計の最初のフェーズでテストケースを作成する。
ペアプログラミング	2 人一組で設計・開発を行うことで、ケアレスミスの防止や、知識・情報の共有を図る。
リファクタリング	モジュールが完成しても、さらなる効率化や可読性を求め、コードを改良していく。
ソースコードの共有	複数の開発メンバがそれぞれの作成したコードを共有する。
継続的インテグレーション	新しいモジュールやリファインされたモジュールの結合を継続的に行う。
反復 (イテレーション)	設計・コーディング・テストを反復的に繰り返しながら、システム開発を進める。

「コードの結合とテストを継続的に繰り返す」という記述は、ここでいう継続的インテグレーションにあたる。したがって、(イ) が適切である。

ア：単体テストの仕様に責任をもつのは、全員である。そのために、ソースコードの共有が重要である。

ウ：前述の様に、テストケースは設計段階で作成する。

エ：リファクタリングは常に行う。

問 51 エ

WBS を使用する目的 (H30 秋・FE 問 51)

WBS (Work Breakdown Structure；作業分割構造) は、システム開発の成果物を作成するためにプロジェクトチームが実行する作業を詳細化し、階層構造で表現したものである。分解した作業のことを要素と呼ぶ。要素分解のレベルに決まりはないが、これらの要素に対して、役割を分担し、責任者を決め、所要時間を見積もるので、それらを管理できるレベルまで分解することが望ましい。したがって、(エ) が適切である。

ア：プロジェクトにおいて、進捗管理及び費用管理を行うトレンドチャートの目的である。

イ：アローダイアグラムを使用する目的である。

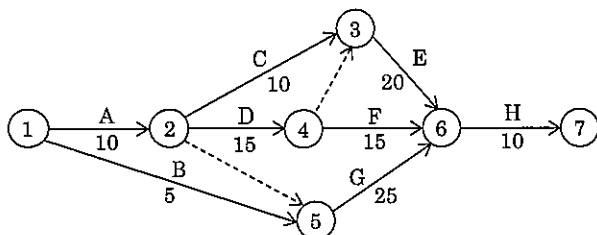
ウ：ガントチャートを使用する目的である。

問 52 エ

プロジェクトの所要日数の計算 (H30 秋・FE 問 52)

問題の図には入っていないが、○の中に数字を入れた次の図で解説する。

②から⑤の点線矢印はダミー作業で、AとBの両方が終わらないと、Gが始まらないことを表している。同様に④から③もダミー作業で、CとDの両方が終わらないとEに進めない。この二つのダミー作業を含めて考えると、図のプロジェクトには五つのパスがあり、所要日数はそれぞれ次のとおりである。



- ・ ①→②→③→⑥→⑦ : $10+10+20+10=50$ 日
- ・ ①→②→④→③→⑥→⑦ : $10+15+20+10=55$ 日
- ・ ①→②→④→⑥→⑦ : $10+15+15+10=50$ 日
- ・ ①→②→⑤→⑥→⑦ : $10+25+10=45$ 日
- ・ ①→⑤→⑥→⑦ : $5+25+10=40$ 日

したがって、①→②→④→③→⑥→⑦がクリティカルパスであり、プロジェクトの所要日数は55日(エ)となる。

問 53 イ

残っている作業量の計算 (H30 秋・FE 問 53)

作業の進捗状況において、全体の工程の何%終了したかを求める問題である。完了予定日や日付時点での進捗状況が示されているが、予定日については全く考慮せずに解答を求めることができる。

計画工数を全て足して全体工数を求めると、

$$2+5+1+4+2+3=17 \text{ 日}$$

残っている作業日は、テスト3日とコンパイル2日と、コーディングの作業のうちの75%(終了したのが25%と問題にある)、つまり4日のうちの3日となり、

$$3+2+3=8 \text{ 日}$$

となる。残っている作業工程は、全体の8日÷17日=0.4705……約47%となる。

したがって、(イ)が正解である。

問 54 エ

プロジェクトに要する全工数の計算 (H30 秋・FE 問 54)

見積り手法であるファンクションポイント法は、開発するシステムに必要な機能 (function) の数を基に開発規模の見積りを行う方法である。この問題では、500 FP (ファンクションポイント) の開発規模と見積もられた新規システム開発について、開発以外の工数も含めた全工数を順に計算していく。

まず、開発規模は 500FP で開発の生産性は 1 人月当たり 10FP とするので、開発工数は $500\text{FP} \div 10\text{FP} / \text{人月} = 50$ 人月となる。

次に、開発工数の他にシステムの導入や開発者教育の工数が 10 人月必要なので、ここまでで合計 $50 + 10 = 60$ 人月必要となる。

更に、プロジェクト管理に、開発と導入・教育を合わせた工数の 10% を要するので、前記 60 人月の 10% に当たる 6 人月を加える必要がある。

したがって、全工数は $60 \text{ 人月} + 6 \text{ 人月} = 66 \text{ 人月}$ となり、(エ) が正解である。

問 55 ア

キャパシティ管理における傾向分析 (H30 秋・FE 問 55)

キャパシティ管理とは、ビジネスが必要とするキャパシティを予測・監視し、最適なコストで改善するプロセスをいい、将来のコンポーネント、並びにサービスの容量・能力及びパフォーマンスを予想する活動は、「ベースラインのモデル化」「傾向分析」「分析モデル化」「シミュレーションのモデル化」の順で実行される。

「傾向分析」とは、データの分布よりも時系列変化を重視して、データの傾向を分析する手法のことである。「特定の資源の利用状況を時系列に把握して、将来における利用の変化を予測する」ことは、時系列変化を重視して、データの傾向を分析しているので、「傾向分析」に該当する。したがって、(ア) が正解である。イ：「待ち行列理論などの数学的技法を利用して、サービスの応答時間及びスループットを予測する」ことは、データの分布よりも時系列変化を重視してデータの傾向を分析していないため、「傾向分析」に該当しない。この選択肢は、数学的技法を利用していることから、「分析モデル化」に該当する。

ウ：「模擬的にトランザクションを発生させて、サービスの応答時間及びスループットを予測する」ことは、データの分布よりも時系列変化を重視してデータの傾向を分析していないため、「傾向分析」に該当しない。この選択肢は、模擬的にトランザクションを発生させていることから、「シミュレーションのモデル化」に該当する。

