

平成 20 年度 春期 システム監査技術者 午前 問題

試験時間

9:30 ~ 11:10 (1 時間 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。
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 55
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	<input type="radio"/> ア	<input type="radio"/> イ	<input checked="" type="radio"/>	<input type="radio"/> 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 RAID の分類において、ミラーリングを用いることで信頼性を高め、障害発生時には冗長ディスクを用いてデータ復元を行う方式はどれか。

- ア RAID1 イ RAID2 ウ RAID3 エ RAID4

問2 仮想記憶方式に関する記述のうち、適切なものはどれか。

ア LRU アルゴリズムは、使用後の経過時間が最長のページを置換対象とするページ置換アルゴリズムである。

イ アドレス変換をインデックス方式で行う場合は、主記憶に存在する全ページ分のページテーブルが必要になる。

ウ ページフォルトが発生した場合は、ガーベジコレクションが必要である。

エ ページングが繰り返されるうちに多数の小さな空きメモリ領域が発生することを、フラグメンテーションという。

問3 グリッドコンピューティングの利用形態に関する記述のうち、適切なものはどれか。

ア 多数の PC やサーバで集めたデータを、中央のサーバに送って集中処理をする。

イ 多数の PC やサーバに分散して格納されているデータのバックアップを、中央のサーバに取得する。

ウ 中央のサーバで、処理を並列処理可能な単位に分割し、それらを多数の PC やサーバで並列処理する。

エ 中央のサーバに集中して格納されているデータを、多数の PC やサーバで共有する。

問4 コンピュータによる伝票処理システムがある。このシステムは、伝票データをためる待ち行列をもち、M/M/1の待ち行列モデルが適用できるものとする。平均待ち時間が T 秒以上となるのは、処理装置の利用率が少なくとも何%以上となったときか。ここで、伝票データをためる待ち行列の特徴は次のとおりである。

- ・伝票データは、ポアソン分布に従って発生する。
- ・伝票データのたまる数に制限はない。
- ・1件の伝票データの処理時間は、平均 T 秒の指数分布に従う。

ア 33

イ 50

ウ 67

エ 80

問5 コンピュータグラフィックスの要素技術に関する記述のうち、適切なものはどれか。

- ア アンチエイリアシングは、周辺の画素との平均化演算などを施し、斜め線や曲線のギザギザを目立たなくする。
- イ メタボールは、光の相互反射を利用して物体表面の光のエネルギーを算出することで、表面の明るさを決定する。
- ウ ラジオシティは、光源からの光線の経路を計算することで光の反射や透過などを表現し、物体の形状を描画する。
- エ レイトレーシングは、物体を球やだ円体の集合として疑似的にモデル化する。

問6 再入可能（リエントラント）プログラムに関する記述のうち、適切なものはどれか。

- ア 再入可能プログラムは、局所変数をタスク単位に格納しなければならない。
- イ 再入可能プログラムは、逐次再使用可能プログラムから呼び出すことはできない。
- ウ 実行途中で待ち状態が発生するプログラムは、再入可能ではない。
- エ 逐次再使用可能なプログラムは、再入可能プログラムでもある。

問7 OSS（Open Source Software）の使用条件として、適切なものはどれか。

- ア 一定の試用期間が設けられ、試用期間後も継続して使用する場合は代金を支払わなければならない。
- イ 著作権を放棄した上で配布され、利用者は、無償で利用、改変、再配布などを行うことができる。
- ウ 無償で入手できるが、再配布や転載に許可が必要であり、商用利用禁止になっていて改変が許可されていない場合がある。
- エ ライセンス条件の下で、ソースコードを利用して作成したソフトウェアを譲渡又は販売できる。

問8 プログラムのテストに関する記述のうち、適切なものはどれか。

- ア 静的テストとは、プログラムを実行することなくテストする手法であり、コード検査、静的解析などがある。
- イ トップダウンテストは、仮の下位モジュールとしてのスタブを結合してテストするので、テストの最終段階になるまで全体に関係するような欠陥が発見されにくい。
- ウ ブラックボックステストは、分岐、反復などの内部構造を検証するため、すべての経路を通過するように、テストケースを設定する。
- エ プログラムのテストによって、プログラムにバグがないことを証明できる。

