

平成 21 年度 春期
システム監査技術者
午前Ⅱ 問題

試験時間

10:50 ～ 11:30 (40 分)

注意事項

1. 試験開始及び終了は、監督員の時計が基準です。監督員の指示に従ってください。
試験時間中は、退室できません。
2. 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。
3. この注意事項は、問題冊子の裏表紙に続きます。必ず読んでください。
4. 答案用紙への受験番号などの記入は、試験開始の合図があってから始めてください。
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25
選択方法	全問必須

6. 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) B 又は 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
----	--

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 アクセス権限を管理しているシステムの利用者 ID リストから、退職による権限喪失者が削除されていることを検証する手続として、最も適切なものはどれか。

ア アクセス権限削除申請書の全件について、利用者 ID リストから削除されていることを確認する。

イ 最新の利用者 ID リストの全件について、対応するアクセス権限削除申請書が存在しないことを確認する。

ウ 人事発令簿の退職者の全件について、利用者 ID リストから削除されていることを確認する。

エ 利用者 ID リストの更新履歴の全件について、対応するアクセス権限削除申請書の存在を確認する。

問2 データベースのインテグリティの維持に関する監査ポイントはどれか。

ア データベースのデータに不具合が発生した場合の障害回復手段が組み込まれているかどうか。

イ データベースの利用効率が適切であるかどうか。

ウ データ領域の使用領域と拡張領域のバランスが適切であるかどうか。

エ 利用者の要求に応じたレスポンスタイムが確保できているかどうか。

問3 “システム監査基準”の定める予備調査に関する記述のうち、適切なものはどれか。

ア 個別計画書を作成するために行う予備的な調査である。

イ 本調査に先立って、監査対象業務の実態を把握するために行う調査である。

ウ 本調査に先立って、被監査部門と監査計画を調整するために行う調査である。

エ 本調査を補完する目的で、本調査と並行して行う調査である。

問4 情報システムの可用性監査において、システム障害報告書に基づき再発防止策の効果をレビューする手続として、適切なものはどれか。

- ア 障害原因と障害発生時の停止時間の記載の有無の確認
- イ 障害報告書の承認体制と承認状況の確認
- ウ 前期及び当期の回復許容時間の予測値の比較
- エ 前期及び当期の障害原因別の障害発生件数と停止時間の比較

問5 “情報セキュリティ監査基準”における保証型監査と助言型監査に関する記述のうち、適切なものはどれか。

- ア 助言型監査とは、監査上の判断尺度として情報セキュリティ管理基準を利用し、情報セキュリティ上の問題点の指摘と改善提言は監査人の自由裁量で行う監査のことである。
- イ 助言型監査とは、監査対象の情報セキュリティに関するマネジメントやコントロールの適切な運用を目的として、情報セキュリティ上の問題点の検出と改善を命令する監査のことである。
- ウ 保証型監査とは、監査手続を実施した限りにおいて、監査対象の情報セキュリティに関するマネジメントやコントロールが適切であることを保証する監査のことである。
- エ 保証型監査とは、監査の結果としてインシデントが発生しないことをステークホルダに対して保証する監査のことである。

問6 情報戦略についてのシステム監査を行う場合、優先して監査すべき事項はどれか。

- ア 経営戦略との整合性を考慮しているか。
- イ 現行の情報戦略を反映しているか。
- ウ 最新の情報技術を取り入れているか。
- エ 情報戦略実現のための解決目標を設定しているか。

問7 システム監査技法の一つである並行シミュレーション法はどれか。

- ア 監査対象プログラムのある部分の機能を特定し、本番データと異なるデータを使って処理論理の正確性を確かめる方法
- イ 監査人が用意した検証用プログラムと監査対象プログラムに同一のデータを入力して、両者の実行結果を比較する方法
- ウ 正規の適用業務処理の中で、架空のテストデータを用い、システム機能の信頼性や効率性を検証する方法
- エ トランザクション処理を継続的に監視するために、監査人が用意した検証用プログラムをシステムに組み込んで本番データを処理する方法

問8 金融庁の財務報告に係る内部統制報告制度における IT に係る全般統制に該当するのはどれか。

- ア エラーの修正と再処理
- イ 外部委託に関する契約の管理
- ウ 業務別トランザクションデータの維持管理
- エ 入力情報の完全性、正確性、正当性などを確保する統制

問9 システム監査に関する記述のうち、適切なものはどれか。

- ア 公認会計士が任意の業務としてシステム監査を実施する場合がある。
- イ システム監査人は、公認会計士が兼務することが望ましい。
- ウ システム監査は、公認会計士による監査の一環として必ず実施されるものである。
- エ システム監査は内部監査であるので、公認会計士が実施することはない。

