AU

令和４年度　秋期
システム監査技術者試験
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. 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。
4. 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

5. 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) 答案用紙は光学式読取り装置で読み取った上で採点しますので，B 又は HB の黒鉛筆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。マークの濃度がうすいなど，マークの記入方法のとおり正しくマークされていない場合は，読み取れないことがあります。特にシャープペンシルを使用する際には，マークの濃度に十分注意してください。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) 受験番号欄に受験番号を，生年月日欄に受験票の生年月日を記入及びマークしてください。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，採点されないことがあります。生年月日欄については，受験票の生年月日を訂正した場合でも，訂正前の生年月日を記入及びマークしてください。
   (3) 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。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。

〔例題〕　秋期の情報処理技術者試験が実施される月はどれか。

ア　8　　イ　9　　ウ　10　　エ　11

正しい答えは“ウ　10”ですから，次のようにマークしてください。

例題	㋐ ㋑ ● 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　情報システムを対象としたデューデリジェンスの説明として，適切なものはどれか。

ア　企業買収などの重要な判断を行う場合に，買収などの対象となる企業の情報システムの価値やリスクを評価すること

イ　情報システムの入力，処理など，日常業務プロセスの信頼性を確保すること

ウ　情報セキュリティに係るリスクマネジメントを構築すること

エ　データにおける個人情報保護などの法令遵守を確保すること

問2　システム監査において実施される“試査”に該当するものはどれか。

ア　監査対象に最も適合した監査手続を決定するために，幾つかの監査技法を試行する。

イ　計算モジュールの正確性を確認するために，ソースプログラムをレビューする。

ウ　全てのトランザクションデータに監査手続を試験的に適用し，その処理の正当性について判断する。

エ　抽出した一定件数のトランザクションデータに監査手続を適用し，データ全件の正当性について判断する。

問３　システム管理基準（平成 30 年）では，前文において同基準の活用における留意点について記述している。記述内容として，適切なものはどれか。

ア　システム管理及びシステム監査の主旨を実現するためには，同基準にのっとって網羅的に管理項目を適用しなければならない。

イ　情報セキュリティの監査・管理を実施する場合には同基準ではなく，情報セキュリティ管理基準に基づいて監査・管理を実施しなければならない。

ウ　大企業だけでなく，中小企業向けの情報システム化戦略，情報システム化実践に関わる適切な自己診断及び監査にも使用できる。

エ　同基準を基に企業などが独自の管理基準を策定する場合には，同基準に規定された管理項目を，可能な限りそのまま採用することによって，管理の有効性を高める。

問４　システム監査基準（平成 30 年）における“フォローアップ”の説明として，適切なものはどれか。

ア　監査対象部門が，監査報告書の指摘事項及び改善勧告を基に改善実施計画の策定を行うこと

イ　監査部門の責任者が，監査報告書を基に監査の実施状況と指摘事項の妥当性を確認すること

ウ　システム監査人が，監査報告書に記載した改善提案の実施状況に関する情報を収集し，改善状況をモニタリングすること

エ　システム監査人が，時間の関係で調査が終了しなかった監査項目を追跡調査して報告すること

問５　システム監査チームが監査結果の評価を行ったとき，一部の項目について，調査不足から監査人の意見が分かれた。この場合の監査チームの対応として，最も適切なものはどれか。

ア　意見の統一を図るために追加の監査手続を実施する。
イ　監査報告書を提出しない。
ウ　多数決で意見を一つにまとめる。
エ　分かれた意見を監査報告書に列挙する。

問６　プライバシーマークを取得しているＡ社は，個人情報管理台帳の取扱いについて内部監査を行った。判明した状況のうち，監査人が，指摘事項として監査報告書に記載すべきものはどれか。