問9 ITIL のサービスデリバリーにおけるサービスレベル管理の説明はどれか。

- ア IT サービスを供給するために使用される IT 資産と資源を財務的に管理するプロセスである。
- イ 顧客と提供者の合意事項が達成できるように IT サービスの品質を維持し、改善するプロセスである。
- ウ サービスの品質を阻害する事象に対して、迅速に元のサービスレベルまで回復させるプロセスである。
- エ 必須となる IT インフラとサービス設備が、合意した期限内に回復できるようにするプロセスである。

問10 ソフトウェアの保守管理において、保守作業の生産性に影響しないものはどれか。

- ア 運用中に発生するソフトウェアの障害件数
- イ ソフトウェアの検証を行うときの難易度
- ウ ソフトウェアを変更するときの難易度
- エ プログラムやドキュメントの理解しやすさの度合い

問11 A 社の Web サーバは、認証局で生成した Web サーバ用のデジタル証明書を使って SSL 通信を行っている。A 社の Web サーバにアクセスした PC が、デジタル証明書を手に入れた後に認証局の公開鍵を利用する処理はどれか。

- ア 暗号化通信に利用する共通鍵を生成し、認証局の公開鍵で暗号化する。
- イ 認証局の公開鍵を使って、暗号化通信に利用する共通鍵を復号する。
- ウ 認証局の公開鍵を使って、デジタル証明書の正当性を検証する。
- エ 秘匿データを認証局の公開鍵で暗号化する。

問12 暗号解読のための攻撃法のうち、ブルートフォース攻撃はどれか。

- ア 与えられた1組の平文と暗号文の鍵候補を総当たりで解読を試みる。
- イ 暗号化関数の統計的な偏りを線形関数によって近似して解読を試みる。
- ウ 暗号化装置のソフトウェアやハードウェアの解析を行って解読を試みる。
- エ 異なる二つの平文とそれぞれの暗号文の差分を観測して解読を試みる。

問13 暗号方式に関する記述のうち、適切なものはどれか。

- ア AESは公開鍵暗号方式、RSAは共通鍵暗号方式の一種である。
- イ 共通鍵暗号方式では、暗号化鍵と復号鍵が同一である。
- ウ 公開鍵暗号方式を通信内容の秘匿に使用する場合は、暗号化鍵を秘密にして、復号鍵を公開する。
- エ デジタル署名に公開鍵暗号方式が使用されることはなく、共通鍵暗号方式が使用される。

問14 Xさんは、Yさんにインターネットを使って電子メールを送ろうとしている。電子メールの内容を秘密にする必要があるので、公開鍵暗号方式を使って暗号化して送信したい。電子メールの内容を暗号化するのに使用する鍵はどれか。

- | | |
|-----------|-----------|
| ア Xさんの公開鍵 | イ Xさんの秘密鍵 |
| ウ Yさんの公開鍵 | エ Yさんの秘密鍵 |

問15 作成者によってデジタル署名された電子文書に、タイムスタンプ機関がタイムスタンプを付与した。この電子文書を公開する場合のタイムスタンプの効果のうち、適切なものはどれか。

