

平成29年度後期 情報検定

<実施 平成30年2月11日（日）>

システムデザインスキル

（説明時間 14：30～14：40）

（試験時間 14：40～16：10）

- ・試験問題は試験開始の合図があるまで開かないでください。
- ・解答用紙（マークシート）への必要事項の記入は、試験開始の合図と同時に行いますので、それまで伏せておいてください。
- ・試験開始の合図の後、次のページを開いてください。＜受験上の注意＞が記載されています。必ず目を通してから解答を始めてください。
- ・試験問題は、すべてマークシート方式です。正解と思われるものを1つ選び、解答欄の○をHBの黒鉛筆でぬりつぶしてください。2つ以上ぬりつぶすと、不正解になります。
- ・辞書、参考書類の使用および筆記用具の貸し借りは一切禁止です。
- ・電卓の使用が認められます。ただし、下記の機種については使用が認められません。

<使用を認めない電卓>

1. 電池式（太陽電池を含む）以外の電卓
2. 文字表示領域が複数行ある電卓（計算状態表示の一行は含まない）
3. プログラムを組み込む機能がある電卓
4. 電卓が主たる機能ではないもの
 - * パソコン（電子メール専用機等を含む）、携帯電話（PHS）、スマートフォン、タブレット、電子手帳、電子メモ、電子辞書、翻訳機能付き電卓、音声応答のある電卓、電卓付き腕時計、時計型ウェアラブル端末等
5. その他試験監督者が不適切と認めるもの

＜受験上の注意＞

1. この試験問題は12ページあります。ページ数を確認してください。
乱丁等がある場合は、手をあげて試験監督者に合図してください。
※問題を読みやすくするために空白ページを設けている場合があります。
2. 解答用紙（マークシート）に、受験者氏名・受験番号を記入し、受験番号下欄の数字をぬりつぶしてください。正しく記入されていない場合は、採点されませんので十分注意してください。
3. 試験問題についての質問には、一切答えられません。自分で判断して解答してください。
4. 試験中の筆記用具の貸し借りは一切禁止します。筆記用具が破損等により使用不能となった場合は、手をあげて試験監督者に合図してください。
5. 試験を開始してから30分以内は途中退出できません。30分経過後退出する場合は、もう一度、受験番号・マーク・氏名が記載されているか確認して退出してください。なお、試験終了5分前の合図以降は退出できません。試験問題は各自お持ち帰りください。
6. 試験後にお知らせする合否結果（合否通知）、および合格者に交付する「合格証・認定証」はすべて、Webページ（PC、モバイル）での認証によるデジタル「合否通知」、デジタル「合格証・認定証」に移行しました。
 - ①団体宛にはこれまでと同様に合否結果一覧ほか、試験結果資料一式を送付します。
 - ②合否等の結果についての電話・手紙等でのお問い合わせには、一切応じられませんので、ご了承ください。

問題を読みやすくするために、
このページは空白にしてあります。

<設問2> 記述中の下線(a)への対応として関係の深いものには「ア」、そうでないものには「イ」を答えよ。

- (7) コピー用紙や筆記具などの事務用品はエコマークが付いている製品を購入する。
- (8) 自社製品の競争力を高めるための設備投資をする。
- (9) 従業員が内部通報できる仕組みを作る。
- (10) 不法行為の発生を抑制するための教育を実施する。

問題2 次のテスト技法に関する記述を読み、各設問に答えよ。

ソフトウェアテストは、プログラムが設計書に定められた機能を満足し、正常に動作するかを検査する工程である。テストは、最小機能単位であるモジュールを一つずつテストする単体テストから始め、単体テストが終了した個々のモジュールを2つ以上組み合わせたときにプログラムが正しく動作するかどうかをテストする結合テスト、実際の動作環境でうまく動作するかをテストするシステムテストというように段階的に進められる。

<設問1> 次の単体テストに関する記述中の□□□□に入れるべき適切な字句を解答群から選べ。

単体テストの手法として代表的なものに、プログラムの内部構造に着目してテストデータを作成し、プログラムの論理が正しいかを検証する□□□□(1)と、プログラムの外部仕様に着目し、入力データと出力結果だけを見て、機能が要求どおりになっているかを検証する□□□□(2)とがある。

□□□□(2)におけるテストデータの設計方法としては、同値分割や□□□□(3)がある。例えば、入力項目が“得点(整数値:0~100)”であるとき、テストデータの最小の組合せとして、同値分割を用いると□□□□(4)となり、□□□□(3)を用いると□□□□(5)となる。

