

平成 18 年度 春期

テクニカルエンジニア（エンベデッドシステム） 午前 問題

注意事項

1. 試験開始の合図があるまで、問題冊子を開いて中を見てはいけません。
2. この注意事項は、問題冊子の裏表紙に続きます。問題冊子を裏返して必ず読んでください。
3. 答案用紙への受験番号などの記入及びマークは、試験開始の合図があってから始めてください。
4. 試験時間は、次の表のとおりです。

試験時間	9:30 ～ 11:10 (1 時間 40 分)
------	--------------------------

途中で退出する場合には、手を挙げて監督員に合図し、答案用紙が回収されてから静かに退出してください。

退出可能時間	10:30 ～ 11:00
--------	---------------

5. 問題は、次の表に従って解答してください。

問題番号	問 1 ～ 問55
選択方法	全問必須

6. 問題に関する質問にはお答えできません。文意どおり解釈してください。
7. 問題冊子の余白などは、適宜利用して構いません。
8. 電卓は、使用できません。

注意事項は問題冊子の裏表紙に続きます。
こちら側から裏返して、必ず読んでください。

問1 DDR-SDRAM の特徴として、適切なものはどれか。

- ア クロック信号の立ち上がりと立ち下りの両方に同期して、データを読み出す。
- イ 高速ページモード DRAM のページアクセスのサイクル時間を短くして、より高速にデータ転送する。
- ウ メモリセルからデータを読み出すとき、一度だけ行アドレスを指定した後、列アドレスを変えながら複数のデータを行バッファから高速に読み出す。
- エ メモリバスクロックに同期して、1クロックにつき一つのデータを読み出す。

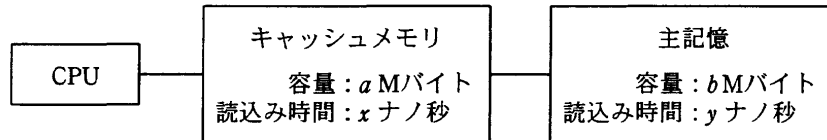
問2 パイプライン制御における遅延分岐の記述として、適切なものはどれか。

- ア 分岐しない方向の命令を先読みしておき、分岐するときには先読みしたものをキャンセルする。
- イ 分岐する方向の命令を先読みしておき、分岐しないときには先読みしたものをキャンセルする。
- ウ 分岐する方向を予測し、予測した方向の命令をあらかじめ実行しておく。
- エ 分岐命令に引き続く幾つかの命令を実行してから実際の分岐を行う。

問3 1 件のトランザクションについて 80 万ステップの命令実行を必要とするシステムがある。プロセッサの性能が 20 MIPS で、プロセッサの使用率が 80%のときのトランザクションの処理能力（件／秒）は幾らか。

- ア 2 イ 20 ウ 25 エ 31

問4 図のアーキテクチャのシステムにおいて、CPU からみた、主記憶とキャッシュメモリを合わせた平均読込み時間を表す式はどれか。ここで、読み込みたいデータがキャッシュメモリに存在しない確率を r とし、キャッシュメモリ管理に関するオーバーヘッドは無視できるものとする。



- ア $\frac{(1-r) \cdot a}{a+b} \cdot x + \frac{r \cdot b}{a+b} \cdot y$ イ $(1-r) \cdot x + r \cdot y$
 ウ $\frac{r \cdot a}{a+b} \cdot x + \frac{(1-r) \cdot b}{a+b} \cdot y$ エ $r \cdot x + (1-r) \cdot y$

問5 CPU と主記憶の間に置かれるキャッシュメモリにおいて、主記憶のあるブロックを、キャッシュメモリの複数の特定ブロックと対応づける方式はどれか。

- ア セットアソシアティブ方式 イ ダイレクトマッピング方式
 ウ フルアソシアティブ方式 エ ライトスルー方式

問6 キャッシュメモリの書込み制御方式の一つであるライトバック方式の特徴はどれか。

- ア キャッシュメモリからデータを追い出すとき、主記憶を更新する必要がない。
 イ キャッシュメモリのデータとそれに対応する主記憶のデータとの間で不一致が生じない。
 ウ データを書き込むとき、キャッシュメモリにあるかどうかにかかわらず、主記憶に書き込む。
 エ 同一番地に繰り返して書き込む場合は、主記憶へのアクセス回数が少なくて済むが、キャッシュメモリと主記憶の不一致状態が続くことがある。

問7 フォンノイマン ボトルネック（プログラムの命令を順番にプロセッサに取り込んで実行する方式のコンピュータの性能向上を妨げる要因）はどれか。

- ア 主記憶容量
- イ 内部装置（プロセッサと主記憶）と入出力装置との間のデータ転送能力
- ウ プロセッサと主記憶との間のデータ転送能力
- エ プロセッサの性能

問8 A/D コンバータの変換時間に関する記述のうち、適切なものはどれか。

- ア 逐次比較方式は高速であり、変換時間は数ナノ秒から数十ナノ秒である。
- イ デルタシグマ方式では、ディジタルフィルタの特性によって変換時間が決定される。
- ウ 二重積分方式はフラッシュ方式に比べると高速であるが、変換時間は数マイクロ秒である。
- エ フラッシュ方式は低速であり、変換時間は数ミリ秒から数百ミリ秒かかる。

問9 入力電圧レンジが $-5 \sim +5 \text{ V}$ で出力が 8 ビットの A/D 変換器において、入力電圧 -5 V の変換値が 16 進数で 00、入力電圧 0 V の変換値が 16 進数で 80 であった。入力電圧 $+2.5 \text{ V}$ の 16 進数での変換値はどれか。ここで、量子化誤差以外の誤差は生じないものとする。