問10 内部統制として効果的な職務の分離の説明はどれか。

- ア 開発部門のプログラマが運用部門のオペレータを兼務しない。
- イ 購買管理で購入物品の検品と検品確認入力を同じ担当者が行わない。
- ウ 資材管理で資材の搬入確認と搬入確認入力を兼務しない。
- エ 電子送金システムでシステムの始動と送金操作を同じ担当者が行わない。

問11 システムの障害対策に関する記述のうち、不適切なものはどれか。

- ア サーバのディスク障害によってデータが破壊された場合を想定し、複数のサーバ間でデータの複製をもつ。
- イ 停電や落雷によるハードウェアの故障の範囲を限定するために、LAN 配線用サージ保護器を設置し、さらにネットワークを幾つかのセグメントに分割する。
- ウ ネットワーク管理ソフトウェアのバグによるシステムの停止を回避するために、複数の CPU を搭載したサーバを導入する。
- エ 不注意によるケーブルの切断によってネットワークが利用できなくなる範囲を最小限にとどめるために、スター型トポロジを採用する。

問12 IT サービスマネジメントを導入する際の手順はどれか。

- a 継続的改善方法の検討
- b 現状の把握
- c ビジョンの明確化
- d 目標達成状況の把握方法の検討
- e 目標達成方法の検討
- f 目標の設定

ア b→c→e→f→d→a

イ b→f→c→a→d→e

ウ c→b→f→e→d→a

エ c→f→b→a→d→e

問13 販売管理システム開発を受注した A 社が、不足する開発要員（プログラマ）を B 社からの派遣によって補うことにした。派遣先である A 社の行為のうち、労働者派遣法に照らして適切なものはどれか。

ア システム開発期間が長期になるので、B 社から派遣されるプログラマの派遣期間を3年とする契約を結ぶ。

イ 派遣期間中は作業負荷がかかることが予想されるので、B 社に対し20代男性の派遣を依頼する。

ウ 派遣されるプログラマ候補者の業務経歴書を提出させ、書類選考によって面接の対象となる候補者を絞り込む。

エ 労務管理実務に詳しい担当者がいないので、責任者を置かず派遣社員からの苦情処理をB社に依頼する。

問14 個人情報保護法で保護される個人情報の条件はどれか。

- ア 企業が管理している顧客に関する情報に限られる。
- イ 個人が秘密にしているプライバシーに関する情報に限られる。
- ウ 生存している個人に関する情報に限られる。
- エ 日本国籍の個人に関する情報に限られる。

問15 表は、CSR（Corporate Social Responsibility）をキャロルによる四つの責任分野に分類し、それぞれの企業活動例を示している。表中のcに入るものはどれか。

責任分野	企業活動例
a	法人税の納付
b	コンプライアンスの徹底
c	環境会計の導入
d	文化・芸術支援活動

- ア 経済的責任 イ 社会貢献責任 ウ 法的責任 エ 倫理的責任

問16 連結売上高総利益率は何%か。ここで、B社はA社の100%子会社で、仕入れはすべて親会社からであり、売上はすべて親会社以外である。また、期首、期末とも在庫はない。

A 社損益計算書		B 社損益計算書	
売上高	4,000	売上高	1,000
子会社売上高	800	売上原価	<u>800</u>
売上原価	<u>3,000</u>	売上総利益	<u>200</u>
売上総利益	<u>1,800</u>		

ア 34

イ 38

ウ 40

エ 56

問17 “学生”表と“学部”表に対し次のSQL文を実行した結果として、正しいものはどれか。

```
SELECT 氏名 FROM 学生,学部
WHERE 所属 = 学部名 AND 学部.住所 = '新宿'
```

学生

氏名	所属	住所
合田知子	理	新宿
青木俊介	工	渋谷
川内聡	人文	渋谷
坂口祐子	経済	新宿

学部

学部名	住所
理	新宿
工	新宿
人文	渋谷
経済	渋谷

ア

氏名
合田知子

イ

氏名
合田知子
青木俊介

ウ

氏名
合田知子
坂口祐子

エ

氏名
合田知子
青木俊介
坂口祐子

問18 TCP, UDP のポート番号を識別し, プライベート IP アドレスとグローバル IP アドレスとの対応関係を管理することによって, プライベート IP アドレスを使用する LAN の複数の端末が, 一つのグローバル IP アドレスを共有してインターネットにアクセスする仕組みはどれか。