(1) ~ (3) の解答群

- | | |
|----------------|----------------|
| ア. 原因-結果グラフ | イ. 限界値分析 |
| ウ. 実験計画法 | エ. ブラックボックステスト |
| オ. ホワイトボックステスト | カ. レグレッションテスト |

(4), (5) の解答群

- | | |
|--------------------|----------------|
| ア. -5, 5, 95, 105 | イ. -5, 85, 120 |
| ウ. -1, 0, 100, 101 | エ. -1, 101 |
| オ. 0, 100 | カ. 101, 120 |

<設問2> 次の結合テストに関する記述中の□□□□に入れるべき適切な字句を解答群から選べ。

結合テストの手法として代表的なものに、□□□□(6)や□□□□(7)がある。

□□□□(6)は、最上位のモジュールから順に下位モジュールへと結合していく方法である。上位のモジュールからテストをするため、□□□□(8)と呼ばれるテスト用モジュールを作成してテストを行う。

(7) は、最下位のモジュールから順に上位のモジュールへ結合していく方法である。下位のモジュールからテストするため、(9) と呼ばれるテスト用のモジュールを作成してテストする。

(6) ~ (9) の解答群

- ア. エミュレータ
- イ. サンドイッチテスト
- ウ. シミュレータ
- エ. スタブ
- オ. トップダウンテスト
- カ. ドライバ
- キ. ビックバンテスト
- ク. ボトムアップテスト

<設問 3> 次のテストケースにおける網羅率に関する記述中の [] に入れるべき適切な字句を解答群から選べ。

プログラムの内部仕様をもとにテストケースを設計する方法では、表のような種類がある。しかし、処理が複雑になると、すべてのテストケースの検証が難しくなるため、テストケースや経路などをどの程度カバーしているかを表す網羅率を利用する。

表 テストケースの種類

種類	説明
命令網羅	すべての命令を実行する
分岐網羅(判定条件網羅)	すべての分岐について、少なくとも1回は実行する
条件網羅	条件判定に用いられているすべての条件に対して、真偽を少なくとも1回は実行する。
複数条件網羅	すべての条件に対して、真偽のすべての組合せを実行する。

ここで、図の流れ図と命令において、テストケースを (a=1, b=-1) と (a=0, b=-1) としてテストすると、命令網羅率と分岐網羅率は (10) % であり、複数条件網羅率は (11) % となる。