エ：「モデル化の第一段階として、現在達成されているパフォーマンスを正確に反映したモデルを作成する」ことは、データの分布よりも時系列変化を重視してデータの傾向を分析していないため、「傾向分析」に該当しない。この選択肢は、モデル化の第一段階であること、現在達成されているパフォーマンスを正確に

反映したモデルを作成することから、「ベースラインのモデル化」に該当する。

問 56 イ

システムを初期状態に戻して再開する方法 (H30 秋・FE 問 56)

初期プログラムロードは、最初にコンピュータの電源が投入されたときにプログラムをロードし、かつ実行することであり、「システムを初期状態に戻して再開する」という意味の (イ) の「コールドスタート」が正解である。

ア：ウォームスタートとは、システム障害時に、処理内容を保持してシステム再開時に保持内容を復元して始動することである。

ウ：ロールバック（後進復帰）とは、システム障害時に実行中であったプログラムの更新結果を更新前ログによって実行開始前の状態まで戻すことである。

エ：ロールフォワード（前進復帰）とは、システム障害時に既にコミットしていてディスクデータに更新内容が反映されていない場合、更新後ログを用いてディスクデータを更新することである。

午前解答

問 57 イ

SLA を満たすサービス停止時間の計算 (H30 秋・FE 問 57)

SLA（サービスレベルアグリーメント）条件に含まれている可用性の指標となるものは、全サービス時間に対する IT サービス提供時間の比率であり、次の式で求められる。

$$\text{可用性} = \frac{\text{IT サービス提供時間}}{\text{全サービス時間}} = \frac{\text{全サービス時間} - \text{IT サービス停止時間}}{\text{全サービス時間}}$$

これに SLA の条件に記載のある 1 日の全サービス時間＝14 時間（午前 8 時～午後 10 時）、可用性＝0.995 以上、1 か月＝30 日を適用すると、次のように計算できる。

$$0.995 \leq \frac{14 \text{ 時間} \times 30 \text{ 日} - \text{サービス停止時間}}{14 \text{ 時間} \times 30 \text{ 日}}$$

$$\Rightarrow 0.995 \times 420 \text{ 時間} \leq 420 \text{ 時間} - \text{サービス停止時間}$$

$$\Rightarrow \text{サービス停止時間} \leq 420 \text{ 時間} \times (1 - 0.995) = 420 \text{ 時間} \times 0.005 = 2.1 \text{ 時間}$$

すなわち、サービス停止時間が最大でも 2.1 時間以内であればよいということで、(イ) が正解となる。

問 58 エ

ISMS 内部監査で監査報告書に記載すべき指摘事項 (H30 秋・FE 問 58)

JIS Q 27001:2014（情報セキュリティマネジメントシステム－要求事項）は、情報セキュリティマネジメントシステム（ISMS）を確立し、実施し、維持し、継続的に改善するための要求事項を提供するために作成されたものである。

「情報セキュリティ監査基準 報告基準ガイドライン」には、情報セキュリティ監査報告書の保証報告書の雛形が挙げられており、「われわれの監査は、『情報セキュリティ監査基準』に準拠して行われた。監査は、情報セキュリティに関わるリスクのマネジメントが効果的に実施されるよう、リスクアセスメントに基づいて適切なコントロールが採用されているか否かについて検討し評価している。採用した監査手続は、われわれが必要と認めたものを適用しており、監査の結果として意見表明のための合理的な根拠を得たと確信している」という記載が示されている。また、「情報セキュリティ監査基準 実施基準ガイドライン」において、監査計画立案における監査対象のリスクアセスメントについて、「情報セキュリティ監査人は、監査計画の立案に役立たせるため、リスクアセスメントを実施することが望ましい。監査計画立案段階におけるリスクアセスメントは、重要な監査対象の戦略的決定にとって有益であるばかりでなく、リスクアセスメントの結果を実施すべき監査手続に反映させることによって全体としてメリハリのある監査を期待でき、もって監査目的を有効かつ効率的に達成することにつながる」「被監査側においてリスクアセスメントが行われている場合、情報セキュリティ監査人は、リスクアセスメントの適切性を確かめた上で、被監査側によって実施されたリスクアセスメントの結果を監査計画の立案に活用することができる。被監査側におけるリスクアセスメントの適切性の判定に当たって、情報セキュリティ監査人は、リスクアセスメント手法の厳密性を検証するのではなく、リスク・マッピング等の工夫によって、リスクアセスメントの結果がコントロールと関連づけられたものであることを確かめておくことが重要である」と記載されている。このように、リスクアセスメントを実施し、リスク受容基準を設定することが求められているため、「リスクアセスメントを実施した後に、リスク受容基準を決めた」ことは、監査人が指摘事項として監査報告書に記載すべきものである。したがって、(エ)が正解である。

ア：「情報セキュリティ監査基準」には、監査報告書の記載事項として、「監査報告書には、実施した監査の対象、実施した監査の概要、保証意見又は助言意見、制約又は除外事項、その他特記すべき事項について、情報セキュリティ監査人が監査の目的に応じて必要と判断した事項を明瞭に記載しなければならない」と記載されている。「USBメモリの使用を、定められた手順に従って許可していた」ことは、情報セキュリティ監査報告書において、実施した監査手続及び項目の全てを列記することは現実的でないばかりか、監査報告書読者の混乱を招く結果ともなりかねないため、監査報告書に記載すべきものではない。

イ：(ア)と同様の理由で、「個人情報の誤廃棄事故を主務官庁などに、規定されたとおりに報告していた」ことは、監査報告書に記載すべきものではない。

ウ：(ア)と同様の理由で、「マルウェアスキャンでスパイウェアが検知され、駆除されていた」ことは、監査報告書に記載すべきものではない。

問 59 エ

セキュリティ監査の報告で記載すべき指摘事項 (H30 秋・FE 問 59)

情報やソフトウェアを格納した媒体の配送に関する情報セキュリティの監査については、JIS Q 27001 (情報セキュリティマネジメントシステム—要求事項) の付属書にある管理策が参考になる。この管理策の中では、「情報を格納した媒体は、組織の物理的境界を越えた配送の途中における、認可されていないアクセス、不正使用、又は破損から保護しなければならない」と規定されている。このような保護のためには、梱包を十分な強度に保つとともに、鍵のかかる容器 (コンテナ) の使用を考慮すべきである。バックアップ媒体を単にダンボール箱に入れた状態で業者に引き渡すのは、強度及び不正使用の両面から問題である。したがって、指摘事項となる状況は (エ) である。