ア IP スプーフィング

イ IP マルチキャスト

ウ NAT

エ NTP3

問19 インターネットを利用した VPN の説明として, 適切なものはどれか。

ア 暗号化技術などを利用して, インターネットを仮想的な専用ネットワークとして安全に利用する。

イ インターネットによって安価な国際電話網を実現するために利用される。

ウ デジタル通信ネットワーク ISDN を使って, 組織内のネットワークとインターネットを接続するために利用される。

エ 同一企業グループに属する複数の企業のイントラネットを, インターネットを用いて接続し, 公開可能な情報だけをやり取りする。

問20 DNS キャッシュポイズニングに分類される攻撃内容はどれか。

- ア DNS サーバのソフトウェアのバージョン情報を入手して、DNS サーバのセキュリティホールを特定する。
- イ PC が参照する DNS サーバに誤ったドメイン管理情報を注入して、偽装された Web サーバに PC の利用者を誘導する。
- ウ 攻撃対象のサービスを妨害するために、攻撃者が DNS サーバを踏み台に利用して再帰的な問合せを大量に行う。
- エ 内部情報を入手するために、DNS サーバが保存するゾーン情報をまとめて転送させる。

問21 情報システムのリスク分析に関する記述のうち、適切なものはどれか。

- ア リスクには、投機的リスクと純粹リスクとがある。情報セキュリティのためのリスク分析で対象とするのは、投機的リスクである。
- イ リスクの予想損失額は、損害予防のために投入されるコスト、復旧に要するコスト、及びほかの手段で業務を継続するための代替コストの合計で表される。
- ウ リスク分析では、現実が発生すれば損失をもたらすリスクが、情報システムのどこに、どのように潜在しているかを識別し、その影響の大きさを測定する。
- エ リスクを金額で測定するリスク評価額は、損害が現実のものになった場合の 1 回当たりの平均予想損失額で表される。

問22 機能要件と非機能要件のうち、機能要件を満たすために行う設計はどれか。

- ア 業務システムを開発するための開発環境を設計する。
- イ 業務の緊急度を分析して障害発生時の復旧時間を明確にする。
- ウ 業務を構成する要素間のデータの流れを明確にする。
- エ 部門業務を効率よく処理するための最適なサーバ配置を設計する。

問23 ハードウェアの保守点検及び修理作業を実施するときに、運用管理者が実施すべき、事前又は事後の確認に関する説明のうち、適切なものはどれか。

- ア システムが自動的に回復処置を行った障害については、障害前後のエラーログが残っているので、障害原因や対応処置の報告ではなく、ログの分析結果を確認する。
- イ 定期保守時の点検項目は事前に分かっているので、事前と事後の確認は省略できるが、作業の開始と終了については、保守作業者に確認する。
- ウ 予防保守を遠隔保守方式で行う場合、遠隔地のシステムへの影響は出ないので、作業内容などの事前確認は行わず、事後に作業実施結果を確認する。
- エ 臨時保守の場合、事前に保守作業者が障害の発生状況を確認したことを確認し、事後に障害原因や作業実施結果を確認する。

問24 ほかの技法では答えが得られにくい、未来予測のような問題に多く用いられ、(1)～(3)の手順に従って行われる予測技法はどれか。

- (1) 複数の専門家を回答者として選定する。
- (2) 質問に対する回答結果をフィードバックし、再度質問を行う。
- (3) 回答結果を統計的に処理し、確率分布とともに回答結果を示す。

ア クロスセクション法

イ シナリオライティング法

ウ 親和図法

エ デルファイ法

問25 バランススコアカードを説明したものはどれか。

ア 外部環境と内部環境の視点から、自社にとっての事業機会を導き出す手法

イ 計画、行動、評価、修正のサイクルで、戦略実行の管理を行うフレームワーク

ウ 財務、顧客、内部プロセス、成長と学習の視点から、経営戦略を支援する手法

エ ビジネス戦略を実現するために設定した、業務プロセスをモニタリングする指標

7. 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。
8. 問題冊子の余白などは、適宜利用して構いません。
9. 試験中、机の上に置けるもの及び使用できるものは、次のものに限ります。
なお、会場での貸出しは行っていません。
受験票、黒鉛筆又はシャープペンシル、鉛筆削り、消しゴム、定規、時計（アラームなど時計以外の機能は使用不可）、ハンカチ、ティッシュ
これら以外は机の上に置けません。使用もできません。
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、いかなる場合でも提出してください。回収時に提出しない場合は、採点されません。
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Ⅰの試験開始は 12:30 です。12:10 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。