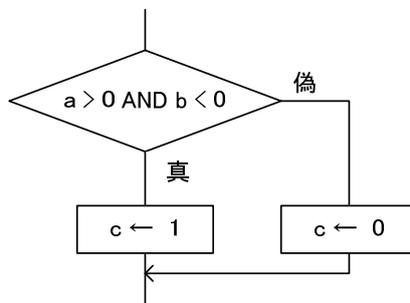


図 分岐の流れ図と命令の具体例

(10), (11) の解答群

- ア. 25
- イ. 50
- ウ. 75
- エ. 100

問題3 次のネットワークに関する記述を読み、各設問に答えよ。

J社の現在のネットワーク構成を図に示す。

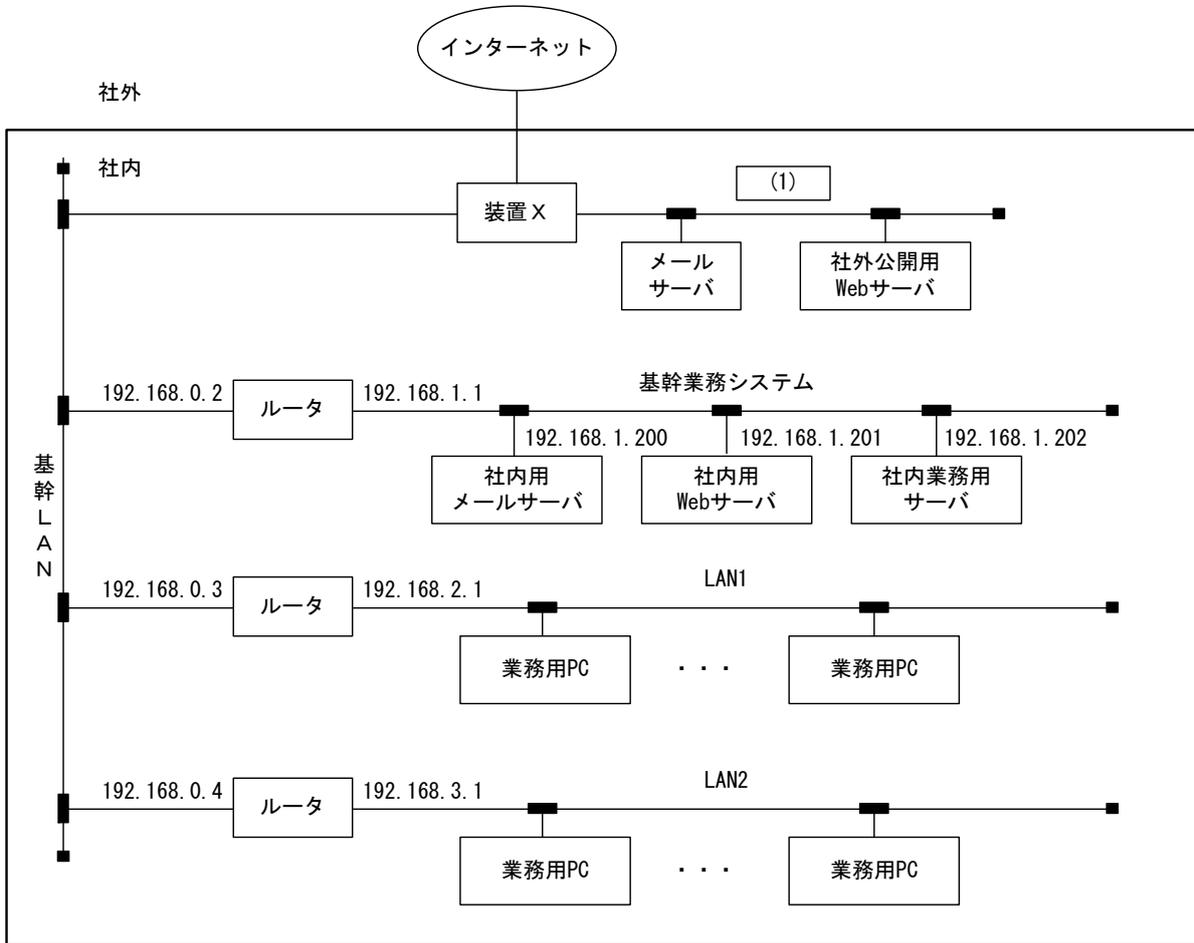


図 J社の現在のネットワーク構成

<設問1> 次のネットワーク構成に関する記述中の [] に入れるべき適切な字句を解答群から選べ。

装置Xによってインターネットからも社内ネットワークからも隔離された場所を [(1)] と呼ぶ。外部に公開するサーバをこの場所に設置することで、装置Xの機能により外部からの不正アクセスを防御する。また、万が一防げずにサーバが被害を受けたとしても、社内ネットワークに影響を及ぼすこともない。このような機能を提供する装置Xまたは機能そのものを [(2)] と呼ぶ。

(1) の解答群

- ア. ASP イ. DHCP ウ. DMZ エ. ISP

(2) の解答群

ア. LAN アダプタ

イ. NIC

ウ. スイッチングハブ

エ. ファイアウォール

<設問 2> 次の IP アドレスに関する記述中の [] に入れるべき適切な字句を解答群から選べ。

J 社の各ネットワークに接続された機器の IP アドレスから、このネットワークはクラス C で設定されていることがわかるので、標準サブネットマスクは [(3)] である。これにより、各 LAN のネットワークアドレスは、基幹 LAN が [(4)]、LAN1 が [(5)]、LAN2 が [(6)] である。