- ア 40
- イ 60
- ウ A0
- エ C0

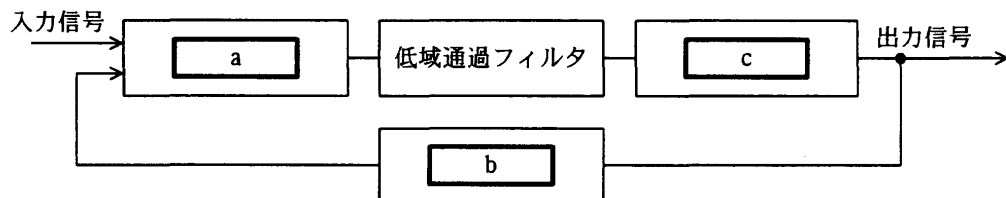
問10 DC モータにおける PWM 制御方法はどれか。

- ア パルス数によって，モータの回転角を制御する。
- イ パルス数によって，モータの回転数を制御する。
- ウ パルスの周期によって，モータの回転角を制御する。
- エ パルスのデューティ比によって，モータの回転数を制御する。

問11 アドレス線が 10 本で，1 M 語の容量をもつ DRAM がある。リフレッシュのために DRAM 内の全 ROW アドレスを 51.2 ミリ秒の間に少なくとも 1 回は選択する必要がある。このときの平均リフレッシュ周期は何マイクロ秒か。

- ア 0.049 イ 12.8 ウ 50 エ 2,560

問12 PLL のブロック図中の a～c に入れるべき適切な組合せはどれか。

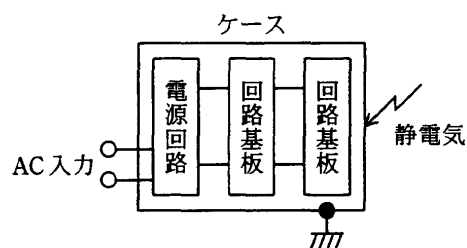


	a	b	c
ア	位相比較器	電圧制御発振器	分周器
イ	位相比較器	分周器	電圧制御発振器
ウ	電圧制御発振器	位相比較器	分周器
エ	電圧制御発振器	分周器	位相比較器

問13 位置決めセンサに用いるインクリメンタルエンコーダの特徴はどれか。

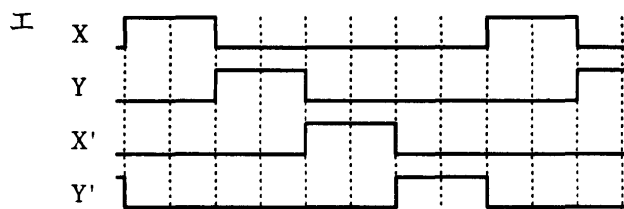
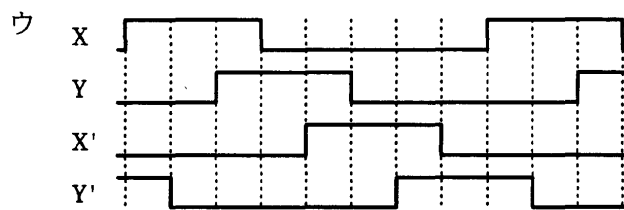
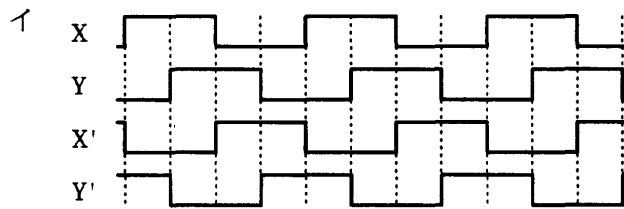
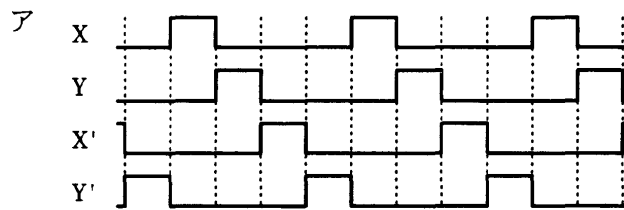
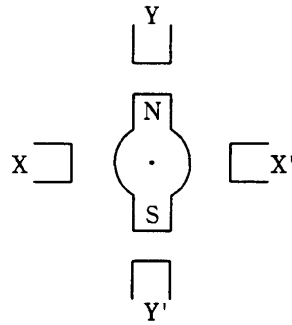
- ア 回転方向を知るために出力信号が2相になっている。
- イ 機械的位置の絶対値をアナログ値で出力する。
- ウ 機械的位置の変化量をアナログ値で出力する。
- エ 内部に機械的位置の絶対値を保持する機能を備えている。

