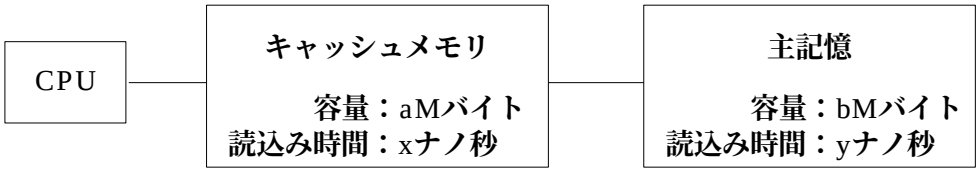
平成１８年度　春期　システム監査技術者　午前問題

問１　図のアーキテクチャのシステムにおいて，CPU からみた，主記憶とキャッシュメモリを合わせた平均読込み時間を表す式はどれか。ここで，読み込みたいデータがキャッシュメモリに存在しない確率を r とし，キャッシュメモリ管理に関するオーバヘッドは無視できるものとする。



ア　$\frac{(1-r)\cdot a}{a+b}\cdot x + \frac{r\cdot b}{a+b}\cdot y$　　イ　$(1-r)\cdot x + r\cdot y$

ウ　$\frac{r\cdot a}{a+b}\cdot x + \frac{(1-r)\cdot b}{a+b}\cdot y$　　エ　$r\cdot x + (1-r)\cdot y$

問２　二つのタスクが共用する二つの資源を排他的に使用するとき，デッドロックが発生する可能性がある。このデッドロックの発生を防ぐ方法はどれか。

ア　一方のタスクの優先度を高くする。

イ　資源獲得の順序を両方のタスクで同じにする。

ウ　資源獲得の順序を両方のタスクで逆にする。

エ　両方のタスクの優先度を同じにする。

問３　自動支払機が 1 台ずつ設置してあった二つの支店を統合し，統合後の支店には自動支払機を 1 台設置する。統合後の自動支払機の平均待ち時間を求める式はどれか。ここで，待ち時間は M/M/1 の待ち行列モデルに従い，平均待ち時間にはサービス時間を含まないものとする。

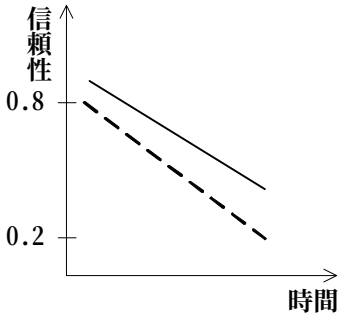
〔条件〕
(1)　平均サービス時間：Ts
(2)　統合前のシステムの利用率：両支店とも ρ
(3)　統合後の利用者数は，統合前の 2 支店の利用者数の合計値

ア　$\frac{\rho}{1-\rho} \times Ts$　　イ　$\frac{\rho}{1-2\rho} \times Ts$

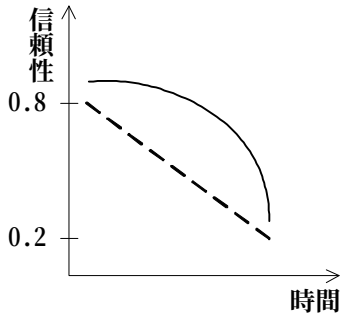
ウ　$\frac{2\rho}{1-\rho} \times Ts$　　エ　$\frac{2\rho}{1-2\rho} \times Ts$

問４　3 個の構成要素のうち 2 個以上が正常ならば正しい結果が得られるようなシステムにおいて，個々の構成要素の信頼性が時間の経過とともに破線のグラフで示すように低下する場合，システム全体の信頼性の変化の傾向を表す実線のグラフとして適切なものはどれか。

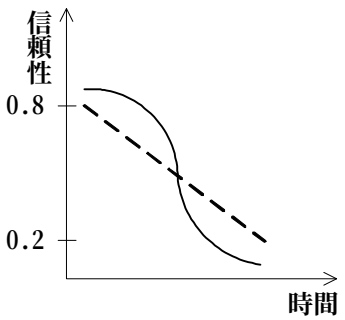
ア



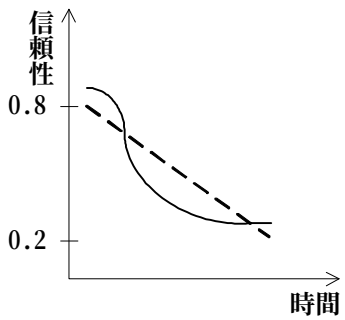
イ



ウ



エ



問５　“缶ビールを購入する顧客は，スナック菓子を同時に買い求める傾向にある”というようなデータベースに蓄積された大量のデータを分析して，新たな情報を得る技術はどれか。

