

平成18年度技術士第二次試験問題（情報工学部門）

必須科目 （16） 情報工学一般

Ⅱ－1 次の20問題のうち15問題を選んで解答せよ。（解答欄に1つだけマークすること。）

Ⅱ－1－1 信号処理に関する次の定理についての記述の中で正しいものはどれか。

定理：信号の帯域の少なくとも（A）倍以上の周波数で（B）を行えば，その中に元の信号のすべての情報が含まれる。

- ① この定理は通常，ウィーナーの名前を冠して呼ばれる。
- ② （A）には「2」，（B）には「量子化」を補うのが正しい。
- ③ この定理を満たす最大の周波数をナイキスト周波数と呼ぶ。
- ④ この定理を満たさないときに偽の信号が得られる現象をエリアシング（aliasing）と呼ぶ。
- ⑤ この定理を満たさない場合の画像の読みとりには，周波数を制約するため，ハイパスフィルタを使用するとよい。

Ⅱ－1－2 色のRGB表現を（ r, g, b ）と表記するものとする。ここで， r, g, b はそれぞれ赤，緑，青成分の大きさを0.0から1.0までの数値で表したものとし，0.0のときはその成分がないことを示し，1.0のときはその成分が表示できる最大値であることを示すものとする。

次の中で一般的なピンク色に近いRGB表現はどれか。

- ① （0, 0, 1）
- ② （0.5, 1, 1）
- ③ （1, 0, 0）
- ④ （1, 0.5, 0.5）
- ⑤ （1, 1, 0.5）

II-1-3 マルチコアプロセッサについて説明した次の中で間違っているのはどれか。

- ① 複数のプロセッサコアを一つのパッケージに集積したマイクロプロセッサをいう。
- ② 二つのプロセッサコアからなる場合は、デュアルコアプロセッサという。
- ③ ソフトウェアから見ると、マルチプロセッサと同じように利用できる。
- ④ 一つの命令に対し複数のデータストリームを並列に実行できる点が最大の特徴である。
- ⑤ 集積度が高くなるので、コストが高くなる傾向がある。

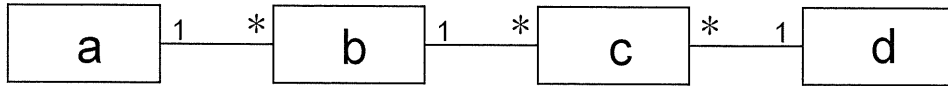
II-1-4 コンピュータの安全性を改善するための方式を挙げた次の中で間違っているものはどれか。

- ① 暗号化
- ② PCグリーンラベル
- ③ ファイルパーミッション機能
- ④ ロールベースアクセス制御
- ⑤ セキュアOS

II-1-5 ニューラルネットに関する次の説明のうち、正しいものはどれか。

- ① 相互結合型ニューラルネットでは、入力信号の流れは常に一方向的である。
- ② バックプロパゲーション学習アルゴリズムは、教師なし学習である。
- ③ ヘップ型学習アルゴリズムは、教師あり学習である。
- ④ ホップフィールドネットは、階層型ニューラルネットである。
- ⑤ ボルツマンマシンでは、焼きなまし（アニーリング）が用いられる。

II-1-6 受注処理に関するエンティティ(顧客, 商品, 注文, 注文明細)間の関係を表現したE-R図において, a, b, c, dに入れるエンティティの組合せとして正しいものはどれか。ただし, 顧客は繰り返して注文し, 一度に複数の商品を注文することがあるものとする。また, エンティティ間の関係の多重度はターゲット側に書き, *は複数を表す。



	a	b	c	d
①	顧客	注文明細	注文	商品
②	注文	注文明細	顧客	商品
③	顧客	注文	注文明細	商品
④	商品	注文	注文明細	顧客
⑤	商品	注文明細	注文	顧客