そのほかの選択肢は、それぞれ次のとおり正しい対応なので監査人が指摘事項として監査報告書に記載すべきものとは言えない。

ア：媒体保管状況は定期的に確認するべきである。

イ：外部への委託契約には必要に応じて機密保持条項を盛り込むことが望ましい。

ウ：媒体引渡し時には記録簿に日付や内容を記録して相手先からの確認印を押印してもらうべきである。

問 60 エ

内部統制の整備及び運用に最終責任を負う者 (H30 秋・FE 問 60)

内部統制とは、健全かつ効率的な組織運営のための体制を企業などが自ら構築し運用する仕組みのことであり、経営者をはじめとする組織内部の構成員がこの仕組みを適切に運用することで、内部統制の目的が達成される。

企業会計審議会「財務報告に係る内部統制の評価及び監査の基準並びに財務報告に係る内部統制の評価及び監査に関する実施基準の改訂について (意見書)」(平成 23 年 3 月 20 日) における「財務報告に係る内部統制の評価及び監査の基準」によると、内部統制に関係を有する者の役割と責任について、「経営者は、組織のすべての活動について最終的な責任を有しており、その一環として、取締役会が決定した基本方針に基づき内部統制を整備及び運用する役割と責任がある」と記載されている。このように、内部統制の整備及び運用に最終的な責任を負っている者は、経営者である。したがって、(エ) が正解である。

ア：株主は、会社の所有主であり、内部統制の整備及び運用に最終的な責任を負ってはいない。よって、株主は、内部統制の整備及び運用に最終的な責任を負っている者としては不適切である。

イ：「財務報告に係る内部統制の評価及び監査の基準」によると、「監査役又は監査委員会は、取締役及び執行役の職務の執行に対する監査の一環として、独立した立場から、内部統制の整備及び運用状況を監視、検証する役割と責任を有している」と記載されている。よって、監査役は、内部統制の整備及び運用に最終的な責任を負っている者としては不適切である。

ウ：「財務報告に係る内部統制の評価及び監査の基準」において、「例えば、日常的モニタリングとして、各業務部門において帳簿記録と実際の製造・在庫ないし販売数量等との照合を行うことや、定期的実施される棚卸手続において在庫の残高の正確性及び網羅性を関連業務担当者が監視する」という記述があるように、業務担当者は内部統制の運用を実施する者であって、内部統制の整備及び運用に最終的な責任を負っていない。よって、業務担当者は、内部統制の整備及び運用に最終的な責任を負っている者としては不適切である。

問 61 エ

IT 投資評価における事前評価の説明 (H30 秋・FE 問 61)

IT 投資の費用対効果の判断の目安となる「IT 投資価値評価ガイドライン」が経済産業省によって公開されている。そこでは、システムの開発プロジェクトの各段階において、投資価値の判断のためにチェックすべき評価項目が設定されており、おおむね次のようになる。

・事前評価（計画→構想・企画段階）

投資の実行を決断するための投資効果及び経営戦略との適合性の評価

・中間評価（実施→開発実行段階）

開発段階における適合性確認のため、事前評価によって計画された投資内容に沿った実行結果が得られているかの評価

・事後評価（完了→開発完了後、稼働後の一定時期）

プロジェクトの終末段階において、システム稼働後に予定された効果が得られているかどうかを判断するための投資効果の評価

これらの内容から、事前評価は投資を実施する前に効果目標を設定し、経営戦略との適合性を評価するための実施可否判断に必要な情報を上位マネジメントに提供するという（エ）が正解である。

ア：「投資額や効果目標の変更が必要かどうかを判断する」とあり、中間評価についての説明である。

イ：「必要に応じて目標を達成するための改善策を検討する」とあり、中間評価についての説明である。

ウ：「その時期（投資効果の実現時期）に合わせて評価を行う」とあり、事後評価についての説明である。

問 62 ウ

BPO の説明 (H30 秋・FE 問 62)

BPO（ビジネスプロセスアウトソーシング）とは、経営資源をコアビジネスに集中させるために、企業などがコアビジネス以外の業務の一部又は全部を、外部の専門業者に委託することである。自社の管理部門が行っている業務やコールセンタなど特定業務の業務プロセス全般を、業務の遂行に必要となる業務システム

の運用などとともに外部の専門業者に委託することで、賃金コストや運用コスト、教育コストなどの削減を図る。したがって、(ウ)が正解である。

ア：レンタルサーバに関する記述である。

イ：SaaS (Software as a Service) に関する記述である。

エ：派遣会社を活用した賃金コストの削減に関する記述である。

問 63 イ

SOAの説明 (H30 秋・FE 問 63)

午前解答

SOA (Service Oriented Architecture) とは、大規模なシステムをサービスの集合として構築する設計手法である。ビジネスプロセス上の独立した業務機能をサービスとしてとらえ、インタフェースが共通化された部品単位で情報システムを構築する。将来におけるシステム構成の変更や今後の他の情報システム開発の場面などにおいて、部品単位での変更や部品の再利用・組合せを行うことによって要求を容易に実現することができるメリットがある。よって、サービスというコンポーネント (部品) からソフトウェアを構築することによって、ビジネス変化に対応しやすくすることが可能となる。したがって、(イ)が正解である。

ア：エンタープライズアーキテクチャ (EA) についての記述である。EA とは、効率の良い組織運営と業務の最適化のために、経済産業省がまとめた業務とシステムの最適化計画であり、あるべき姿の組織の構造と機能を包括的に設計するための全社的な情報化計画に関する情報化の指針となる。

ウ：トム・デマルコなどが提唱した構造化分析設計についての記述である。データフローダイアグラム (DFD) は、業務に必要な情報 (データ) の流れに注目して業務をモデル化する図法である。構造化分析設計では、DFD 以外にデータディクショナリ、ミニ仕様書なども併用する。

エ：構造化プログラミングについての記述である。構造化プログラミングは、連接、選択、反復の三つの論理構造による構造化定理に基づいて行うモジュール論理設計である。基本構造を守ってプログラミングする制約はあるが、プログラムは理解しやすい形で作成されるため、保守しやすいプログラムとなる。

問 64 イ

システム化計画の立案 (H30 秋・FE 問 64)

システム化計画については、独立行政法人 情報処理推進機構 (IPA) が発行している「共通フレーム」に記載されている。「共通フレーム」とは、ソフトウェアの構想から開発、運用、保守、廃棄に至るまでのライフサイクルを通じて必要な作業項目、役割などを包括的に規定した共通の枠組みであり、何を実施するべきかが記述されている「IT システム開発の作業規定」である。

