AU

平成27年度　春期
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，読み取れません。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ご注意ください。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**のとおり記入及び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〕　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 ● 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。

問題文中で共通に使用される表記ルール

各問題文中に注記がない限り，次の表記ルールが適用されているものとする。

試験問題での表記	規格・標準の名称
JIS Q 9001	JIS Q 9001:2008
JIS Q 14001	JIS Q 14001:2004
JIS Q 15001	JIS Q 15001:2006
JIS Q 20000-1	JIS Q 20000-1:2012
JIS Q 20000-2	JIS Q 20000-2:2013
JIS Q 27000	JIS Q 27000:2014
JIS Q 27001	JIS Q 27001:2014
JIS Q 27002	JIS Q 27002:2014
JIS X 0160	JIS X 0160:2012
ISO 21500	ISO 21500:2012
ITIL	ITIL 2011 edition
PMBOK	PMBOK ガイド 第5版
共通フレーム	共通フレーム 2013

問1　システム監査技法であるITF（Integrated Test Facility）法の説明はどれか。

ア　監査機能をもったモジュールを監査対象プログラムに組み込んで実環境下で実行し，抽出条件に合った例外データ，異常データなどを収集し，監査対象プログラムの処理の正確性を検証する方法である。

イ　監査対象ファイルにシステム監査人用の口座を設け，実稼働中にテストデータを入力し，その結果をあらかじめ用意した正しい結果と照合して，監査対象プログラムの処理の正確性を検証する方法である。

ウ　システム監査人が準備した監査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，両者の実行結果を比較することによって，監査対象プログラムの処理の正確性を検証する方法である。

エ　プログラムの検証したい部分を通過したときの状態を出力し，それらのデータを基に監査対象プログラムの処理の正確性を検証する方法である。

問2　インシデントの究明やシステム監査にも利用できる，証拠を収集し保全する技法はどれか。

ア　コンティンジェンシープラン　　イ　サンプリング

ウ　ディジタルフォレンジックス　　エ　ベンチマーキング

問3　システム監査において，ペネトレーションテストが最も適合するチェックポイントはどれか。

ア　オフィスへの入退に，不正防止及び機密保護の物理的な対策が講じられているか。

イ　データ入力が漏れなく，重複なく正確に行われているか。

ウ　ネットワークの負荷状況の推移が記録，分析されているか。

エ　ネットワークへのアクセスコントロールが有効に機能しているか。

問4　テストデータ法をシステム監査手続として使用する上での留意点はどれか。

ア　監査モジュールを適時に組み込み，本番データの正当性を検証すること
イ　テスト対象プログラムのロジックが本番で稼働しているものと同一であるかを確認すること
ウ　テストデータには本番データをそのまま用いること
エ　テストデータの作成に当たっては統計的サンプリング手法を用いること

問5　システム監査報告書に記載された改善勧告への取組みに対する監査人のフォローアップとして，適切なものはどれか。

ア　改善勧告に対する改善の実施を，被監査部門の長に指示する。
イ　改善勧告に対する被監査部門の改善実施状況を確認する。
ウ　改善勧告に対する被監査部門の改善実施プロジェクトの管理を行う。
エ　改善勧告の内容を被監査部門に示し，改善実施計画を策定する。

問6　システムの開発，運用及び保守を担当者が 1 人だけで実施している企業におけるシステム監査に関する記述のうち，最も適切なものはどれか。

ア　開発，運用及び保守の実施状況を熟知している当該担当者に対するヒアリング結果だけを監査証拠にする。
イ　システム改修時の利用部門による動作確認及び責任者による承認の実施状況を確認できる監査手続にする。
ウ　適正な監査手続の実施が不可能であることを当然のこととして，監査意見を形成する。
エ　内部統制による牽制が十分であることを当然のこととして，監査計画を策定する。

問7　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行う。

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順に経て，最終結論を下す。

ウ　本調査の作業は，予備調査結果の確認，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8　システム監査における監査証跡はどれか。

ア　監査業務の全過程において，監査人が収集及び作成した資料である。

イ　監査対象システムの入力から出力に至る過程を追跡できる一連の仕組みと記録である。

ウ　監査人が監査証拠を入手するために実施する監査技術の組合せである。

エ　監査人が監査手続を実施して収集した資料を監査人の判断に基づいて評価した結果である。

問9　個人情報取扱事業者に対する監査において，個人情報の第三者提供の観点から指摘事項に該当するものはどれか。

ア　社員が意識不明に陥り，家族とも連絡がつかないときに，救急隊員に社員本人の個人情報を，本人の同意を得ずに渡した。

イ　税務署の要請によって，従業員の給与振込先口座の情報を，本人の同意を得ずに提出した。

ウ　フランチャイズの本部から加盟店に，顧客の個人情報を，本人の同意を得ずに渡した。

エ　法令で定められた共同利用に関する事項を Web サイトに明示した上で，プレゼントキャンペーンの応募者データを，本人の同意を得ずにグループ会社と共同利用した。

問10　人事給与システムのシステム監査において，勤怠データの入力漏れを発見するコントロールの評価項目として，適切なものはどれか。

ア　人事マスタに未登録の社員の勤怠データは，通常の入力操作では入力できないこと

イ　データ入力を行う担当者に，正規の手続によってアクセス権限が付与されていること

ウ　入力された勤怠時間に対する限界値チェック機能が，システムに組み込まれていること

エ　入力された内容がプルーフリストとして出力され，人事部の管理者が入力原票と照合を行っていること

問11 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　個別計画書には監査対象ごとに重点監査テーマを記載し，システム監査の方針とする。