II-1-7 McCabeの提唱したベースパステストは、テストの回数を見積もる方法の原点である。この方法は、実行される可能性のある基本パス(ベースパス)の集合を求め、その各パスに対応するテストケースを1個ずつ実行すれば、プログラムのすべての文を少なくとも1度は実行することを保証するというものである。次のJava言語のプログラムaverageに対するベースパステストケースの数はいくつか。

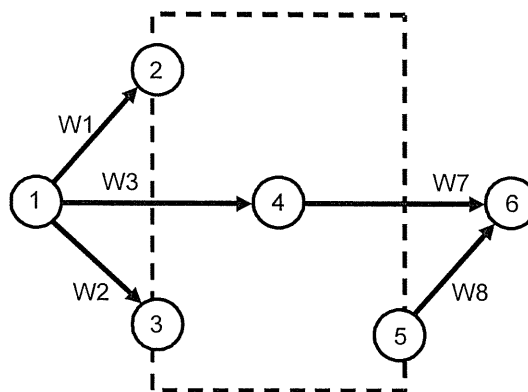
```
void average (int min, int max, int [] array) {
    double sum = 0.0;
    int valid = 0;
    for (int i=0; i<array.length; i++) {
        if ( (min <= array[i]) && (array[i] <= max) ) {
            valid++;
            sum += array[i];
        }
    }
    System.out.println ("有効数=" + valid);
    if (valid > 0) {
        System.out.println ("平均値=" + sum / valid);
    }
}
```

- ① 3 ② 4 ③ 5 ④ 6 ⑤ 7

Ⅱ－１－８ (表 a) の工程表で示される作業工程があるとき、クリティカルパスの長さを求めよ。ヒントとして (図 b) に不完全なアローダイアグラムを示すので、点線内を完成させるとよい。

(表 a) 工程表

作業	所要日数	先行作業
W1	6	なし
W2	7	なし
W3	5	なし
W4	4	W1
W5	3	W2
W6	8	W2,W3,W4
W7	10	W2,W3,W4
W8	9	W5,W6



(図 b) 不完全なアローダイアグラム

- ① 15日 ② 17日 ③ 24日 ④ 27日 ⑤ 34日

Ⅱ－１－９ ある店舗に、ケンドール記法でM/M/1モデル(到着の仕方がランダム、すなわちポアソン分布で、サービスが指数分布に従う窓口1のモデル)に従うレジがあるものとする。その店に16時間の営業時間中に平均128人の客が到着し、1人の客あたりの平均サービス時間を6分とすると、その場合の平均待ち時間は何分となるか。

- ① 6分 ② 12分 ③ 18分 ④ 24分 ⑤ 30分

II-1-10 次のコードは、JAVAによるある処理の再帰（recursive）プログラムである。
このプログラムに $m=806$ 、 $n=338$ を与えた場合に得られる値を次の中から選べ。

```
public int abc(int m, int n) {  
    if (m==n) {  
        return n;  
    } else if (m<n) {  
        return abc(m, n-m);  
    } else {  
        return abc(m-n, n);  
    }  
}
```

- ① 2 ② 5 ③ 13 ④ 19 ⑤ 26

II-1-11 特定電子メールの送信の適正化等に関する法律（平成十四年四月十七日法律二十六号，最終改正平成一七年七月二六日法律第八七号）および特定電子メールの送信の適正化等に関する法律施行規則（平成十四年六月二十一日総務省令第六十六号，最終改正平成一七年一〇月二六日総務省令第一四八号）について，次の選択肢から正しいものを選べ。

- ① この法律には罰則規定が定められていない。
- ② 送信者は，その送信をした特定電子メールの受信者であって，特定電子メールの送信をしないように求める旨を当該送信者に対して通知したものに対して，特定電子メールの送信をしてはならない。
- ③ 電気通信事業者は，一時に多数の架空電子メールアドレスに宛てた電子メールが送信された場合，いかなる状況でもその電気通信役務の提供を拒むことはできない。
- ④ 特定電子メールの送信にあたっては，送信者の住所氏名の表示だけが義務付けられている。
- ⑤ 特定電子メールの送信にあたっては，例えば（未承認です）や（承認なしにお送りしています）のように，受信者の承諾を得ていないことが分かる任意の文章の表示が義務付けられている。