「システム化計画の立案」は、システム化構想を具体化するために、対象業務について運用や効果などの実現性を考慮したシステム化計画及びプロジェクト計画を具体化し、利害関係者の合意を得るプロセスである。「システム構築の組織体

制を策定するとき、業務部門、情報システム部門の役割分担を明確にし、費用の検討においては開発、運用及び保守の費用の算出基礎を明確にしておくことは、対象業務のシステム化による新業務モデル策定、その実現可能性と費用対効果の明確化、プロジェクト推進体制の決定を行うものである。「システム化計画の立案プロセス」で実施すべき項目である。したがって、(イ)が正しい。

ア:「画面や帳票などのインタフェースを決定し、設計書に記載するために、要件定義書を基に作業する」ことは、新たに構築するシステム化の範囲を明確にし、システムがもつべき要件を列挙・検討して利害関係者間で合意する目的を有する「要件定義プロセス」で実施すべき事項である。

ウ:「システムの起動・終了、監視、ファイルメンテナンスなどを計画的に行い、業務が円滑に遂行していることを確認する」ことは、完成したシステムが意図された環境で安定して稼働するためのプロセスである「運用プロセス」で実施すべき事項である。

エ:「システムを業務及び環境に適合するように維持管理を行い、修正依頼が発生した場合は、その内容を分析し、影響を明らかにする」ことは、システムを改善・変更する作業である「保守プロセス」で実施すべき事項である。

問 65 ア

要件定義プロセスで実施すべきもの (H30 秋・FE 問 65)

システム開発プロセスの標準化を目的とした共通フレーム 2013 では、要件定義プロセスの中で、利害関係者の識別や、要件の識別、要件の抽出、制約条件の定義といったアクティビティ (活動) が掲げられている。したがって、(ア)が正解である。

イ:企画プロセスの中のプロセス実施計画の作成アクティビティで行うべき内容である。

ウ:システム方式設計プロセスの中のシステム方式の確立アクティビティで行うべき内容である。

エ:ソフトウェア方式設計プロセスの中のソフトウェア方式設計の評価及びレビューアクティビティで行うべき内容である。

問 66 イ

情報システムの調達手順 (H30 秋・FE 問 66)

RFP (Request For Proposal ; 提案依頼書) とは、発注元が調達先に提出する提案書の依頼文書である。導入を希望する情報システムの目的や概要、システム要件、必要とする機能やサービスレベルなどの仕様や調達条件などが記載される。システム開発を依頼する前の段階として、この RFP によってシステム開発上の重要事項について書面によって明確化し、RFP を受け取ったシステムベンダ側 (調達先) は、これを基にユーザ側 (発注元) に対して提案書を作成して、ユーザ側の了承を経てから契約を締結する。したがって、(イ)が正解である。

ア：RFI (Request For Information；情報提供依頼書)とは、情報システムの導入の検討段階において、ユーザ側が新技術や新規格、最新のマネジメント分野の動向などに関する情報を得る目的で、システムベンダに対して情報提供を求めるために発行される文書である。空欄 a には「情報提供を依頼する」とあることから、RFI が入る。

ウ：「調達先を決定する」ことから、供給者の選定は空欄 c に入る。

エ：「文書で相互に確認する」ことから、契約の締結は空欄 d に入る。

問 67 ア

プロダクトライフサイクルの成長期 (H30 秋・FE 問 67)

プロダクトライフサイクルは、商品の誕生から市場の拡大、そして衰退に至る過程を、導入期、成長期、成熟期 (市場飽和期)、衰退期の四つに分類する考え方である。このうち、成長期の特徴としては、市場が成長すること、すなわち、市場規模の拡大が続いていることにある。すると、拡大した市場によって、市場が商品の価値を理解し始める。また、引き続き市場が拡大していくため、製品の種類や販売チャネルを増やすための投資も必要となってくる。したがって、(ア)が正解である。

参考までに、プロダクトライフサイクルの時間を横軸に、売上高を縦軸にした売上曲線は、一般に次のようになる。

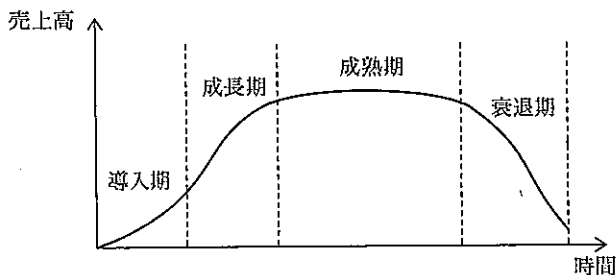


図 プロダクトライフサイクル

イ：成熟期 (市場飽和期) の特徴である。

ウ：衰退期の特徴である。

エ：導入期の特徴である。

問 68 エ

需要数の計算 (H30 秋・FE 問 68)

設定価格と需要の関係は 1 次式で表せるとあるので、それぞれの変化量が比例関係にあることになる。(1)、(2)の記述から、設定価格が 3,000 円から 1,000 円になると、需要は 0 個から 60,000 個になることから、比例関係で考えると、設定

価格 2,000 円は 3,000 円と 1,000 円の平均値であり、そのときの需要は 0 個と 60,000 個の平均値で 30,000 個になると予想できる。

更に、設定価格 1,000 円と 2,000 円の平均値である 1,500 円を考えると、需要は 30,000 個と 60,000 個の平均値の 45,000 個になると予想できる。したがって、(エ) が適切である。

参考までに、設定価格を x 、需要を y として、近似する 1 次式 $y=ax+b$ を求めると、次のようになる。

(1), (2)をそれぞれこの式に当てはめると、

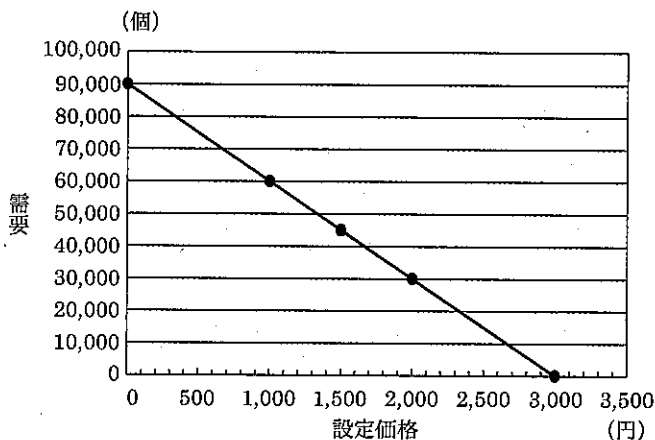
$$0=3,000a+b \quad \cdots\cdots\textcircled{1}$$

$$60,000=1,000a+b \quad \cdots\cdots\textcircled{2}$$

となる。この連立 1 次方程式から係数 a 、 b を求めると、 $\textcircled{1}$ から $b=-3,000a$ となり、これを $\textcircled{2}$ の b に代入すると、 $60,000=1,000a+(-3,000a)$ から、 $a=-30$ となる。更に、 $a=-30$ を $\textcircled{1}$ の式に代入すると、 $b=90,000$ となる。