ア タイムスタンプの時刻以前に存在したことを示し、作成者が、電子文書の作成を否認することを防止する。

イ タイムスタンプの時刻以前に存在したことを示し、第三者が、電子文書を改ざんすることを防止する。

ウ タイムスタンプを付与した時刻以降に、作成者が、ほかの電子文書へ流用することを防止する。

エ タイムスタンプを付与した時刻以降に、第三者が、ほかの電子文書へ流用することを防止する。

問16 Webアプリケーションの脅威とそのセキュリティ対策の適切な組合せはどれか。

ア OS コマンドインジェクションを防ぐために、Webアプリケーションが発行するセッションIDを推測困難なものにする。

イ SQL インジェクションを防ぐために、Webアプリケーション内で問合せを作成する際にバインド機構を使用する。

ウ クロスサイトスクリプティングを防ぐために、外部から渡す入力データにWebサーバ内のファイル名を直接指定しない。

エ セッションハイジャックを防ぐために、Webアプリケーションからシェルを起動できないようにする。

問17 コンピュータフォレンジクスの説明として、適切なものはどれか。

- ア あらかじめ設定した運用基準に従って、メールサーバを通過する送受信メールをフィルタリングすること
- イ 磁気ディスクなどの書換え可能な記憶媒体を単に初期化するだけでは復元される可能性があるため、覆い隠すようにデータを上書きすること
- ウ ネットワークやホストに対する外部からの攻撃や侵入を検出し、管理者に通報すること
- エ 不正アクセスなどコンピュータに関する犯罪の法的な証拠性を明らかにするために、原因究明に必要な情報を収集して分析すること

問18 パケットフィルタリング方式の適用によって実現できるものはどれか。

- ア ftp サービスで転送できるファイルとできないファイルを識別し、制御できる。
- イ 通常モードで接続する ftp サービスの使用だけを許可できる。
- ウ 特定のポートの通過を禁止して、ネットワークを介した telnet によるログインを禁止できる。
- エ 利用する権限をもっている対象者だけに、telnet サービスの使用を許可できる。

問19 パケットフィルタリング型ファイアウォールがルール一覧に示したアクションに基づいてパケットを制御する場合、パケット A に対する処理はどれか。ここで、ファイアウォールでの処理は、ルール一覧に示す番号の 1 から順に行い、一つのルールが適用された場合には残りのルールは適用されない。

ルール一覧

番号	送信元 アドレス	送信先 アドレス	プロトコル	送信元 ポート	送信先 ポート	アクション
1	10.1.2.3	*	*	*	*	通過禁止
2	*	10.2.3.*	TCP	*	25	通過許可
3	*	10.1.*	TCP	*	25	通過許可
4	*	*	*	*	*	通過禁止

注 * は任意のパターンを表す。

パケット A

送信元 アドレス	送信先 アドレス	プロトコル	送信元 ポート	送信先 ポート
10.1.2.3	10.2.3.4	TCP	2100	25

- ア 番号 1 によって、通過が禁止される。
- イ 番号 2 によって、通過が許可される。
- ウ 番号 3 によって、通過が許可される。
- エ 番号 4 によって、通過が禁止される。

問20 JIS Q 27001:2006 における情報システムのリスクとその評価に関する記述のうち、適切なものはどれか。

ア 脅威とは、脆弱性が顕在化する確率のことであり、情報システムに組み込まれた技術的管理策によって決まる。

イ 脆弱性とは、情報システムに対して悪い影響を与える要因のことであり、自然災害、システム障害、人為的過失及び不正行為に大別される。

ウ リスクとは、脅威が情報資産の脆弱性につけ込み、情報資産に損失又は損害を与える可能性のことである。

エ リスク評価とは、リスクの大きさを判断して対策を決めることであり、リスク回避とリスク低減の二つに分類される。

問21 金融庁の“財務報告に係る内部統制の評価及び監査の基準”における内部統制に係る有する者の役割と責任に関する記述のうち、適切なものはどれか。

ア 監査役は、取締役の職務の執行に対する監査の一環として、内部統制の整備及び運用状況を監視、検証する。

イ 公認会計士は、内部統制の整備及び運用に係る基本方針を決定する。

ウ 取締役会は、経営者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。

エ 内部監査人は、内部統制の枠組みから独立した立場で、内部統制の整備及び運用状況を検討、評価し、必要に応じて、その改善を促す。

問22 経済産業省の“システム管理基準”に該当する記述はどれか。

- ア ITIL という IT サービスの品質向上のためのガイドラインを基に作成した、IT サービスマネジメントに関するフレームワークである。
- イ 一般基準、実施基準及び報告基準から構成されており、一般基準ではシステム監査人の独立性や職業倫理について規定されている。
- ウ システム監査業務の品質を確保し、有効かつ効率的に監査を実施することを目的とした監査人の行為規範である。
- エ 情報システム戦略に基づき、効果的な情報システム投資のための、また、リスクを低減するためのコントロールを適切に整備・運用するための実践規範である。