ア　個人情報管理台帳に，概数でしかつかめない個人情報の保有件数は概数だけで記載している。
イ　個人情報管理台帳に，個人情報の名称，内容，利用範囲などの項目に加えて，個人情報の保管場所，保管方法，保管期限を記載している。
ウ　個人情報管理台帳の機密性を守るための保護措置を講じている。
エ　個人情報管理台帳の見直しは，新たな個人情報の取得があった場合にだけ行っている。

問７　JIS Q 27002:2014（情報セキュリティ管理策の実践のための規範）では，運用システムに対する監査活動の影響を最小限にするための管理策及び実施の手引を定めている。その中で守ることが最も望ましいとされている事項はどれか。

ア　運用システムに影響を与えないよう，監査におけるテストについては，アクセス監視やログ取得の対象外とする。

イ　運用システムや当該システム上のデータへのアクセスに関する監査要求事項については，当該システムの運用担当者に限定して同意を得る。

ウ　監査におけるテストがシステムの可用性に影響する可能性がある場合は，当該テストを営業時間内に実施する。

エ　監査におけるテストでソフトウェア及びデータにアクセスする場合は，読出し専用のアクセスに限定する。

問８　システム管理基準（平成 30 年）において，経営陣が IT ガバナンスを成功に導くために採用することが望ましい原則としているものはどれか。

ア　監視，情勢判断，意思決定，行動

イ　計画，組織化，命令，調整，統制

ウ　顧客重視，リーダーシップ，人々の積極的参加，プロセスアプローチ，改善，客観的事実に基づく意思決定，関係性管理

エ　責任，戦略，取得，パフォーマンス，適合，人間行動

問９　金融庁“財務報告に係る内部統制の評価及び監査の基準（令和元年）”における，内部統制の基本的要素である“統制活動”はどれか。

ア　経営者の命令及び指示が適切に実行されることを確保するために定める方針及び手続である。

イ　組織の気風を決定し，組織内の全ての者の統制に対する意識に影響を与えるものである。

ウ　組織目標の達成を阻害する要因をリスクとして識別，分析及び評価し，適切な対応を行うプロセスである。

エ　必要な情報が識別，把握及び処理され，組織内外及び関係者相互に正しく伝えられることを確保することである。

問10　金融庁“財務報告に係る内部統制の評価及び監査に関する実施基準（令和元年）”に基づき，今年度改修した“自動化されたITに係る業務処理統制（ITAC）”の整備状況が有効であるとき，人手による内部統制よりも，サンプル数を減らし，サンプリングの対象期間を短くするなどITACの運用状況の評価作業を減らすことができる条件として，最も適切なものはどれか。

ア　ITACの前年度の運用状況の評価が有効である。

イ　ITに係る全般統制が有効である。

ウ　人手による業務処理統制の運用状況が有効である。

エ　人手による業務処理統制の整備状況が有効である。

問11　紙型，IC カード型又はサーバ型の前払式支払手段（プリペイドカード，電子マネーなど）の発行者に対し，その発行業務に係る情報の漏えい，滅失又は毀損の防止措置を求める法律はどれか。

ア　資金決済法　　イ　消費者契約法

ウ　電子帳簿保存法　　エ　特定商取引法

問12　バックアップサイトを用いたサービス復旧方法の説明のうち，ウォームスタンバイの説明として，最も適切なものはどれか。

ア　同じようなシステムを運用する外部の企業や組織と協定を結び，緊急時には互いのシステムを貸し借りして，サービスを復旧する。

イ　緊急時にはバックアップシステムを持ち込んでシステムを再開し，サービスを復旧する。

ウ　常にデータの同期が取れているバックアップシステムを用意しておき，緊急時にはバックアップシステムに切り替えて直ちにサービスを復旧する。

エ　バックアップシステムを用意しておき，緊急時にはバックアップシステムを起動して，データを最新状態にする処理を行った後にサービスを復旧する。

問13　システムAとシステムBのフルバックアップのデータ量は，それぞれ400Gバイトと600Gバイトである。次の条件でバックアップデータを磁気テープに記録する場合に，システムAとシステムBとで必要となる磁気テープの本数は，それぞれ最少で何本か。