以上から、1 次式は $y=-30x+90,000$ と表すことができ、設定価格 x に 1,500 を代入すると、 $y=45,000$ となる。

二つの関係をグラフにすると、次のようになる。



問 69 工

購入見込み人数の試算表 (H30 秋・FE 問 69)

顧客が新商品を購入する割合と新規顧客数の試算に関する問題である。表の値と、それぞれの項目の内容を突き合わせることで、正解を求めることができる。

まず、正解となる (エ) の項目に人数を当てはめると、新商品 S の新規顧客数は 23,000 人、商品 C の購入者のうち商品 S を購入する人数は、 $80,000 \times 0.3 = 24,000$ 人となる。

したがって、

(新商品 S の新規顧客数) < (商品 C の購入者のうち商品 S を購入する人数) となり、(エ) が適切である。

ア：商品 A の購入者のうち、新商品 Q を購入すると予想できるのは、 $10,000 \times 0.3 = 3,000$ 人である。よって、新商品 Q を購入すると予想している 1,000 人と異なる。

イ：商品 B の購入者が、新商品 P, Q, R, S のどれかを購入するには、新商品 P, Q, R, S の購入割合の合計が全体 (1.0) を示している必要がある。表から新商品 P, Q, R, S 購入割合の合計は 0.9 なので商品 B の購入者が、新商品 P, Q, R, S のどれかを購入することにはならない。

ウ：新商品 P の購入見込者のうち、商品 A の購入者の割合は、

$$\frac{10,000 \times 0.5}{15,000 + 5,000} \times 100 = 25 \text{ (％)} \text{ で 5 割 (50％) ではない。}$$

問 70 ア

技術進化過程を表すもの (H30 秋・FE 問 70)

技術進化過程の特性 (開発の成果) を導入期、成長期、成熟期、衰退期のフェーズで表すと、次の図のような曲線で示すことができる。

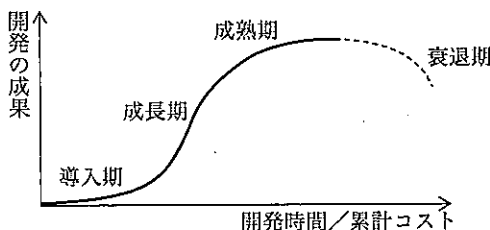


図 A 技術の S カーブ

曲線は、最初は緩やかに立ち上がり、ある段階で急速に進歩する。その後の成熟段階になると徐々に限界に近づいていくが、この段階で他の技術が成長してくると、旧来の技術は省みられなくなる。この導入期から成熟期を経て限界に達するまでのカーブが S 字に似ているので、技術の S カーブと呼ばれている。したがって、(ア) が正解である。

イ：需要曲線は、商品の価格と需要量の関係を表したものである。一般に、価格が高いと需要量は少なく、価格が安くなると需要量が増える。これに、価格と供給の関係を表した供給曲線を加えたものが需要・供給曲線である。

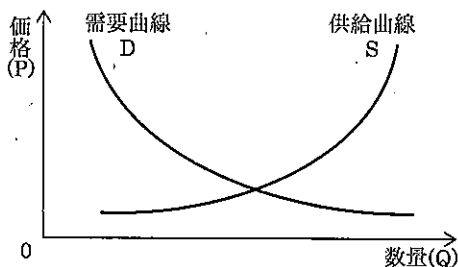


図 B 需要・供給曲線

ウ：バスタブ曲線は、ハードウェア故障発生率と使用時間の関係を示したもので、その形状から初期故障期間、偶発故障期間、摩耗故障期間の三つのフェーズに分けられる。

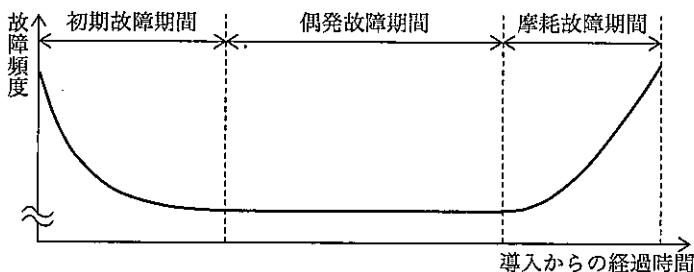


図 C バスタブ曲線

エ：ラーニングカーブ（学習曲線あるいは経験曲線あるいは習熟曲線）は、学習時間と、その成果との関係を示したものである。学習時間（量）が増えるにつれて、経験則が上がり、効率が高まっていくということが表れている。一般的に、最初はなかなか成果が表れず、徐々に成果が表れてきて、その後、成果の伸びが少なくなってくるため S 字の形状を示す。この曲線も S カーブと呼ばれることがある。

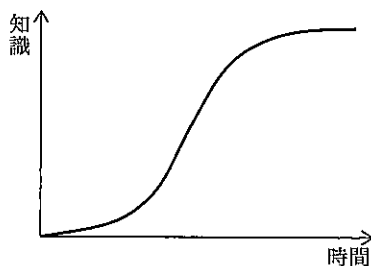


図 D ラーニングカーブ

問 71 イ

IoT の構成要素 (H30 秋・FE 問 71)

IoT (Internet of Things:モノのインターネット) とは、様々なモノがインターネットなどに接続され、情報を交換することによって相互に制御する仕組みの

ことをいう。総務省『平成 27 年版情報通信白書 特集テーマ「ICT の過去・現在・未来」』によると、「IoT のコンセプトは、自動車、家電、ロボット、施設などあらゆるモノがインターネットにつながり、情報のやり取りをすることで、モノのデータ化やそれに基づく自動化等が進展し、新たな付加価値を生み出すというものである」とある。