問23 JIS Q 9000:2006 で規定されている妥当性確認はどれか。

- ア 客観的証拠を提示することによって、規定要求事項が満たされていることを確認すること
- イ 客観的証拠を提示することによって、特定の意図された用途又は適用に関する要求事項が満たされていることを確認すること
- ウ 手順に従って特性を明確にすること
- エ 必要に応じて測定、試験又はゲージ合わせを伴う、観察及び判定による適合性を評価すること

問24 JIS Q 27001:2006 における ISMS の確立に必要な事項①～③の順序関係のうち、適切なものはどれか。

- ① 適用宣言書の作成
- ② リスク対応のための管理目的及び管理策の選択
- ③ リスクの分析と評価

ア ①→②→③

イ ①→③→②

ウ ②→③→①

エ ③→②→①

問25 セキュリティ対策に関連する標準又は規格に関する記述のうち、適切なものはどれか。

ア JIS Q 27002 は、製品やシステムのセキュリティ機能及び実装のレベルを技術面から評価する基準である。

イ JIS X 5070 は、セキュリティ組織から設備管理に及ぶ運用管理全体の規約を定めた実践規範であり、アクセス制御も評価対象とする。

ウ JIS X 5731-8 (ITU-T X.509) は、XML 文書の暗号化とデジタル署名関連の規格であり、Web 関連技術における HTTP や HTML の標準化を行う任意団体 W3C が任意団体 IETF と協力して定めたものである。

エ インターネットの各種技術の標準化を進めている任意団体 IETF は技術仕様を RFC として発行しており、セキュリティ分野には RADIUS や LDAP の仕様がある。

問26 職能部門別組織を説明したものはどれか。

- ア 業務遂行に必要な機能と利益責任を、製品別、顧客別又は地域別にもつことによって、自己完結的な経営活動が展開できる組織である。
- イ 構成員が、自己の専門とする職能部門と特定の事業を遂行する部門の両方に所属する組織である。
- ウ 購買・生産・販売・財務などの仕事の特性によって、部門を編成した組織である。
- エ 特定の課題のもとに各部門から専門家を集めて編成し、期間と目標を定めて活動する一時的かつ柔軟な組織である。

問27 現在の動向から未来を予測したり、システム分析に使用したりする手法であり、専門的知識や経験を有する複数の人にアンケート調査を行い、その結果を互いに参照した上で調査を繰り返して、集団としての意見を収束させる手法はどれか。

- | | |
|------------|-------------|
| ア 因果関係分析法 | イ クロスセクション法 |
| ウ 時系列回帰分析法 | エ デルファイ法 |

問28 アクションラーニングを説明したものはどれか。

- ア ある企業や業界で起こった事例を基にして、問題解決や意思決定について議論する学習方法
- イ 自社が直面する経営課題に対して参加者が自ら施策を立案し、問題解決に向けた取り組みを実践していく学習方法
- ウ シミュレーション機能を使用して、販売、製造、人事、財務における意思決定を模擬体験する学習方法
- エ 特定の状況設定の下で、様々な立場の役割を演じて、それぞれの問題点や解決方法を考える学習方法

問29 経済産業省の“システム管理基準”で示された“全体最適化”に含まれる作業はどれか。

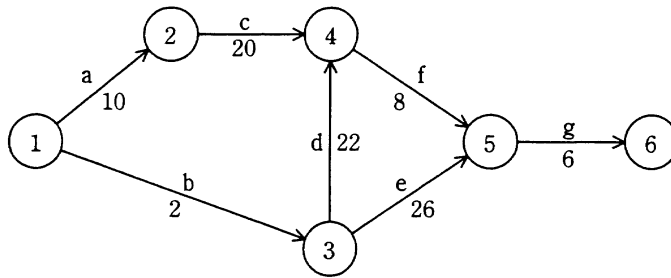
- ア 委託先を含む開発体制の策定
- イ 開発スケジュールの策定
- ウ 個別システムのハードウェアの導入スケジュールの策定
- エ 情報システム基盤の整備計画の策定