また、LAN 内のすべての装置に対して一斉に送信することを [(7)] と呼ぶ。

(3) の解答群

ア. 255.0.0.0

イ. 255.255.0.0

ウ. 255.255.240.0

エ. 255.255.255.0

(4) ~ (6) の解答群

ア. 192.168.0.0

イ. 192.168.1.0

ウ. 192.168.2.0

エ. 192.168.3.0

(7) の解答群

ア. エニーキャスト

イ. ブロードキャスト

ウ. マルチキャスト

エ. ユニキャスト

<設問 3> LAN1 の業務用 PC に設定する IP アドレスとして、不適切なものを解答群から選べ。

(8) の解答群

ア. 192.168.2.10

イ. 192.168.2.100

ウ. 192.168.2.200

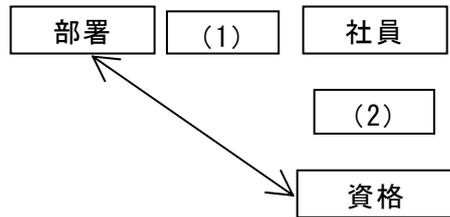
エ. 192.168.2.255

問題4 次のデータベースに関する記述を読み、各設問に答えよ。

J社では、社員の技術向上のため資格の取得を勧めている。部署には複数の社員が所属し、社員は一つの部署だけに所属する。部署ごとに必要な資格は複数あり、同じ資格でも部署により重要度が異なる。これをスコアとして設定している。なお、どの資格も取得していない社員や、複数の資格を取得している社員もいる。

資格取得の状況を管理するため、資格取得管理システムを構築し運用している。

<設問1> 次の社員と部署および資格をモデル化したE-R図の[]に入れるべき適切なエンティティ間のリレーションを解答群から選べ。



凡例 ———: 1対1 ———>: 1対多 <=>: 多対多

図 資格取得管理システムに関するE-R図

(1) の解答群

- ア. ——— イ. ———> ウ. <—— エ. <=>

(2) の解答群

- ア. | イ. ↓ ウ. ↑ エ. ⇕

E-R図をもとにデータベースを設計構築した。今回の処理で使用する表を示す。下線の項目は主キーであり、(FK)が付いている項目は外部キーである。

[社員表]

<u>社員番号</u>	社員氏名	部署コード(FK)	入社年
-------------	------	-----------	-----

[資格取得表]

<u>社員番号(FK)</u>	<u>取得資格コード(FK)</u>
-----------------	--------------------

[資格表]

<u>資格コード</u>	資格名
--------------	-----

[部署表]

部署コード	部署名
-------	-----

[部署指定資格表]

部署コード(FK)	資格コード(FK)	スコア
-----------	-----------	-----

<設問 2 > 部署内で社員ごとのスコアの合計を求める次の SQL 文の に入れるべき適切な字句を解答群から選べ。なお、表示順は、部署コードの昇順、合計スコアの降順とし、スコアの合計が同じ場合は、社員番号の昇順に表示する。

```
SELECT 社員表.部署コード, 社員表.社員番号, SUM(スコア) AS 合計スコア
FROM 社員表, 部署指定資格表, 資格取得表
WHERE  (3)
GROUP BY  (4)
ORDER BY  (5)
```

(3) の解答群

- ア. 社員表.社員番号 = 資格取得表.社員番号
AND 社員表.部署コード = 部署指定資格表.部署コード
- イ. 社員表.社員番号 = 資格取得表.社員番号
AND 社員表.部署コード = 部署指定資格表.部署コード
AND 資格表.資格コード = 部署指定資格表.資格コード
- ウ. 社員表.社員番号 = 資格取得表.社員番号
AND 資格取得表.取得資格コード = 部署指定資格表.資格コード
- エ. 社員表.社員番号 = 資格取得表.社員番号
AND 社員表.部署コード = 部署指定資格表.部署コード
AND 資格取得表.取得資格コード = 部署指定資格表.資格コード

(4) の解答群

- ア. 社員表.社員番号, 部署指定資格表.部署コード
- イ. 社員表.社員番号, 部署指定資格表.資格コード
- ウ. 社員表.部署コード, 社員表.社員番号
- エ. 部署指定資格表.部署コード, 社員表.社員番号

(5) の解答群

- ア. 社員表.社員番号, 合計スコア, 社員表.部署コード
- イ. 社員表.社員番号, 合計スコア DESC, 社員表.部署コード
- ウ. 社員表.部署コード, 合計スコア DESC, 社員表.社員番号
- エ. 社員表.部署コード DESC, 合計スコア DESC, 社員表.社員番号 DESC

<設問 3> レコードの追加に関する次の SQL 文の [] に入れるべき適切な字句を解答群から選べ。

新しい資格を資格表に登録するため、次の SQL 文を実行した。

資格コード：2081

資格名：情報スペシャリスト試験

[(6)] 資格表 (資格コード, 資格名)

[(7)] ('2081', '情報スペシャリスト試験')