ア　データウェアハウス　　イ　データエンティティ

ウ　データマート　　エ　データマイニング

問６　UML を DFD 又は E-R 図と対比した記述のうち，適切なものはどれか。

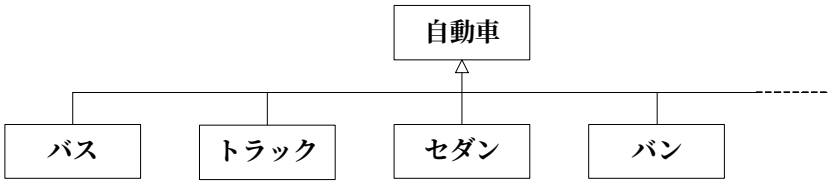
ア　UML ではデータの関係を記述できないので，E-R 図を併用する必要がある。

イ　UML ではデータの流れを記述できないので，DFD を併用する必要がある。

ウ　UML におけるコラボレーション図（協調図）やコンポーネント図が DFD に相当する。

エ　UML における静的な構造を示すクラス図が，E-R 図に相当する。

問７　オブジェクト指向において図のような階層のクラスを構成する場合，クラス間の関係の説明として，適切なものはどれか。



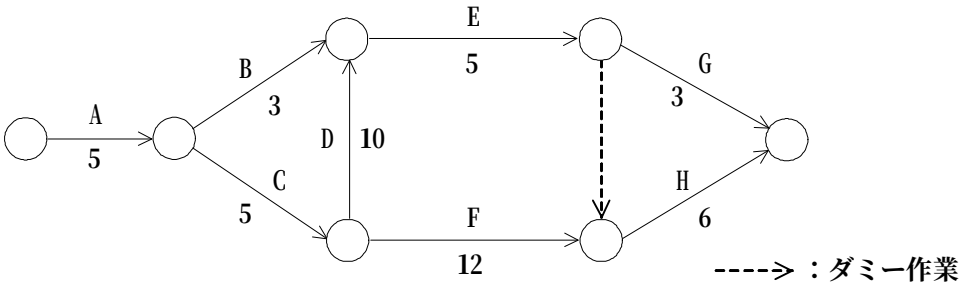
ア　“バス”,“トラック”などのクラスが“自動車”の定義を引き継ぐことを，インスタンスという。

イ　“バス”,“トラック”などのクラスの共通部分を抽出して,“自動車”のクラスとして定義することを，汎化という。

ウ　“バス”,“トラック”などのクラスは,“自動車”のクラスに対して，オブジェクトという。

エ　“バス”,“トラック”などのそれぞれのクラスの違いを“自動車”のクラスとして定義することを，特化という。

問８　次のアローダイアグラムで表される作業A～Hを見直したところ,作業Dだけが短縮可能であり,その所要日数を 6 日間にできることが分かった。業務全体の所要日数は何日間短縮できるか。ここで，矢印に示す数字は各作業の所要日数を表す。



ア　1　　イ　2　　ウ　3　　エ　4

問９　運用しやすいシステム作りや，本稼働へのスムーズな移行のために，運用部門が果たすべき役割として，適切なものはどれか。

ア　システム開発部門が作成したジョブ構成を変更せずに管理する。

イ　システム開発部門が作成した本稼働への移行手順を利用部門に周知徹底する。

ウ　システム開発部門の開発スケジュールを優先して本稼働までの日程計画を立てる。

エ　システムの設計段階からプロジェクトに参加して運用ドキュメントの標準化を進める。

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　公開鍵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，NIST が公募し，1997 年に決定した公開鍵暗号方式の一種である。