問30 今年度の A 社の営業実績を表に示す。来年度、固定費が 5%上昇し、販売単価が 5%低下すると予測されるとき、今年度と同じ営業利益を確保するためには、最低何台を販売する必要があるか。

販売台数	2,500 台
販売単価	200 千円
固定費	150,000 千円
変動費	100 千円/台

- ア 2,575 イ 2,750 ウ 2,778 エ 2,862

問34 図はあるプロジェクトの作業工程（a～g）を示したものである。クリティカルパス上にある作業のうち、最長の作業に要する日数を半分に短縮した場合、短縮後のプロジェクトの所要日数は、何日になるか。ここで、矢線に示す数字は各作業の所要日数を表す。



ア 34

イ 38

ウ 39

エ 44

問35 電子政府におけるワンストップサービスの実現と普及のための要件はどれか。

- ア PC やインターネットを利用することが前提となるので、デジタルディバイドに対する施策が必要になる。
- イ 一般市民に的を絞ったサービスなので、生活上の各種イベントを想定して、ワンストップ化を実現することが求められる。
- ウ 一つのポータルサイトにアクセスすることで様々な情報やサービスを得られるように、実際のサービス提供者も統合されている必要がある。
- エ ワンストップ化を実現するためには、個人情報を集約し、それらの情報をいろいろな目的に利用することが求められる。

問36 開発されたプログラムの著作権の帰属に関する規定が契約に定められていないとき、著作権の原始的な帰属はどのようになるか。

- ア 請負の場合は発注先に、派遣の場合は派遣先に帰属する。
- イ 請負の場合は発注先に、派遣の場合は派遣元に帰属する。
- ウ 請負の場合は発注元に、派遣の場合は派遣先に帰属する。
- エ 請負の場合は発注元に、派遣の場合は派遣元に帰属する。

問37 労働者派遣法に適合するものはどれか。

- ア 派遣契約の内容にかかわらず合理的な理由がある場合には、派遣先の作業指示者の判断で派遣労働者に残業を命じることができる。
- イ 派遣先の事業所に属する従業員はだれでも、派遣労働者に業務命令を行うことができる。
- ウ 労働者派遣法で認められた業務であれば、派遣先の判断で派遣労働者の業務内容を変更できる。
- エ 労働者派遣法で認められた特殊な技能を要する業務であれば、同一人の派遣を3年を超えて行うことができる。

問38 月100時間を超える時間外労働など、省令に定められる要件に該当する従業員がいる場合、企業のとるべき措置として労働安全衛生法で規定されているものはどれか。

- ア 安全衛生委員による就業状況の日次確認を実施する。
- イ 医師による面接指導を受けさせる。
- ウ 強制的に有給休暇を取得させる。
- エ 労働基準監督署に改善策を含めた報告書を提出する。

問39 A社はB社に対して業務システムの開発を委託し、A社とB社は請負契約を結んでいる。作業の実態から、偽装請負とされる事象はどれか。

ア A社の従業員が、B社を作業場所として、A社の責任者の指揮命令に従ってシステムの検証を行っている。

イ A社の従業員が、B社を作業場所として、B社の責任者の指揮命令に従ってシステムの検証を行っている。

ウ B社の従業員が、A社を作業場所として、A社の責任者の指揮命令に従って設計書を作成している。

エ B社の従業員が、A社を作業場所として、B社の責任者の指揮命令に従って設計書を作成している。

問40 コンピュータの不正利用に関する条文を含む法規はどれか。

ア 刑法

イ 個人情報保護法

ウ 著作権法

エ 不正競争防止法

問41 アプリケーションプログラムに識別コード及びパスワードによるアクセスコントロールを組み込んだ。この場合、コントロール可能なリスクはどれか。

ア 通信上のデータの盗聴

イ データの入力エラー

ウ ハードウェアの物理的な破壊

エ ファイル、データ内容の改ざん

問42 “システム監査基準”の前文に記述されている基準の利用の目的として、適切なものはどれか。

- ア システム監査業務の品質を確保し、有効かつ効率的に監査を実施することを目的とした監査人の行為規範である。
- イ システム監査人が監査上の判断の尺度として用いる基準であって、情報セキュリティ監査基準と一体となって機能する基準である。
- ウ 情報システムに保証を付与することを目的とした監査でなく、改善のための助言を行うことを目的とした監査に利用する基準である。
- エ 組織体の外部者に監査を依頼するシステム監査でなく、組織体の内部監査部門等が実施するシステム監査に利用する基準である。