問14 図に示す装置の金属製のケースに静電気を放電したところ、場所によってグラウンド電位に差が生じて回路が誤動作した。対策として、適切なものはどれか。

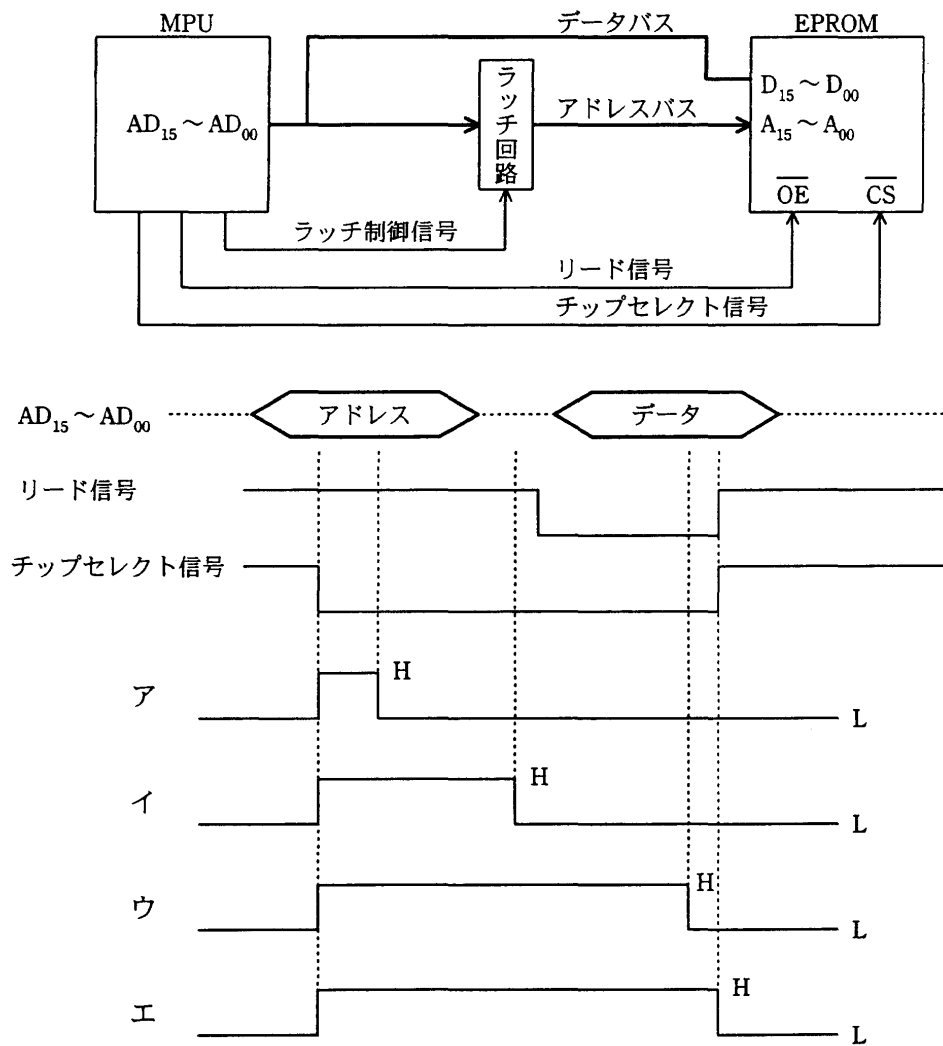


- ア AC入力にラインフィルタを挿入する。
- イ ケースと回路ブロック間を接続しているグラウンドラインを太くする。
- ウ ケースのインピーダンスを下げる。
- エ 電源とグラウンド間にバイパスコンデンサを接続する。

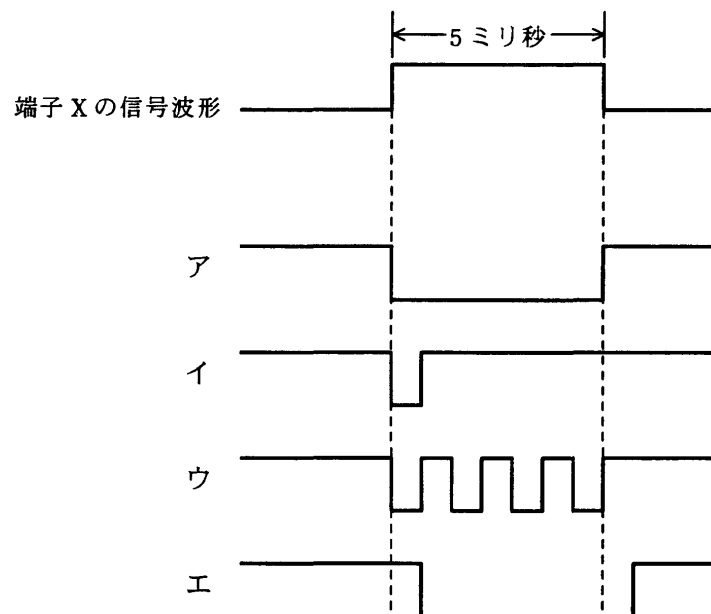
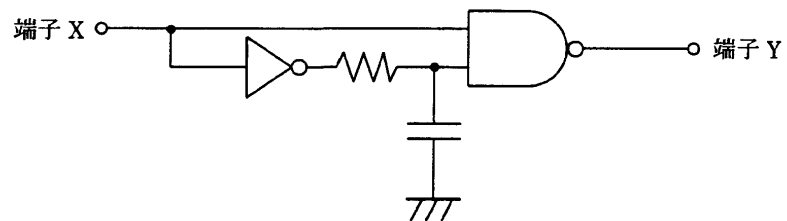
問15 図のステッピングモータ（パルスモータ）に印加する励磁パルスのうち、1-2 相励磁方式はどれか。