〔条件〕

・毎週，日曜日にフルバックアップを行った後，月曜日から土曜日までは毎日，差分バックアップを行う。この1週間分のデータをバックアップデータの1世代として管理する。
・バックアップデータは，3世代分を確保する。
・1本の磁気テープには複数の世代のバックアップデータが記録できる。
・1世代のバックアップデータは，複数の磁気テープにまたがって記録できる。
・1週間分の差分バックアップのデータ量の合計は，フルバックアップのデータ量の25%である。
・1本の磁気テープに記録できるデータ量は，1,000Gバイトである。
・不要になったバックアップデータだけとなった磁気テープは，再利用する。
・磁気テープ中の，ブロック間の使用できないギャップ領域は考慮しない。

	システムAの磁気テープの本数	システムBの磁気テープの本数
ア	2	3
イ	2	4
ウ	3	4
エ	3	5

問14　JIS X 9251:2021 において，個人識別可能情報の処理に関する潜在的なプライバシー影響の，特定，分析，評価，協議，伝達及び対応の計画を立てるための全体的なプロセスと定義されているものはどれか。

ア　eKYC　　イ　GDPR　　ウ　PIA　　エ　PII

問15　インターネットのショッピングサイトで，商品の広告をする際に，商品の販売価格，商品の代金の支払時期及び支払方法，商品の引渡時期，売買契約の解除に関する事項などの表示を義務付けている法律はどれか。

ア　商標法　　イ　電子契約法

ウ　特定商取引法　　エ　不正競争防止法

問16　コンティンジェンシー理論の説明はどれか。

ア　いかなる状況でも最適な組織形態は存在せず，組織の在り方は個々の企業が置かれた外部環境に依存するという考え方

イ　意思決定は，選択機会，問題，解及び参加者という諸要素が偶発的に結びついて行われるという考え方

ウ　事業計画には，災害などの不測の事態を想定した基本的な対応方針をあらかじめ組み込んでおくという考え方

エ　組織形態は個々の企業が採用する経営戦略に応じて決定され，戦略が組織形態に先行するという考え方

問17　AES の特徴はどれか。

ア　鍵長によって，段数が決まる。

イ　段数は，6 段以内の範囲で選択できる。

ウ　データの暗号化，復号，暗号化の順に 3 回繰り返す。

エ　同一の公開鍵を用いて暗号化を 3 回繰り返す。

問18　公開鍵暗号方式を使った暗号通信をｎ人が相互に行う場合，全部で何個の異なる鍵が必要になるか。ここで，一組の公開鍵と秘密鍵は２個と数える。

ア　$n+1$　　イ　$2n$　　ウ　$\frac{n(n-1)}{2}$　　エ　n^2

問19　マルウェアの検出手法であるビヘイビア法を説明したものはどれか。

ア　あらかじめ特徴的なコードをパターンとして登録したマルウェア定義ファイルを用いてマルウェア検査対象と比較し，同じパターンがあればマルウェアとして検出する。

イ　マルウェアに感染していないことを保証する情報をあらかじめ検査対象に付加しておき，検査時に不整合があればマルウェアとして検出する。

ウ　マルウェアへの感染が疑わしい検査対象のハッシュ値と，安全な場所に保管されている原本のハッシュ値を比較し，マルウェアを検出する。

エ　マルウェアへの感染によって生じるデータの読込みの動作，書込みの動作，通信などを監視して，マルウェアを検出する。

問20　ISP “A” 管理下のネットワークから別の ISP “B” 管理下の宛先に SMTP で電子メールを送信する。電子メール送信者が SMTP-AUTH を利用していない場合，スパムメール対策 OP25B によって遮断される電子メールはどれか。