(6), (7) の解答群

- ア. AS イ. AS SELECT ウ. INSERT INTO
エ. UPDATE オ. SET カ. VALUES

<設問 4> 次のレコードの追加に関する記述中の [] に入れるべき適切な字句の組合せを解答群から選べ。

資格表に未登録の資格を登録し、その資格を取得した社員と、その資格を部署指定資格表に加える部署を登録する場合は、最初に [(a)] に登録し、次に [(b)] の順に登録する。

(8) の解答群

	(a)	(b)
ア.	資格表	資格取得表 および 部署指定資格表
イ.	資格取得表	資格表 および 部署指定資格表
ウ.	社員表	資格取得表 および 部署指定資格表
エ.	部署指定資格表	資格表 および 資格取得表

問題5 次の情報セキュリティに関する各設問に答えよ。

＜設問1＞ 次のデジタル署名に関する記述中の□□□□に入れるべき適切な字句を解答群から選べ。

契約書などの書面に、当事者本人であることを証明するために署名や捺印することと同様に、デジタル化された文書に添付するのがデジタル署名である。これは、公開かぎ暗号方式を利用したもので、署名者の正当性を保証する仕組みである。署名者は□□(1)で署名を暗号化して送信し、受信者は□□(2)で復号することで、署名者(送信者)の正当性を確認できる。しかし、デジタル署名だけではかぎの信頼性まで確認できない。

そこで、署名者は第三者機関である認証局に自分の作成した公開かぎを登録して、デジタル証明書を発行してもらい、デジタル署名に添付する。デジタル証明書は□□(3)で暗号化されており、受信者は□□(4)で復号することで、送信者の公開かぎの信頼性を確認できる。

(1) ～ (4) の解答群

- | | |
|-------------|-------------|
| ア. 受信者の公開かぎ | イ. 受信者の秘密かぎ |
| ウ. 署名者の公開かぎ | エ. 署名者の秘密かぎ |
| オ. 認証局の公開かぎ | カ. 認証局の秘密かぎ |

＜設問2＞ 次の認証局に関する記述中の□□□□に入れるべき適切な字句を解答群から選べ。

認証局は、大きくは登録局と発行局という二つの機関に分けられる。登録局は申請を受け付け、申請者を審査する機関で、申請者に問題が無ければ発行局に伝達し、発行局が申請者にデジタル証明書を発行すると共に、デジタル証明書を保管するデータベースにも登録する。デジタル証明書には、申請者情報、□□(5)、有効期限、認証局情報などが含まれている。有効期限内であっても申請者の秘密かぎが盗まれてしまった場合などで、デジタル証明書を廃棄する場合がある。この場合も発行局が□□(6)として公開する。

(5) , (6) の解答群

- | | |
|--------------|----------------|
| ア. クライアント証明書 | イ. クライアントの機種情報 |
| ウ. 証明書失効リスト | エ. 証明書署名要求 |
| オ. 申請者の公開かぎ | カ. 申請者の秘密かぎ |

<設問 3 > 次の暗号化通信に関する記述中の に入れるべき適切な字句を解答群から選べ。

インターネットで情報を暗号化してやり取りする際のプロトコルが TLS である。SSL3.0 を基に規格化され、SSL の脆弱性が発見されてから TLS で運用されているが、SSL の名称が広く普及していたこともあり、現在も SSL や SSL/TLS と併記する名称が使われている。

TLS は、公開かぎ暗号方式、共通かぎ暗号方式、デジタル署名、デジタル証明書の技術を利用して実現する。

TLS によりクライアントと Web サーバ間で通信を始めるには、まず次のような手順で処理する。

- ① クライアントから Web サーバへリクエストを送信する。
- ② Web サーバは、デジタル証明書、デジタル署名、Web サーバの公開かぎなどが含まれたサーバ証明書をクライアントに送信する。
- ③ クライアントは、受け取ったデジタル証明書を基に、Web サーバの公開かぎが正当であるかを確認する。
- ④ クライアントは共通かぎを生成する
- ⑤ ④で生成した共通かぎを (7) で暗号化して Web サーバへ送信する。
- ⑥ Web サーバは受信した情報を (8) で復号する。

この後は、 (9) を使用した暗号化通信を行う。

(7) ~ (9) の解答群

- ア. Web サーバの公開かぎ
- ウ. 共通かぎ
- オ. 認証局の秘密かぎ

- イ. Web サーバの秘密かぎ
- エ. 認証局の公開かぎ

<メモ欄>