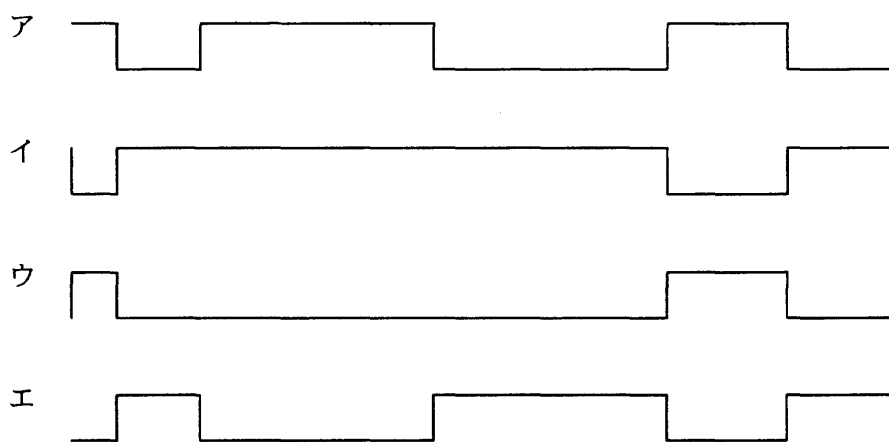
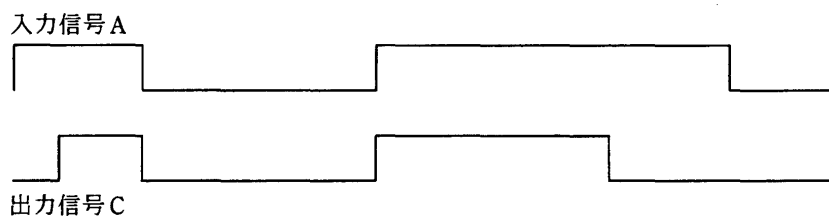
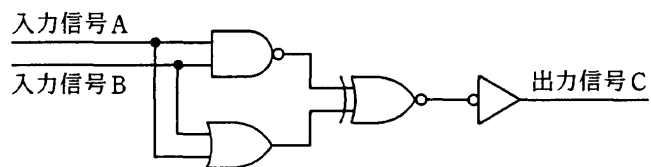
問16 アドレスバスとデータバスを共用する MPU に EPROM を接続するため、図の回路構成にする。この場合、ラッチ回路を制御するための制御信号として、適切なものはどれか。ここで、ラッチ回路は、ラッチ制御信号が H レベルなら入力を通過させ、L レベルになるとそれを保持するものとする。



問17 回路の端子 X に図に示す幅 5 ミリ秒のパルス信号を入力したときに、端子 Y に現れる信号波形として適切なものはどれか。ここで、RC 回路の時定数 τ を約 1 ミリ秒、ゲート遅延は τ に比べて十分に小さいものとする。図中の  は NAND 回路、 は NOT 回路を表す。



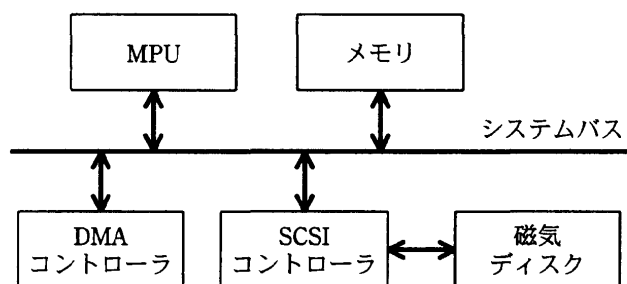
問18 図の論理回路の入力信号 A と出力信号 C を観測した。このときの入力信号 B として適切なものはどれか。ここで、 は AND 回路、 は OR 回路、 は XOR 回路、 はバッファ回路を表す。○は論理状態の反転を表す。



問19 非同期信号を同期化する方法として、適切なものはどれか。

- ア D フリップフロップを2段にして、初段の出力を2段目でもう一度受け直す。
- イ RS フリップフロップでチャタリングを防止する。
- ウ セットアップ時間を満たすように回路遅延を調整する。
- エ ホールド時間を満たすように回路遅延を調整する。

問20 図のシステムでは、磁気ディスクのデータを、SCSI コントローラを介してメモリとの間でDMA 転送する。このシステムのDMA データ転送に関する記述のうち、適切なものはどれか。ここで、SCSI コントローラは十分な容量のデータバッファをもち、MPU はキャッシュメモリを内蔵しているものとする。



- ア 仮想記憶を使用すれば、転送データのサイズがページサイズを超えたときに DMA 転送は自動的に停止する。
- イ 磁気ディスクからのデータ読出しには、ブロック転送モードを使用できない。
- ウ 磁気ディスクからメモリへ DMA 転送すると、MPU 内のキャッシュメモリの内容が正しくなくなることがある。
- エ 磁気ディスクからメモリへ DMA 転送するときには、MPU 内のキャッシュメモリへも同時に DMA 転送する。

問21 ほとんどのプログラムの大きさがページサイズの半分以下のシステムにおいて、ページサイズを半分にしたときに予想されるものはどれか。ここで、システムは主記憶が不足しがちで、多重度やスループットなどはシステム性能の限界で運用しているものとする。

- ア ページインの回数が増大するので、システム性能が低下する。
- イ ページ数が増加するので、領域管理などのオーバーヘッドが減少する。
- ウ ページ内に余裕がなくなるので、ページ置換えの効率が低下する。
- エ ページ内の無駄な空き領域が減少するので、主記憶不足が緩和される。

問22 一つのジョブについての、ターンアラウンドタイム、CPU 時間、入出力時間及び処理待ち時間の四つの時間の関係を表す式はどれか。ここで、ほかのオーバーヘッド時間は考慮しないものとする。

- ア 処理待ち時間 = CPU 時間 + ターンアラウンドタイム + 入出力時間
- イ 処理待ち時間 = CPU 時間 - ターンアラウンドタイム + 入出力時間
- ウ 処理待ち時間 = ターンアラウンドタイム - CPU 時間 - 入出力時間
- エ 処理待ち時間 = 入出力時間 - CPU 時間 - ターンアラウンドタイム

問23 二つのタスクが共用する二つの資源を排他的に使用するとき、デッドロックが発生する可能性がある。このデッドロックの発生を防ぐ方法はどれか。

- ア 一方のタスクの優先度を高くする。
- イ 資源獲得の順序を両方のタスクで同じにする。
- ウ 資源獲得の順序を両方のタスクで逆にする。
- エ 両方のタスクの優先度を同じにする。