II-1-12 サーバ側のWeb技術に関する次の選択肢から正しいものを選び。

- ① Java ScriptはJavaでサーバアプリケーションを構築するためのクラスライブラリである。
- ② Java ScriptではHTMLに埋め込んだスクリプトがサーバ側で実行される。
- ③ Java Servletはサーバ側のJava VM上で動作するが、いったん起動されるとメモリに常駐して実行される。
- ④ JSP (JavaServerPages) はJavaでサーバアプリケーションを構築するためのクラスライブラリである。
- ⑤ SSI (Server Side Include) とはサーバとの通信を暗号化してセキュリティを高めるための仕組みである。

II-1-13 基幹システムで蓄積された大量のデータを分析し、単なる検索アルゴリズムだけでは発見が困難な規則や相関関係を抽出するために使用される技法はどれか。

- ① データクリーニング ② データスーツ ③ データマイニング
- ④ データマート ⑤ データリンク

II-1-14 主記憶上で、配列にN個の見出し付きデータが格納されているものとする。このデータに対する操作についての記述の中で、誤っているものを選び。

- ① 2分探索法を用いて見出し探索 (key search) を行う場合には、データを見出し順にソートしておく必要はない。
- ② データが見出し順にソートされているとき、その状態をくずさないように追加し、または削除してつめるために必要な平均計算量は、いずれも $O(N)$ である。
- ③ 線形探索法を用いて見出し探索を行う場合、一つの見出しの探索に要する計算量の最大は $O(N)$ である。
- ④ 2分探索法を用いて見出し探索を行う場合、一つの見出しの探索に要する計算量の平均は $O(\log N)$ である。
- ⑤ 2分探索法は、見出しの探索空間を1回の比較操作ごとに2分の1ずつに狭める探索法である。

II-1-15 分散システム環境でのトランザクション処理は、データベースの保全性 (integrity) を維持するために、ACID特性を保持することが不可欠である。次の用語の中でACID特性に含まれないものを選べ。

- ① トランザクション処理の過程において、データベースの状態を遷移させるとき、処理の前後において状態の一貫性は維持される (一貫性)。
- ② トランザクションはシステム障害発生時における自律的な回復機能をもつ (自律性)。
- ③ トランザクションは障害発生時における回復の単位であり、コミットされるとシステムクラッシュが発生してもその処理内容は失われない (耐久性)。
- ④ 一つのトランザクションは、完遂されるかまったく実行されないかという悉無律に従う、不可分の処理単位である (原子性)。
- ⑤ 複数のトランザクションが同時に実行される場合、それぞれは干渉の無い無関係の隔離された処理単位として実行される (隔離性)。

II-1-16 電子メールに関する次の説明のうち、正しいものを選べ。

- ① メールクライアントがメールサーバからメールを取り出すプロトコルであるPOP3 (Post Office Protocol 3) はメールサーバに着信したメールをクライアント側にすべてダウンロードする。POP3はクライアントからのメール送信時にも利用される。
- ② メールクライアントがメールサーバからメールを取り出すプロトコルであるIMAP4 (Internet Message Access Protocol 4) はメールサーバでメールを管理し、指定されたメールだけをクライアントで取り出す。Webメールで使われるプロトコルはIMAP4のみである。
- ③ メールヘッダ部が日本語の場合、ヘッダ部をISO-2022-JPと呼ばれるJISコード変換方式を用いて7ビットのJISコードに変換するだけでメールサーバに送ることができる。
- ④ Bcc (Blind Carbon Copy) に指定されたアドレスはメールサーバに送られるデータのヘッダに書かれるが、受信時にヘッダから削除されるために受信者にはBccで指定された送信先が見えない。
- ⑤ 電子メールを暗号化して送受信するために使われるS/MIME (Secure Multipurpose Internet Mail Extensions) では公開鍵暗号方式と共通鍵暗号方式の両方を使う。