IoT は、機器、ゲートウェイ、サーバという 3 つの要素から構成されており、各構成要素間を繋ぐネットワークが存在している。よって、IoT の構成要素は、「インターネット又は閉域網に接続できる全てのものが対象となる」。したがって、(イ) が正解である。

ア：「アナログ式の機器を除く、デジタル式の機器が IoT の構成要素の対象となる」ということであれば、例えば、フィルム式ではない、デジタル式のカメライは IoT ということになる。しかし、単なるデジタル式のカメラが存在するだけでは、IoT とはいえない。インターネットなどに接続され、情報を交換することによって相互に制御する仕組みを有していないからである。よって、記述は適切とはいえない。

ウ：「自律的にデータを収集してデータ分析を行う機器だけが IoT の構成要素の対象となる」ということであれば、例えば、ドアに装着するだけで、スマートフォンでドアの鍵の開け閉めができるスマートロックは、自律的にデータを収集してデータ分析をしているわけではないので、IoT ではないということになる。しかし、この事例は、IoT といえる。インターネットなどに接続され、情報を交換することによって相互に制御する仕組みを有しているからである。よって、記述は適切とはいえない。

エ：「人や生物を除く、形のある全てのものが IoT の構成要素の対象となる」ということであれば、例えば、鉛筆は IoT ということになる。しかし、単なる鉛筆が存在するだけでは、IoT とはいえない。インターネットなどに接続され、情報を交換することによって相互に制御する仕組みを有していないからである。よって、記述は適切とはいえない。

問 72 エ

IC タグ (RFID) の特徴 (H30 秋・FE 問 72)

IC タグ (RFID ; Radio Frequency IDentification) は、小さい IC チップを埋め込んだタグ (荷札) であり、至近距離の無線通信による情報のやり取りで内容の読み書きが可能なものである。

現在の主流はパッシブタイプといわれるもので、タグ自体に電源はないが、リーダーが放射する電波を受信し、それを利用して電流を発生させ、情報の処理と発信ができるようになっている。従来のバーコード方式に比べて、記憶情報量が大きく非接触式なので、見えない位置でも、汚れがあっても、読取りと書き込みが可能という長所がある。したがって、(エ) が正解である。

ア：GPS (Global Positioning System ; 全地球測位システム) では、複数の GPS

衛星から電波信号を受信して現在地の位置を計算するが、受信し表示するものは、GPS 受信機とこれに接続する表示装置で、IC タグとは関係ない。

イ：挿入型の IC カード（チップカード、スマートカード）の説明である。IC タグは、読取り装置への挿入を必要とする、というものではない。

ウ：IC タグは、情報を IC チップに内蔵するのが特徴で、外部記憶装置は使用しない。

問 73 エ

ネットビジネスでの O to O (H30 秋・FE 問 73)

ネットビジネスでの O to O は「Online to Offline」の略であり、ネット上（オンライン）からネット外の実地（オフライン）での行動を促したり、ネット外の実地（オフライン）からネット上（オンライン）での行動を促したりする仕組みのことである。

O to O の事例としては、実店舗をもつ飲食店が、スマートフォンを通じオンラインで割引クーポンやサービス追加クーポンを提供したり、テレビのコマーシャルにおいて「続きは Web でご覧になれます」といった誘導や、電車内広告における「詳しくは『〇〇』で検索」といったような誘導をしたりするものなどが挙げられる。このように、「モバイル端末などを利用している顧客を、仮想店舗から実店舗に、又は実店舗から仮想店舗に誘導しながら、購入につなげる仕組み」が、ネットビジネスでの O to O である。したがって、(エ) が正解である。

ア：「基本的なサービスや製品を無料で提供し、高度な機能や特別な機能については料金を課金するビジネスモデル」は、「フリーミアム (Freemium)」である。これは、「フリー」(Free, 無料) と「プレミアム」(Premium, 割増) を合わせて作られた造語である。

イ：「顧客仕様に応じたカスタマイズを実現するために、顧客からの注文後に最終製品の生産を始める方式」は、「BTO (Build To Order)」である。事例としては、パソコンメーカーであるデルのビジネスモデル（デル・ダイレクト・モデル）が有名である。

ウ：「電子商取引で、代金を払ったのに商品が届かない、商品を送ったのに代金が支払われないなどのトラブルが防止できる仕組み」は、「エスクローサービス」である。これは、商取引の安全性を保証する仲介サービスで、エスクローとは第三者預託を意味する。

問 74 エ

CIO の説明 (H30 秋・FE 問 74)

CIO (Chief Information Officer；情報統括役員、最高情報責任者) は、企業内の情報システムや情報の流通を統括し、情報戦略のトップの立場にある。情報化戦略の立案だけではなく、情報を基に CEO (Chief Executive Officer；最高経営責任者) から経営陣に対して適切な報告・助言を行うことも求められ、経営戦略

に関する理解と能力が必要となる。したがって、(エ)が正解である。

ア：CEO (Chief Executive Officer; 最高経営責任者)の説明である。業務執行だけを行う、COO (Chief Operating Officer; 最高執行責任者)との違いは、経営戦略の立案に携わるかどうかであるが、実際には明確な区別はなく CEO が対外的な企業のトップ、COO は社内の業務部門のトップというケースが多い。

イ：CFO (Chief Financial Officer; 財務担当役員、最高財務責任者)の説明である。

ウ：CTO (Chief Technology Officer; 技術担当役員、最高技術責任者)の説明である。

問 75 ウ

利益の期待値が最大になる仕入個数 (H30 秋・FE 問 75)

問題の表の見方であるが、左の「仕入個数」が4個から7個と変動する場合、上の「販売個数」が4個から7個になる予想確率を示している。例えば仕入個数が4個であれば、4個以上売れる可能性は0なので、販売個数4個となる予想確率が100%である。言い換えると4個は絶対に売り切る自信があるということである。これに対して5個を仕入れた場合は4個しか売れない確率は30%であり、70%の確率で5個売り切る自信があることを示している。同様に仕入個数が増えると増えた分の個数も売り切る可能性が少なからずある、ということを示している。

利益の期待値が最大になる仕入個数を求める問題である。仕入個数ごとに、販売個数単位で売残りの廃棄ロスを差し引いて、販売確率を掛けた合計を比較することによって特定できる。問題の表から、個別に利益の期待値を求めると次のようになる。