問24 メモリリークに関する記述として、適切なものはどれか。

- ア アプリケーションの同時実行数を増やした場合に、主記憶容量が不足し、処理時間のほとんどがページングに費やされ、極端なスループットの低下を招くことである。
- イ アプリケーションや OS のバグなどが原因で、動作中に確保した主記憶が解放されないことであり、これが発生すると主記憶中の利用できる部分が減少する。
- ウ 実行時のプログラム領域の大きさに制限があるときに、必要になったモジュールを主記憶に取り込む手法である。
- エ 主記憶の内容と補助記憶の内容とを交換する処理のことである。

問25 メールボックスに関する操作で、タスクが待ち状態に遷移するものはどれか。

- ア 受信待ちをしているタスクが存在するメールボックスに対して受信要求をしたとき
- イ 受信待ちをしているタスクが存在するメールボックスに対して送信要求をしたとき
- ウ メッセージが存在するメールボックスに対して受信要求をしたとき
- エ メッセージが存在するメールボックスに対して送信要求をしたとき

問26 システムの性能向上策の適用に関して、次の式から導くことができるものはどれか。

$$P = \frac{1}{(1-a) + \frac{a}{V}}$$

ここで、 P はシステムの性能向上率、 V はその性能向上策の性能向上率、 a はその性能向上策が及ぶ範囲の全体に対する比率とする。

- ア 幾つかの性能向上策を組み合わせ、相乗効果を出すべきである。
- イ 性能向上策が及ぶ範囲の比率が一定で変化しない性能向上策を適用すべきである。
- ウ 性能面のボトルネック要因を解消する性能向上策を適用すべきである。
- エ できる限り多くの性能向上策を適用すべきである。

問27 自動支払機が 1 台ずつ設置してあった二つの支店を統合し、統合後の支店には自動支払機を 1 台設置する。統合後の自動支払機の平均待ち時間を求める式はどれか。ここで、待ち時間は M/M/1 の待ち行列モデルに従い、平均待ち時間にはサービス時間を含まないものとする。

〔条件〕

- (1) 平均サービス時間： T_s
- (2) 統合前のシステムの利用率： 両支店とも ρ
- (3) 統合後の利用者数は、統合前の 2 支店の利用者数の合計値

ア $\frac{\rho}{1-\rho} \times T_s$ イ $\frac{\rho}{1-2\rho} \times T_s$ ウ $\frac{2\rho}{1-\rho} \times T_s$ エ $\frac{2\rho}{1-2\rho} \times T_s$

問28 主記憶への1回のアクセスが200ナノ秒で、ページフォールトが発生すると1回当たり100ミリ秒のオーバーヘッドを伴うコンピュータがある。ページフォールトが主記憶アクセス50万回に1度の割合で発生する場合、ページフォールトは1秒当たり最大何回発生するか。ここで、ページフォールト以外のオーバーヘッドは考慮しないものとする。

ア 3

イ 4

ウ 5

エ 6

問29 システムの信頼性の指標であるMTBF及びMTTRに関する記述のうち、適切なものはどれか。

ア 遠隔保守はMTBFを短くし、システムの稼働率を高くする。

イ 機能分散したシステムでは、縮退運転を行うことによってMTTRは短くなる。

ウ システムを構成する機器を直列に接続すると、全体のMTBFは長くなる。

エ 予防保守はMTBFを長くし、システムの稼働率を高くする。

問30 フェールソフトの説明として、適切なものはどれか。

ア システムの一部に障害が発生したとき、それ以外の部分の機能でシステムの運転を継続する。

イ システムの一部に障害が発生したとき、致命的影響を与えないよう、システムをあらかじめ定めた安全な状態に移行する。

ウ 信頼度の高い部品を使用したり、バグの少ないソフトウェアを開発したりして、信頼性の高いシステムを構築する。

エ 特定の時点でデータベースのバックアップを取り、障害が発生した場合には、バックアップを取った時点の状態まで戻して運転を継続する。

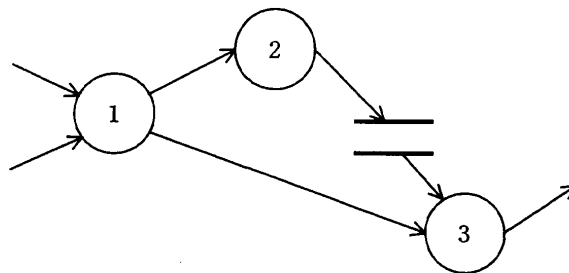
問31 Java サブレットの説明はどれか。

- ア HTML 文書に記述されたスクリプトを実行する Web コンポーネントである。
- イ Java で CGI を開発するための機能である。
- ウ 一度ロードされるとサーバに常駐し、スレッドとして実行される Web コンポーネントである。
- エ 分散オブジェクト技術を用いたソフトウェア部品が開発できるプラットフォームである。

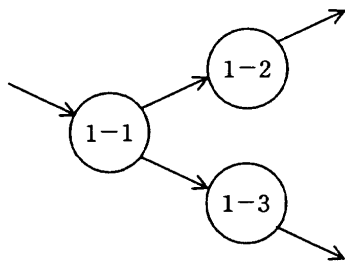
問32 CMMI を説明したものはどれか。

- ア 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するためのモデルである。
- イ ソフトウェア開発のプロセスモデルの一種である。
- ウ ソフトウェアを中心としたシステム開発及び取引のための共通フレームのことである。
- エ プロジェクトの成熟度に応じてソフトウェア開発の手順を定義したモデルである。