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12 JIS Q 20000-1 の“サービスマネジメントシステムの監視及びレビュー”の要求事項のうち，適切なものはどれか。

ア　監査員は，自らの仕事を監査してはならない。

イ　監査の基準は，文書化された手順の中に定義してはならない。

ウ　特定された不適合，懸念事項は，該当する利害関係者であっても開示してはならない。

エ　レビューの間隔は，あらかじめ定めてはならない。

問13 IT サービスマネジメントにおける，インシデント及びサービス要求管理の主な活動はどれか。

ア　インシデントの影響を最小限にするための既知の誤り記録の作成

イ　インシデントの解決とサービスの復旧

ウ　インシデントの傾向分析と予防処置

エ　インシデントの未知の根本原因の特定

問14　プログラムの著作物について，著作権法上，適法である行為はどれか。

ア　海賊版を複製したプログラムと事前に知りながら入手し，業務で使用した。
イ　業務処理用に購入したプログラムを複製し，社内教育用として各部門に配布した。
ウ　職務著作のプログラムを，作成した担当者が独断で複製し，他社に貸与した。
エ　処理速度を向上させるために，購入したプログラムを改変した。

問15　電子帳簿保存法の要件に**反しない**事実関係はどれか。

ア　自社内に会計システムをもたない会社が，委託先会計事務所の電子計算機を用いて，取引の最初の記録から一貫して国税関係の帳簿を作成している。
イ　支店などの新設がない場合において，仕訳帳を会計期間の中途から電磁的に記録している。
ウ　電子帳簿保存を行うシステム関係書類（システム概要書，システム仕様書，操作説明書）の備え付けはしていない。
エ　電子帳簿保存を行うシステムで仕訳情報の登録，削除の内容は検索できるが，訂正の内容は検索ができない。

問16　合格となるべきロットが，抜取検査で誤って不合格となる確率のことを何というか。

ア　合格品質水準　　イ　消費者危険
ウ　生産者危険　　エ　有意水準

問17 関係データベースのビューを利用する目的はどれか。

ア DISTINCT 指定，GROUP BY 句及び HAVING 句をもつ演算処理を独立させて，プログラムに単純化したデータ更新手段を提供する。

イ 行や列を特定の条件で絞り込んだビューだけをアクセスさせることによって，基となる表のデータの一部を隠蔽して保護する手段を提供する。

ウ データベースの物理的記憶構造の変更に影響されないように，アプリケーションプログラムに対して物理的データ独立性を提供する。

エ 複数の表を結合したビューにインデックスを付与することによって，複数の表にまたがった高度な検索手段を提供する。

問18 Web ページ内で info@example.co.jp が電子メールアドレスであることを表し，このアドレスへの電子メールの送信に利用される URI はどれか。

ア imap:info@example.co.jp

イ mailto:info@example.co.jp

ウ pop:info@example.co.jp

エ smtp:info@example.co.jp

問19 共通鍵暗号方式において，100 人の送受信者のそれぞれが，相互に暗号化通信を行うときに必要な共通鍵の総数は幾つか。

ア 200　　イ 4,950　　ウ 9,900　　エ 10,000

問20　“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している。

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21　PCI データセキュリティ基準（PCI DSS Version 3.0）のセキュリティ要件から見て，適切なものはどれか。

ア　管理者のアクセスログは取得するが，プライバシを考慮して，一般利用者のアクセスログは取得しない。

イ　従業員によるネットワーク外部からのリモートアクセスを許可する場合，管理者以外の従業員は利用者 ID とその ID のパスワードだけの認証でよい。

ウ　伝送中及び保存中のパスワードは，暗号化して解読不能にする。

エ　利用されない利用者 ID の削除及び無効化は，1 年に 1 回まとめて行う。

問22 安全性と信頼性について，次の方針でプログラム設計を行う場合，その方針を表す用語はどれか。

〔方針〕

不特定多数の人が使用するプログラムには，自分だけが使用するプログラムに比べて，より多くのデータチェックの機能を組み込む。プログラムが処理できるデータの前提条件を文書に書いておくだけでなく，その前提条件を満たしていないデータが実際に入力されたときは，エラーメッセージを表示して再入力を促すようにプログラムを作る。

ア　フールプルーフ　　イ　フェールセーフ

ウ　フェールソフト　　エ　フォールトトレラント

問23 JIS X 25010:2013 で規定されるシステム及びソフトウェア製品の品質特性の定義のうち，“性能効率性”の定義はどれか。

ア　意図した保守者によって，製品又はシステムが修正することができる有効性及び効率性の度合い

イ　明記された状態（条件）で使用する資源の量に関係する性能の度合い

ウ　明示された時間帯で，明示された条件下に，システム，製品又は構成要素が明示された機能を実行する度合い

エ　明示された条件下で使用するとき，明示的ニーズ及び暗黙のニーズを満足させる機能を，製品又はシステムが提供する度合い

問24 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%，1 人当たり年平均売上高が 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

問25 バランススコアカードを説明したものはどれか。

ア 企業のビジョンと戦略を実現するために，財務，顧客，内部ビジネスプロセス，学習と成長という四つの視点から検討するマネジメント手法

イ 経営環境を，強み，弱み，機会，脅威という四つのカテゴリに分類して分析し，企業にとっての事業機会を導き出すマネジメント手法

ウ 製品を，導入期，成長期，成熟期，衰退期という四つの段階に分類し，企業にとっての最適な事業戦略を立案するマネジメント手法

エ ビジネスを，問題児，花形，金のなる木，負け犬という四つのカテゴリに分類し，経営資源配分を決定するためのマネジメント手法

〔 メ モ 用 紙 〕

〔 メ モ 用 紙 〕

〔 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。
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（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。