イ　RSA は，素因数分解の計算の困難さを利用した，公開鍵暗号方式の一種である。

ウ　公開鍵暗号方式の難点は，鍵の管理が煩雑になることである。

エ　通信文の内容の秘匿に公開鍵暗号方式を使用する場合は，受信者の復号鍵を公開する。

問 12　ディジタル署名を利用する目的はどれか。

ア　受信者が署名用の鍵を使って暗号文を元の平文に戻すことができるようにする。

イ　送信者が署名用の鍵を使って作成した署名を平文に付加することによって，受信者が送信者を確認できるようにする。

ウ　送信者が署名用の鍵を使って平文を暗号化し，平文の内容を関係者以外に分からないようにする。

エ　送信者が定数を付加した平文を署名用の鍵を使って暗号化し，受信者が復号した定数を確認することによって，メッセージの改ざん部位を特定できるようにする。

問 13　JPCERT/CC（JPCERT コーディネーションセンター）では，インシデントを六つのタイプに分類している。

Scan　　：プローブ，スキャン，そのほかの不審なアクセス
Abuse　：サーバプログラムの機能を悪用した不正中継
Forged　：送信ヘッダを詐称した電子メールの配送
Intrusion：システムへの侵入
DoS　　：サービス運用妨害につながる攻撃
Other：その他

次の三つのインシデントに対するタイプの組合せのうち，適切なものはどれか。
インシデント 1：ワームの攻撃が試みられた形跡があるが，侵入されていない。
インシデント 2：ネットワークの輻輳による妨害を受けた。
インシデント 3：DoS 用の踏み台プログラムがシステムに設置されていた。

	インシデント 1	インシデント 2	インシデント 3
ア	Abuse	DoS	Intrusion
イ	Abuse	Forged	DoS
ウ	Scan	DoS	Intrusion
エ	Scan	Forged	DoS

問 14　不正利用を防止するための，メールサーバの設定はどれか。

ア　ゾーン転送のアクセス元を制御する。
イ　第三者中継を禁止する。
ウ　ディレクトリに存在するファイル名の表示を禁止する。
エ　特定のディレクトリ以外での CGI プログラムの実行を禁止する。

問 15　認証局（CA）に登録されている通信相手の公開鍵を使用して行えることはどれか。

ア　CA から証明書の発行を受ける。
イ　受信した暗号文を復号する。
ウ　ディジタル署名を検証する。
エ　メッセージにディジタル署名をする。

問 16　IDS（Intrusion Detection System）の特徴のうち，適切なものはどれか。

ア　ネットワーク型 IDS では，SSL を利用したアプリケーションを介して行われる攻撃を検知できる。

イ　ネットワーク型 IDS では，通信内容の解析によって，ファイルの改ざんを検知できる。

ウ　ホスト型 IDS では，シグネチャとのパターンマッチングを失敗させるためのパケットが挿入された攻撃でも検知できる。

エ　ホスト型 IDS では，到着する不正パケットの解析によって，ネットワークセグメント上の不正パケットを検知できる。

問 17　クロスサイトスクリプティングに該当するものはどれか。

ア　悪意をもったスクリプトを，標的となるサイト経由でユーザのブラウザに送り込み，その標的にアクセスしたユーザのクッキーにある個人情報を盗み取る。

イ　クラッカの Web サイトにアクセスしたユーザに悪意をもったスクリプトを送り込み，そのスクリプトを実行させて Web ページ中の HTML タグを変換する。

ウ　攻撃者が，JavaScript を使ったセッション管理に使うクッキーにアクセスし，ブラウザに広告などのダミー画面を表示する。

エ　入力情報を確認するためにフォームの入力値を画面表示するプログラムの脆弱性を利用して，クッキーにある個人情報を改ざんする。

問 18　ステガノグラフィの機能はどれか。

ア　画像データなどにメッセージを埋め込み，メッセージの存在そのものを隠す。

イ　メッセージの改ざん，なりすましの検出，及び否認防止を行う。

ウ　メッセージの認証を行って改ざんの有無を検出する。

エ　メッセージを決まった手順で変換し，通信途中での盗聴を防ぐ。

問 19　送信者がメッセージからブロック暗号（方式）を用いて生成したメッセージ認証符号（MAC：message authentication code）をメッセージとともに送り，受信者が受け取ったメッセージからMACを生成して，送られてきたMACと一致することを確認するメッセージ認証で使用される鍵の組合せはどれか。

	送信者	受信者
ア	受信者と共有している共通鍵	送信者と共有している共通鍵
イ	受信者の公開鍵	受信者の秘密鍵
ウ	送信者の公開鍵	受信者の秘密鍵
エ	送信者の秘密鍵	受信者の公開鍵

問 20　SSLの利用に関する記述のうち，適切なものはどれか。

ア　SSLで使用する個人認証用のディジタル証明書は，ICカードなどに格納できるので，格納場所を特定のPCに限定する必要はない。

イ　SSLは特定利用者間の通信のために開発されたプロトコルであり，事前の利用者登録が不可欠である。

ウ　ディジタル証明書にはIPアドレスが組み込まれているので，SSLを利用するWebサーバのIPアドレスを変更する場合は，ディジタル証明書を再度取得する必要がある。