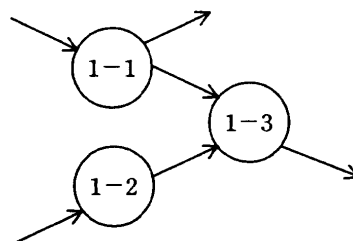
問33 図は、階層化された DFD における、あるレベルの DFD の一部である。プロセス 1 を子プロセスに分割して詳細化した DFD のうち、適切なものはどれか。ここで、プロセス 1 の子プロセスは、プロセス 1-1、1-2 及び 1-3 と表す。



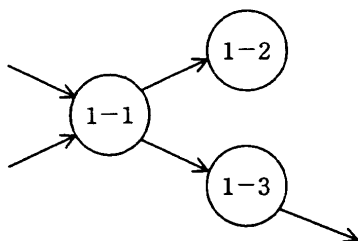
ア



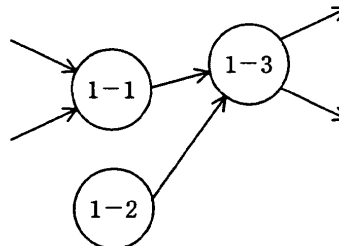
イ



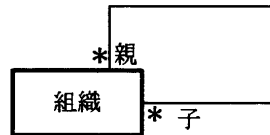
ウ



エ



問34 次の E-R 図の解釈として、適切なものはどれか。ここで、多重度の*印は 0 以上を表すものとする。また、自己参照は除くものとする。

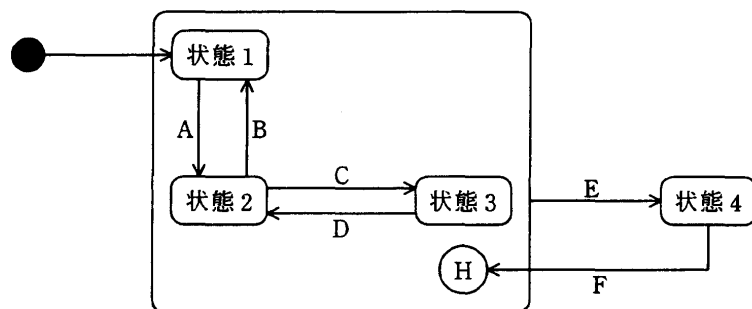


- ア 子組織の数より親組織の数が多い可能性がある。
- イ 組織は2段階の階層構造である。
- ウ 組織は必ず子組織をもつ。
- エ 組織はネットワーク構造になっていない。

問35 オブジェクト指向におけるインヘリタンスに関する記述はどれか。

- ア あるクラスのサブクラスを定義するとき、基底クラスで定義されたデータ構造と手続をサブクラスで引き継いで使うことができる。
- イ オブジェクトの性格を決めるデータ構造や値を隠ぺいし、オブジェクトの外部から直接アクセスすることを禁止する。
- ウ オブジェクトのデータ構造や手続を変更した場合でも、外部への影響を避けることができ、オブジェクトの独立性を向上させることができる。
- エ 同一のデータ構造と同一の手続をもつオブジェクトをまとめて表現したものである。

問36 次のステートチャート図で、イベントが A, B, A, C, D, E, F の順で発生した後の状態はどれか。



ア 状態1 イ 状態2 ウ 状態3 エ 状態4

問37 モジュール設計に関する記述のうち、モジュール強度が最も高いものはどれか。

- ア ある木構造データを扱う機能をデータとともに一つにまとめ、木構造データをモジュールの外から見えないようにした。
- イ 複数の機能のそれぞれに必要な初期設定の操作が、ある時点で一括して実行できるので、一つのモジュールにまとめた。
- ウ 二つの機能 A, B のコードは重複する部分が多いので、A, B を一つのモジュールとし、A, B の機能を使い分けるための引数を設けた。
- エ 二つの機能 A, B は必ず A, B の順番に実行され、しかも A で計算した結果を B で使うことがあるので、一つのモジュールにまとめた。

問38 二つの独立したテストグループ A, B が、あるシステムについて一定期間並行してテストを行い、それぞれ N_A 個及び N_B 個のエラーを検出した。このうち、共通のエラーは N_{AB} 個であった。このシステムの総エラー数 N を予測する式はどれか。ここで、 $N_A > 0$, $N_B > 0$, $N_{AB} > 0$ とし、グループ A, B のエラーを検出する能力及び効率は等しいものとする。

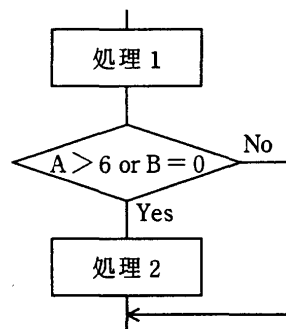
ア $N = N_A + N_B - N_{AB}$

イ $N = N_{AB} \times N_A \times N_B$

ウ $N = (N_A + N_B) / N_{AB}$

エ $N = N_A \times N_B / N_{AB}$

問39 あるプログラムについて、流れ図で示される部分に関するテストデータを、判定条件網羅（分岐網羅）によって設定した。このテストデータを、複数条件網羅による設定に変更したとき、加えるべきテストデータとして、適切なものはどれか。ここで、（ ）で囲んだ部分は、一組のテストデータを表すものとする。

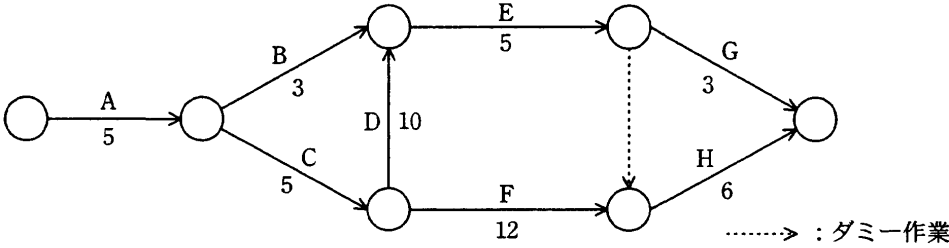


・判定条件網羅（分岐網羅）によるテストデータ

(A=4, B=1), (A=5, B=0)