ア　ISP “A” 管理下の固定 IP アドレスの PC から送信しようとしたが，受信者の承諾を得ていなかった広告の電子メール

イ　ISP “A” 管理下の固定 IP アドレスの PC から送信しようとしたが，送信元 IP アドレスが DNS で逆引きできなかった電子メール

ウ　ISP “A” 管理下の動的 IP アドレスの PC から ISP “A” のメールサーバを経由して送信される電子メール

エ　ISP “A” 管理下の動的 IP アドレスの PC から ISP “A” のメールサーバを経由せずに直接送信される電子メール

問21　データベースのデータを更新するトランザクションが，実行途中で異常終了したとき，更新中のデータに対して行われる処理はどれか。

ア　異常終了時点までのトランザクションの更新ログ情報を破棄することによって，データをトランザクション開始前の状態に回復する。

イ　チェックポイント時点からコミットが完了しているトランザクションの更新ログ情報を使ってロールフォワードすることによって，データを回復する。

ウ　トランザクションの更新ログ情報を使い異常終了時点までロールフォワードすることによって，データを回復する。

エ　トランザクションの更新ログ情報を使いロールバックすることによって，データをトランザクション開始前の状態に回復する。

問22　DNSSEC に関する記述として，適切なものはどれか。

ア　DNS サーバへの DoS 攻撃を防止できる。

イ　IPsec による暗号化通信が前提となっている。

ウ　代表的な DNS サーバの実装である BIND の代替として使用する。

エ　デジタル署名によって DNS 応答の正当性を確認できる。

問23　JIS X 0153:2015（利用者用文書類の設計者及び作成者のための要求事項）によれば，システム及びソフトウェアの利用者用文書類の利用モードには“教習モード”及び“参照モード”がある。“参照モード”の利用者用文書に対する要求事項として，適切なものはどれか。

〔教習モード〕

ソフトウェアの利用経験のない人が作業を遂行できるようにするために，作業を実行するときにソフトウェアの使用法を教える利用モード

〔参照モード〕

ソフトウェアの機能に慣れている利用者のために，選択した要素の全ての事実を含み，特定の情報への迅速なアクセスを提供する利用モード

ア　エラーメッセージの説明には，問題の識別，推定される原因，及び利用者が行うことが望ましい是正処置を含める。

イ　ソフトウェアの命令については，利用者が一般的な作業で使用する命令の情報だけを記述する。

ウ　文書の章立ては，簡単な作業を複雑な作業の前に，一般的な作業を頻繁には行わない作業の前に，初期作業を後続作業の前に提示する構成にする。

エ　文書の情報には，読者層の中で最も経験のない利用者がソフトウェアの機能を使って，選択した作業を遂行できるために必要な最小限の情報を含める。

問24　バリューチェーンでは，付加価値を生み出す事業活動を，五つの主活動と四つの支援活動に分類している。支援活動に該当するものはどれか。

ア　技術開発　　イ　購買物流　　ウ　サービス　　エ　製造

問25　ある顧客層の今後 3 年間を通しての，年間顧客維持率が 40%，顧客 1 人当たりの年平均売上高が 200 万円，売上高コスト比率が 50%と想定される場合，今後 3 年間の LTV（顧客 1 人当たりの生涯価値）は何万円か。ここで，割引率は考慮しないものとする。

ア　62.4　　イ　156　　ウ　210　　エ　312

〔 メ モ 用 紙 〕

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。ただし，問題冊子を切り離して利用することはできません。
8. 試験時間中，机上に置けるものは，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，黒鉛筆及びシャープペンシル（B 又は HB），鉛筆削り，消しゴム，定規，時計（時計型ウェアラブル端末は除く。アラームなど時計以外の機能は使用不可），ハンカチ，ポケットティッシュ，目薬

   これら以外は机上に置けません。使用もできません。
9. 試験終了後，この問題冊子は持ち帰ることができます。
10. 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。
11. 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。
12. 午後Ⅰの試験開始は 12:30 ですので，12:10 までに着席してください。