II-1-17 次の説明で(a)～(d)の組合せとして正しいものを選び。

IP (Internet Protocol)v4のIPアドレスは32ビットであるのに対し、IPv6のIPアドレスは (a) ビットである。IPv4とIPv6の共存方法には (b) や (c) がある。IPv6は (d) によるセキュリティ機能を標準で装備している。

	(a)	(b)	(c)	(d)
①	128	IPマスカレード	NAT	SSL
②	128	IPマスカレード	デュアルスタック	IPsec
③	128	トンネリング	デュアルスタック	IPsec
④	256	トンネリング	DHCP	SSL
⑤	256	ネゴシエーション	エンベロープ	IPsec

DHCP : Dynamic Host Configuration Protocol

IPsec : IP security

NAT : Network Address Translation

SSL : Secure Socket Layer

II-1-18 ファイアウォールに関する次の説明のうち、正しいものを選び。

- ① パケット・フィルタリング方式のファイアウォールは、MAC (Media Access Control) アドレスなどフレーム単位でアクセスデータをチェックし、不正なアクセスを阻止する。
- ② アプリケーション・ゲートウェイ方式のファイアウォールでは、通信相手が不正侵入者でないか秘密鍵を用いて認証することが、主たる不正アクセス防止機能である。
- ③ ステートフル・インスペクション方式のファイアウォールは、セッションの状態をチェックして、不正なアクセスを阻止する。
- ④ 一般に、アプリケーション・ゲートウェイ方式のファイアウォールはステートフル・インスペクション方式のファイアウォールと比べ、ハードウェアの負荷が小さい。
- ⑤ IDS (Intrusion Detection System) は不正侵入を検知する役割を持っており、ファイアウォールの不正侵入阻止とは役割が異なる。そのため、IDSが収集した情報をファイアウォールの設定情報として活用することは有効ではない。

II-1-19 IEEE802.11方式無線LAN (Local Area Network) のセキュリティに関する次の説明のうち、正しいものを選び。

- ① SSID (Service Set Identifier) というパスワードをユーザごとにあらかじめ設定登録することで、登録されたパスワードと異なる値を設定されたPC (Personal Computer) からのアクセスを拒否できる。
- ② どの値のMAC (Media Access Control) アドレスでもアクセスを許可する「ANY」と呼ばれるモードがある。
- ③ PC固有のMACアドレスを利用して、アクセスを制限する方式を、MACアドレスフィルタリングという。
- ④ 通信フレームを暗号化するWEP (Wired Equivalent Privacy) では、暗号処理の負荷が軽いブロック暗号のDES (Data Encryption Standard) が用いられる。
- ⑤ WEPで使用される暗号方式よりも優れた方式としてWPA-TKIP (Wi-Fi Protected Access Temporal Key Integrity Protocol) があり、暗号鍵は固定であるが、公開鍵暗号方式が使用されており、暗号強度が高い。

II-1-20 TCP (Transmission Control Protocol - RFC793) 及びUDP (User Datagram Protocol - RFC768) のポートに関する次の記述のうち、正しいものを選び。

- ① サーバプログラムで要求を受け付けるポートはTCP及びUDPいずれの場合も1024番以下を用いなければならない。
- ② DNS (Domain Name System) サーバプログラムでUDPの53番ポートを用いた場合、TCPの53番ポートは利用してはならない。
- ③ Well Knownポートとして割り当てられたポート番号を用いている場合でも、そのサーバプログラムがWell Knownポートとして指定されたサービスを実行しているとは限らない。
- ④ 一つのサーバプログラムで複数のポート番号を用いてはならない。
- ⑤ IP (Internet Protocol)v6では、IPアドレスの拡張に伴いポート番号も32ビットに拡張された。