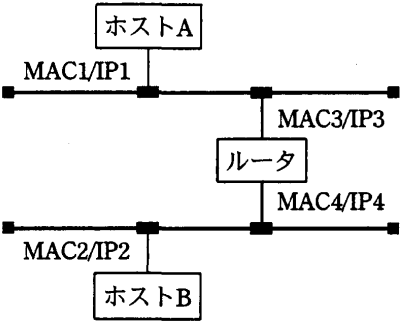
	加えるべきテストデータ
ア	(A=3, B=0), (A=7, B=2)
イ	(A=3, B=2), (A=8, B=0)
ウ	(A=4, B=0), (A=8, B=0)
エ	(A=7, B=0), (A=8, B=2)

問40 次のアローダイアグラムで表される作業 A～H を見直したところ、作業 D だけが短縮可能であり、その所要日数を 6 日間にできることが分かった。業務全体の所要日数は何日間短縮できるか。ここで、矢印に示す数字は各作業の所要日数を表す。



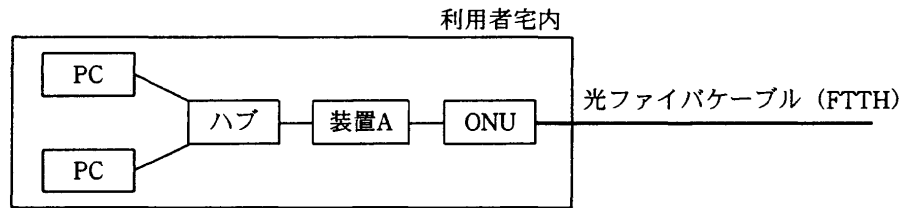
ア 1 イ 2 ウ 3 エ 4

問41 図のような IP ネットワークの LAN 環境で、ホスト A からホスト B にパケットを送信する。パケットがホスト A からルータに伝送されるとき、パケット内のイーサネットフレームのあて先と IP データグラムのあて先の組合せとして適切なものはどれか。ここで、図中の MAC n /IP m はホスト又はルータがもつインタフェースの MAC アドレスと IP アドレスを示す。



	イーサネットフレームのあて先	IP データグラムのあて先
ア	MAC2	IP2
イ	MAC2	IP3
ウ	MAC3	IP2
エ	MAC3	IP3

問42 LAN に接続されている複数の PC を FTTH を使って、インターネットに接続するシステムがあり、装置 A の WAN 側インタフェースには 1 個のグローバル IP アドレスが割り当てられている。この 1 個のグローバル IP アドレスを使って複数の PC がインターネットを利用するのに必要となる装置 A の機能はどれか。



- | | |
|---------|--------------------|
| ア DHCP | イ NAPT (IP マスカレード) |
| ウ PPPoE | エ パケットフィルタリング |

問43 誤り検出方式である CRC に関する記述として、適切なものはどれか。

- ア 検査用データは、検査対象のデータを生成多項式で処理して得られる 1 ビットの値である。
- イ 受信側では、付加されてきた検査用データで検査対象のデータを割り、余りがなければ送信が正しかったと判断する。
- ウ 送信側では、生成多項式を用いて検査対象のデータから検査用データを作り、これを検査対象のデータに付けて送信する。
- エ 送信側と受信側では、異なる生成多項式が用いられる。

問44 6,000 バイトのデータの送信を 5 秒以内に行うために、必要な回線速度は最低何ビット／秒か。ここで、伝送制御のための情報は考慮しないこととし、回線の伝送効率は 60% とする。

- | | | | |
|---------|---------|---------|----------|
| ア 1,200 | イ 4,800 | ウ 9,600 | エ 19,200 |
|---------|---------|---------|----------|

問45 LAN のアクセス制御方式である CSMA/CD 方式に関する説明として、適切なものはどれか。

- ア 送出した信号の衝突を検知した場合は、ランダムな時間の経過後に再送信する。
- イ 送信権を与えるメッセージ（フリートークン）を得たノードがデータを送信する。
- ウ デジタル信号をアナログ信号に変換（変調）して通信を行う。
- エ 転送する情報を、セルと呼ばれる固定長のブロックに分割して転送する。

問46 公開鍵暗号方式に関する記述のうち、適切なものはどれか。

- ア AES は、NIST が公募し、1997 年に決定した公開鍵暗号方式の一種である。
- イ RSA は、素因数分解の計算の困難さを利用した、公開鍵暗号方式の一種である。
- ウ 公開鍵暗号方式の難点は、鍵の管理が煩雑になることである。
- エ 通信文の内容の秘匿に公開鍵暗号方式を使用する場合は、受信者の復号鍵を公開する。

問47 デジタル署名を利用する目的はどれか。

- ア 受信者が署名用の鍵を使って暗号文を元の平文に戻すことができるようにする。
- イ 送信者が署名用の鍵を使って作成した署名を平文に付加することによって、受信者が送信者を確認できるようにする。
- ウ 送信者が署名用の鍵を使って平文を暗号化し、平文の内容を関係者以外に分からないようにする。
- エ 送信者が定数を付加した平文を署名用の鍵を使って暗号化し、受信者が復号した定数を確認することによって、メッセージの改ざん部位を特定できるようにする。