問43 “システム監査基準”の一般基準に規定するシステム監査人の精神上的独立性はどれか。

- ア 監査対象から独立し、被監査主体と身分上、密接な利害関係を有しない。
- イ 職業倫理に従い、誠実に業務を実施する。
- ウ 正当な理由なく、監査の業務上知り得た秘密を他に開示しない。
- エ 偏向を排し、常に公正かつ客観的に監査判断を行う。

問44 システム監査の手順に関する記述のうち、適切なものはどれか。

- ア 監査作業は、予備調査、本調査、評価・結論、指摘事項に対する改善の順に実施する。
- イ 評価・結論の作業は、監査担当者による評価、被監査部門による評価、監査責任者による評価を経て、最終結論を下す。
- ウ 本調査の作業手順は、現状の確認、監査証拠の入手、証拠能力の評価の順に行う。
- エ 予備調査の作業は、同業他社の状況調査、被監査部門の過去の監査結果の評価、サンプリングによる実地調査の順に行う。

問45 システム監査において、監査証拠となるものはどれか。

- ア システム監査チームが監査意見を取りまとめるためのミーティングの議事録
- イ システム監査チームが監査報告書に記載した指摘事項
- ウ システム監査チームが作成した個別監査計画書
- エ システム監査チームが被監査部門から入手したシステム運用記録

問46 “システム管理基準”で定めている、運用業務におけるソフトウェア管理に該当するものはどれか。

- ア プログラムからの出力情報の利用状況を記録し、定期的に分析する。
- イ プログラムで用いるデータファイルへのアクセスをコントロールする。
- ウ プログラムの違法コピーが発生しないよう教育する。
- エ プログラムのテスト結果を記録し保管する。

問47 システム監査報告書に記載された監査意見のうち、保証意見はどれか。

- ア 販売管理システムに係る安全性のコントロールに重大な不備があり、改善提案のように改善すべきである。
- イ 販売管理システムに係る効率性のコントロールは、業務処理に重大な影響を与える可能性があり、緊急の改善が必要である。
- ウ 販売管理システムに係る信頼性のコントロールについて、被監査部門と合意した手続によって調査を行った結果を、指摘事項として掲げた。
- エ 販売管理システムに係る信頼性のコントロールは、システム管理基準に照らして、指摘事項に挙げた不備を除いて有効に機能している。

問48 監査調書はどれか。

- ア 監査人が行った監査手続の実施記録であり、監査意見の根拠となるもの
- イ 監査人が監査実施に当たり、被監査部門などへ提出する監査人自身のセキュリティ誓約書をまとめたもの
- ウ 監査人が検討に利用した基準書、ガイドラインをまとめたもの
- エ 監査人が判断根拠とする資料であり、監査報告書とともに公表するよう義務付けられたもの

問49 表はコンピュータを利用して行うシステム監査技法についてまとめたものである。

(1)～(4)の組合せとして適切なものはどれか。

技 法	主な機能					
	システム のテスト	(1)	(2)	(3)	(4)	稼働中のオンラインシ ステムからのデータ抽出
テストデータ法	○					
汎用監査ソフトウェア法					○	
組込み監査モジュール法					○	○
ITF 法	○	○				
並行シミュレーション法	○		○			
スナップショット法			○			
トレーシング法			○			
コード比較法				○		

	(1)	(2)	(3)	(4)
ア	稼働中オンライン システムのテスト	プログラムの検証	データの抽出	プログラムロジッ クの分析
イ	稼働中オンライン システムのテスト	プログラムロジッ クの分析	プログラムの検証	データの抽出
ウ	データの抽出	稼働中オンライン システムのテスト	プログラムロジッ クの分析	プログラムの検証
エ	データの抽出	プログラムロジッ クの分析	稼働中オンライン システムのテスト	プログラムの検証