4 個の場合… $4 \times 1,000 \text{ 円} = 4,000 \text{ 円}$

5 個の場合… $((4 \times 1,000 \text{ 円} - 300 \text{ 円}) \times 0.3) + ((5 \times 1,000 \text{ 円}) \times 0.7) = 4,610 \text{ 円}$

6 個の場合… $((4 \times 1,000 \text{ 円} - 300 \text{ 円} \times 2) \times 0.3) + ((5 \times 1,000 \text{ 円} - 300 \text{ 円}) \times 0.3) + ((6 \times 1,000 \text{ 円}) \times 0.4) = 4,830 \text{ 円}$

7 個の場合… $((4 \times 1,000 \text{ 円} - 300 \text{ 円} \times 3) \times 0.3) + ((5 \times 1,000 \text{ 円} - 300 \text{ 円} \times 2) \times 0.3) + ((6 \times 1,000 \text{ 円} - 300 \text{ 円}) \times 0.3) + ((7 \times 1,000 \text{ 円}) \times 0.1) = 4,660 \text{ 円}$

したがって、(ウ)が正解である。

問 76 ウ

連関図法 (H30 秋・FE 問 76)

連関図法は、構成要素の因果関係を明らかにしたり、解決策を導き出したりするのに用いられる。複雑に絡み合う原因と結果を矢印で結んでいく。矢印の方向によって、原因結果型、目的手段型に分けられる。「新 QC 七つ道具」の一つである。したがって、(ウ)の説明が正解である。

- ア：PDPC（Process Decision Program Chart）法に関する記述である。「新 QC 七つ道具」の一つである。目的達成までのプロセスを改善する方策を考える。
- イ：親和図法に関する記述である。収集した情報や課題などの対象物をグループ化し、グループごとに解決すべき課題を明確にする。「新 QC 七つ道具」の一つである。
- エ：系統図法に関する記述である。目的・目標とその手段について、抽象的なものから具体的なものへと展開していくことで、最適手段・方策を求めていく。「新 QC 七つ道具」の一つである。
- ・新 QC 七つ道具：従来の「QC 七つ道具」は、数値を用いて製品の品質を一定に保つための分析方法であった。新 QC 七つ道具は、やはり製品の品質を一定に保つための分析方法であるが、漠然とした問題を解決するための道具で、データとして数値よりも言語を用いるものが多い。（ア）～（エ）の他に、マトリックス図、マトリックスデータ解析、アローダイアグラムがある。

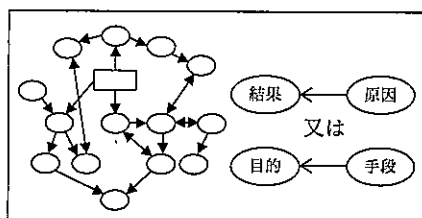


図 A 連関図法

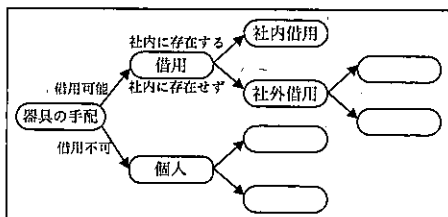


図 B PDPC 法

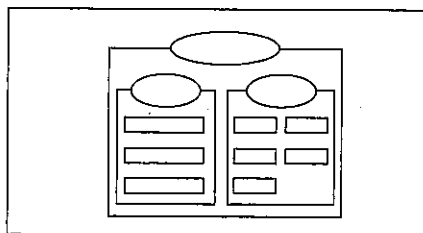


図 C 親和図法

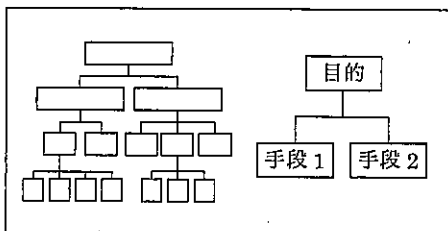


図 D 系統図法

問 77 イ

先入先出法による売上原価の計算 (H30 秋・FE 問 77)

売上原価とは、仕入の合計ではなく、売上分の仕入値合計のことである。そして、同じ商品に関する仕入と売上が数回にわたって行われ、その際に値段が毎回違う場合、売上個数の元になる仕入個数をどのように対応付けていくか、いわゆる消込みをどう行うか、という観点で会計処理としては先入先出法がシンプルであり、試験問題としてもよく出題される。先入先出法は、先に仕入れたものから先に売れたと考えて原価を算出する方法である。売上原価の算出法としてこの他

に、先入先出法の逆の後入先出法や、仕入の都度、平均原価を計算し直す移動平均法がある。

当年度の売上の合計数量は $70+60=130$ 個ある。これを仕入れた順に商品を割り当て、原価を計算する（先入先出法）。

まず、100 個については、前月繰越分から割り当て、その原価は $200 \text{ 円} \times 100 \text{ 個} = 20,000 \text{ 円}$ 、残りの 30 個は 5 日に仕入れた 50 個の中から割り当てるので、原価は $215 \text{ 円} \times 30 \text{ 個} = 6,450 \text{ 円}$ となる。したがって、130 個分の原価は、 $20,000 + 6,450 = 26,450 \text{ 円}$ となり、(イ) が正解である。

問 78 ア

コンピュータウイルスを作成する行為を処罰する法律 (H30 秋・FE 問 78)

コンピュータウイルスを作成する行為を処罰の対象とする法律は刑法である。これは刑法第 168 条の 2 第 1 項の不正指令電磁的記録作成・提供罪に当たり、正当な理由なく、コンピュータウイルスを作成する行為を処罰の対象としている。一般的には、ウイルス作成罪と呼ばれ、3 年以下の懲役又は 50 万円以下の罰金が科せられる。したがって、(ア) が正解である。

2011 年 7 月に「情報処理の高度化等に対処するための刑法等の一部を改正する法律」が施行され、法務省はこれを通称「サイバー刑法」と呼んでいる。

イ：不正アクセス禁止法とは、「不正アクセス行為」と「不正アクセス行為を助長する行為」を禁止する 2000 年 2 月に施行された法律である。具体的には「ID・パスワードの不正な使用」や「そのほかの攻撃手法」によってアクセス権限のないコンピュータ資源へアクセスすることを禁止している。

ウ：不正競争防止法とは、公正な競争と国際約束の的確な実施を確保するため、不正競争の防止を目的として設けられた法律である。

エ：プロバイダ責任制限法（特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律）とは、Web サイトの掲示板に個人のプライバシーを侵害する書き込みがあった場合などの事例に対し、プロバイダや掲示板の運営者の責任範囲を定めた法律である。