問48 IDS (Intrusion Detection System) の特徴のうち、適切なものはどれか。

- ア ネットワーク型 IDS では、SSL を利用したアプリケーションを介して行われる攻撃を検知できる。
- イ ネットワーク型 IDS では、通信内容の解析によって、ファイルの改ざんを検知できる。
- ウ ホスト型 IDS では、シグネチャとのパターンマッチングを失敗させるためのパケットが挿入された攻撃でも検知できる。
- エ ホスト型 IDS では、到着する不正パケットの解析によって、ネットワークセグメント上の不正パケットを検知できる。

問49 ステガノグラフィの機能はどれか。

- ア 画像データなどにメッセージを埋め込み、メッセージの存在そのものを隠す。
- イ メッセージの改ざん、なりすましの検出、及び否認防止を行う。
- ウ メッセージの認証を行って改ざんの有無を検出する。
- エ メッセージを決まった手順で変換し、通信途中での盗聴を防ぐ。

問50 送信者がメッセージからブロック暗号（方式）を用いて生成したメッセージ認証符号（MAC: message authentication code）をメッセージとともに送り、受信者が受け取ったメッセージから MAC を生成して、送られてきた MAC と一致することを確認するメッセージ認証で使用する鍵の組合せはどれか。

	送信者	受信者
ア	受信者と共有している共通鍵	送信者と共有している共通鍵
イ	受信者の公開鍵	受信者の秘密鍵
ウ	送信者の公開鍵	受信者の秘密鍵
エ	送信者の秘密鍵	受信者の公開鍵

問51 情報システムへの脅威とセキュリティ対策の組合せのうち、適切なものはどれか。

	脅威	セキュリティ対策
ア	地震と火災	フォールトトレラント方式のコンピュータによるシステムの二重化
イ	データの物理的な盗難と破壊	ディスクアレイやファイアウォール
ウ	伝送中のデータへの不正アクセス	HDLC プロトコルの CRC
エ	メッセージの改ざん	公開鍵暗号方式を応用したデジタル署名

問52 SSL の利用に関する記述のうち、適切なものはどれか。

- ア SSL で使用する個人認証用のデジタル証明書は、IC カードなどに格納できるので、格納場所を特定の PC に限定する必要はない。
- イ SSL は特定利用者間の通信のために開発されたプロトコルであり、事前の利用者登録が不可欠である。
- ウ デジタル証明書には IP アドレスが組み込まれているので、SSL を利用する Web サーバの IP アドレスを変更する場合は、デジタル証明書を再度取得する必要がある。
- エ 日本国内では、SSL で使用する共通鍵の長さは、128 ビット未満に制限されている。

問53 情報セキュリティ基本方針文書の取扱いについて、ISMS 認証基準に定められているものはどれか。

- ア 一度決めた内容は変更せず、セキュリティ事故発生時に見直す。
- イ 機密情報であるので関連する管理者にだけ内容を教育する。
- ウ 経営陣によって承認され、全従業員に公表し通知する。
- エ 作成したメンバ自身で実施状況を点検する。

問54 JIS Q 9001 (ISO 9001) に規定されているものはどれか。

- ア 外部から購入したソフトウェア製品を最終製品に組み込む場合は、動作検査を実施した後に行う。
- イ 設計の妥当性確認は、ソフトウェア開発者自身が行うテスト及びデバッグによって実現される設計検証の一つとして実施する。
- ウ トレーサビリティが要求される製品は、製造番号などによって固有の識別を管理し記録する。
- エ 納入製品に組み込むために提供された顧客の所有物には、顧客の知的所有権は含まれない。

問55 国際標準化の動向に関する記述のうち、適切なものはどれか。

- ア “情報技術－情報セキュリティマネジメントの実践のための規範”を規定している ISO/IEC 17799 は、JIS X 5080 の基になっている。
- イ “品質及び／又は環境マネジメントシステム監査のための指針”を規定している ISO 19011 は、システム監査基準の基になっている。
- ウ “品質システム－設計・開発・製造における品質保証モデル”を規定している ISO 9001 は、共通フレーム 98 (SLCP-JCF98) の基になっている。
- エ “プロジェクトマネジメントにおける品質の指針”を規定している ISO 10006 は、PMBOK の基になっている。

9. 答案用紙の記入に当たっては、次の指示に従ってください。
- (1) HB の黒鉛筆又はシャープペンシルを使用してください。訂正の場合は、あとが残らないように消しゴムできれいに消し、消しくずを残さないでください。
 - (2) 答案用紙は光学式読取り装置で処理しますので、答案用紙のマークの記入方法のとおりマークしてください。
 - (3) 受験番号欄に、受験番号を記入及びマークしてください。正しくマークされていない場合、答案用紙のマークの記入方法のとおりマークされていない場合は、採点されません。
 - (4) 生年月日欄に、受験票に印字されているとおりの生年月日を記入及びマークしてください。正しくマークされていない場合は、採点されないことがあります。
 - (5) 解答は、次の例題にならって、解答欄に一つだけマークしてください。

〔例題〕 春の情報処理技術者試験が実施される月はどれか。

ア 2 イ 3 ウ 4 エ 5

正しい答えは“ウ 4”ですから、次のようにマークしてください。

例題	☐ ア	☐ イ	☒ ウ	☐ エ
----	-------------------------	-------------------------	------------------------------------	-------------------------

- 10. 試験終了後、この問題冊子は持ち帰ることができます。
- 11. 答案用紙は、白紙であっても提出してください。
- 12. 試験時間中にトイレへ行きたくなったり、気分が悪くなったりした場合は、手を挙げて監督員に合図してください。
- 13. 午後の試験開始は 12:10 です。12:00 までに着席してください。

試験問題に記載されている会社名又は製品名は、それぞれ各社の商標又は登録商標です。

なお、試験問題では、® 及び ™ を明記していません。