問50 システム監査の個別計画書の記載内容を説明したものはどれか。

- ア 個別計画書に記述される監査時期，監査日程には，本調査だけでなく，予備調査や監査結果の報告会，フォローアップも含める。
- イ 個別計画書に記述される監査手続とは，監査項目に対応した監査の基本方針のことである。
- ウ 個別計画書の監査対象ごとに重点監査テーマが設定され，記載されており，システム監査の方針となる。
- エ 個別計画書は監査の具体的な実行計画なので，計画策定後はその内容をたとえ組織体の長の意向であっても変更すべきではない。

問51 予備調査で実施するシステム監査手続はどれか。

- ア アンケート調査を行い，監査対象に対する被監査部門の管理者及び担当者のリスクの認識についての情報を収集する。
- イ 監査対象に関する手順書や実施記録及び被監査部門から入手した監査証拠に基づいて，指摘事項をまとめる。
- ウ 被監査部門の管理者の説明を受けながら，被監査部門が業務を行っている現場を実際に見て，改善提案の実現可能性を確かめる。
- エ 被監査部門の担当者に対して，監査手続書に従ってヒアリングを行い，監査対象の実態を詳細に調査する。

問52 情報システムのコントロールの評価を整備状況の評価と運用状況の評価に分けたとき、ユーザのシステムへのログインパスワード管理について、運用状況の評価に該当するものはどれか。

- ア システム仕様書の承認ルールを閲覧して、パスワード管理方針に基づいた設計が行われていることを確認する。
- イ システム部門の責任者への質問によって、パスワード管理に関する会社の方針を確認する。
- ウ パスワード管理マニュアルを閲覧して、パスワード設定ルールを確認する。
- エ パスワードを管理しているファイルを出力し、パスワードの設定状況を確認する。

問53 アクセス制御を監査するシステム監査人のとった行動のうち、適切なものはどれか。

- ア ソフトウェアに関するアクセス制御の管理表の作成と保管
- イ データに関するアクセス制御の管理状況の確認
- ウ ネットワークに関するアクセス制御の管理方針の制定
- エ ハードウェアに関するアクセス制御の運用管理の実施

問54 A社は、自社のシステム開発課長の指揮監督下でB社のプログラマーが開発する形態の契約を行う。システム監査の指摘事項のうち、適切なものはどれか。

ア B社が一般労働者派遣事業の許可を得ていない場合、派遣契約はできないので、請負契約に改める必要がある。

イ 請負契約であり、B社に対してはコーディング業務に限定して発注する必要がある。

ウ 請負契約であり、著作権の帰属があいまいになるので、法人著作である旨と著作者人格権とを、A社の権利として、契約条項に記載する必要がある。

エ 派遣契約であり、B社のプログラマーがA社の著作権を侵害した場合の措置に関する規定を設けておく必要がある。

問55 リスクアプローチに基づく監査において、固有リスクと統制リスクのレベルが高く、その結果許容できる発見リスクを低く抑えなければならない場合、監査手続を決めるに当たって監査人が採用すべき対応はどれか。ここで、監査リスクモデルは次式とする。

$$\text{監査リスク} = \text{固有リスク} \times \text{統制リスク} \times \text{発見リスク}$$

ア 外部証拠の入手範囲の拡大

イ 各種規程類の閲覧範囲の拡大

ウ 監査日数の短縮

エ サンプル数の縮小

[メモ用紙]

7. 途中で退室する場合には、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室してください。

退室可能時間	10:30 ~ 11:00
--------	---------------

8. 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。
9. 問題冊子の余白などは、適宜利用して構いません。
10. 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が付いているものは不可）、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。
11. 試験終了後、この問題冊子は持ち帰ることができます。
12. 答案用紙は、いかなる場合でも、すべて提出してください。回収時に提出しない場合は、採点されません。
13. 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。
14. 午後Ⅰの試験開始は 12:10 ですので、11:50 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。