問 79 エ

個人情報に該当しないもの (H30 秋・FE 問 79)

個人情報保護委員会「個人情報の保護に関する法律についてのガイドライン（通則編）平成 28 年 11 月（平成 29 年 3 月一部改正）」によると、第 2 条第 1 項に、個人情報の定義について次のように規定されている。

「この法律において『個人情報』とは、生存する個人に関する情報であつて、次の各号のいずれかに該当するものをいう。

- (1) 当該情報に含まれる氏名、生年月日その他の記述等（文書、図画若しくは電磁的記録（電磁的方式（電子的方式、磁気的方式その他の人の知覚によっては認識することができない方式をいう。次項第 2 号において同じ。）で作ら

れる記録をいう。第 18 条第 2 項において同じ。)に記載され、若しくは記録され、又は音声、動作その他の方法を用いて表された一切の事項(個人識別符号を除く。)をいう。以下同じ。)により特定の個人を識別することができるもの(他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。)

(2) 個人識別符号が含まれるもの」

この規定によると、「匿名加工情報に加工された利用者アンケート情報」は、匿名に加工することによって特定の個人を識別することができないようにしてあるものであるため、前記のガイドラインにおける「特定の個人を識別することができるもの」ではないので、個人情報には該当しない。したがって、(エ)が正解である。

ア:「受付に設置した監視カメラに録画された、本人が判別できる映像データ」は、前記ガイドラインの規定における「動作その他の方法を用いて表された一切の事項により特定の個人を識別することができるもの」であるため、個人情報に該当する。なお、前記のガイドラインには、個人情報に該当する事例として、「事例 3) 防犯カメラに記録された情報等本人が判別できる映像情報」という記載がある。

イ:「個人番号の記載がない、社員に交付する源泉徴収票」は、個人番号の記載がないものであっても、社員名が記載されているものであることから、前記のガイドラインの規定における「特定の個人を識別することができるもの」であるため、個人情報に該当する。

ウ:「指紋認証のための指紋データのバックアップデータ」は、個人識別符号に該当し、指紋を認証し、他の情報と容易に照合することができ、それによって特定の個人を識別することができる。そのため、前記ガイドラインの規定における「特定の個人を識別することができるもの」であり、個人情報に該当する。なお、個人情報の保護に関する法律第 2 条第 2 項に、「個人識別符号」について、「特定の個人の身体の一部の特徴を電子計算機の用に供するために変換した文字、番号、記号その他の符号であって、当該特定の個人を識別することができるもの」と規定されており、政令(個人情報の保護に関する法律施行令:平成 15 年政令第 507 号)第 1 条第 1 項に「指紋又は掌紋」が挙げられている。

問 80 ア

請負契約でも派遣とみなされる受託者の行為 (H30 秋・FE 問 80)

請負契約は、当事者の一方が仕事を完成させることを約束し、相手方が仕事の結果に対して報酬を支払うことを約束する契約である(民法第 632 条)。ここでは、発注者側は仕事の結果としての製品やサービスを受け入れる立場であり、受託者側はその仕事を行う労働者を雇用して雇用契約に基づいて管理する。したがって、作業の指示や労働者の評価、職場秩序の維持などは全て受託企業の責任事項となる。一方、派遣契約は自企業の雇用する労働者を他企業のために労働に従

事させる契約で、受託者は作業の完成を約束するのでなく労働者の派遣を約束する。派遣労働者は派遣先の指揮命令に従って作業することになり、労働場所や就業時間その他の労働条件は必要に応じて派遣契約の内容に取り入れて両社で決める（労働者派遣法）。休暇取得ルールは雇用契約に伴う就業条件であり、請負契約なら請負作業の受託者側の責任で決めればよいので、雇用関係がない発注者側には発言権はない。請負契約を締結しながら労働者の休暇取得ルールを発注者側の指示に従って取り決めているとすると、労働者を雇用している受託者側で管理すべき労働条件を発注者側で指示しているので、請負契約といいながら実態は派遣契約の方法で運用していることになる。したがって、(ア)が正解である。このような運用は偽装派遣と呼ばれ、請負契約があったとしても法律上は労働者派遣とみなされる。

イ：請負業務の受託者が自己の雇用する労働者指導や評価を行うのは当然である。

ウ：請負業務の受託者が職場規律や職場秩序の保持に努めるのは当然である。

エ：請負業務では発注者側の要請は受託者側の責任者が窓口となって受け付けることになる。

●平成 30 年度秋期

午後問題 解答・解説

問1 情報セキュリティ事故と対策（情報セキュリティ）

（H30 秋・FE 午後問 1）

【解答】

〔設問 1〕 ウ

〔設問 2〕 a-エ, b-ア, c-エ

〔設問 3〕 イ

【解説】

公開サーバの Web アプリケーションソフト（本問では Web アプリ）への攻撃、及びセキュリティ対策をテーマとした出題である。「SQL インジェクション」、「クロスサイトスクリプティング」、「WAF」などのセキュリティの専門的な言葉が数多く登場する。しかし、これらはいずれも基本情報技術者試験の出題範囲に含まれる用語である。なお、表 1 の「ブレースホルグ」は、「?」などの特別な文字列を使って SQL 文を完成させる SQL インジェクション対策である。

この問題は、難易度は標準的と言えるが、たとえ難しい問題であっても、4 択という利点を生かし、基礎知識を使って消去法で正解を導くテクニックも活用して、合格ラインを突破してほしい。

さて、設問の解説に入る前に、問題文から想定される A 社のシステム構成図を図 A に示す。構成図をイメージしながら設問を解くことは重要である。

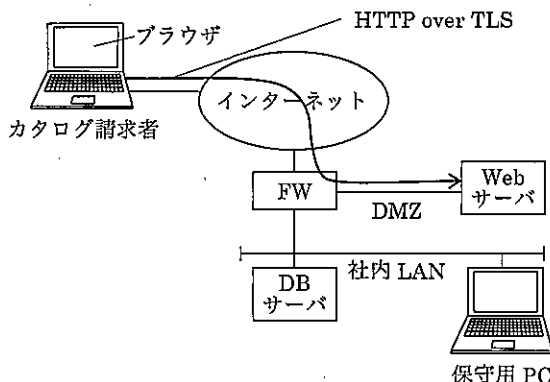


図 A A 社のシステム構成図