エ　日本国内では，SSLで使用する共通鍵の長さは，128ビット未満に制限されている。

問 21　情報セキュリティ基本方針文書の取扱いについて，ISMS認証基準に定められているものはどれか。

ア　一度決めた内容は変更せず，セキュリティ事故発生時に見直す。

イ　機密情報であるので関連する管理者にだけ内容を教育する。

ウ　経営陣によって承認され，全従業員に公表し通知する。

エ　作成したメンバ自身で実施状況を点検する。

問 22　コンピュータフォレンジクスを説明したものはどれか。

ア　画像や音楽などのディジタルコンテンツに著作権者などの情報を埋め込む。

イ　コンピュータやネットワークのセキュリティ上の弱点を発見するテスト手法の一つであり，システムを実際に攻撃して侵入を試みる。

ウ　証拠となりうるデータを保全し，その後の訴訟などに備える。

エ　ネットワークの管理者や利用者などから，巧みな話術や盗み聞き，盗み見などの手段によって，パスワードなどのセキュリティ上重要な情報を入手する。

問 23　JIS Q 9001（ISO 9001）に規定されているものはどれか。

ア　外部から購入したソフトウェア製品を最終製品に組み込む場合は，動作検査を実施した後に行う。

イ　設計の妥当性確認は，ソフトウェア開発者自身が行うテスト及びデバッグによって実現される設計検証の一つとして実施する。

ウ　トレーサビリティが要求される製品は，製造番号などによって固有の識別を管理し記録する。

エ　納入製品に組み込むために提供された顧客の所有物には，顧客の知的所有権は含まれない。

問 24　国際標準化の動向に関する記述のうち，適切なものはどれか。

ア　“情報技術－情報セキュリティマネジメントの実践のための規範”を規定している ISO/IEC 17799 は，JIS X 5080 の基になっている。

イ　“品質及び／又は環境マネジメントシステム監査のための指針”を規定している ISO 19011 は，システム監査基準の基になっている。

ウ　“品質システム－設計・開発・製造における品質保証モデル”を規定している ISO 9001 は，共通フレーム 98（SLCP-JCF98）の基になっている。

エ　“プロジェクトマネジメントにおける品質の指針”を規定している ISO 10006 は，PMBOK の基になっている。

問 25　コンピュータで使われている文字符号の説明のうち，適切なものはどれか。

ア　ASCII 符号はアルファベット，数字，特殊文字及び制御文字からなり，漢字に関する規定はない。

イ　EUC は文字符号の世界標準を作成しようとして考案された 16 ビット以上の符号体系であり，漢字に関する規定はない。

ウ　Unicode は文字の 1 バイト目で漢字かどうかが分かるようにする目的で制定され，漢字と ASCII 符号を混在可能にした符号体系である。

エ　シフト JIS 符号は UNIX における多言語対応の一環として制定され，ISO として標準化されている。

問 26　バランストスコアカードにおける業績評価指標のうち，“学習と成長の視点”に分類されるものはどれか。

ア　顧客満足度調査の結果　　イ　従業員 1 人当たりの売上高

ウ　従業員の提案件数　　エ　新製品導入率

問 27　経営戦略の立案で用いられる分析技法の説明のうち，適切なものはどれか。

ア　SWOT 分析は，経営戦略を立てるために，自社の強みと弱み，機会と脅威を分析する手法である。

イ　事業成功要因分析は，企業の財務諸表を基に，収益性及び安全性を分析する手法である。

ウ　市場分析は，自社製品・サービスの市場での位置付けや評価を明らかにする手法であり，苦情分析，故障分析，売上分析などがある。

エ　プロダクトミックス分析は，自社製品の価格設定のために，市場での競争力を分析する手法である。

問 28　マトリックス組織を説明したものはどれか。

ア　事業部制組織と職能制組織との両方の特徴を生かそうとする組織である。

イ　新事業開発のために社内に独立した活動単位として設置し，小さな企業であるかのように運営する組織である。

ウ　製品群などを事業単位として構成し，事業単位ごとに意思決定を行う組織である。

エ　専門化を志向した組織であり，研究開発，製造，販売，人事・総務，経理・財務のような職能別に構成された組織である。

問 29　情報システムの全体計画立案のために E-R モデルを採用して全社のデータモデルを作成する場合，適切な手順はどれか。

ア　管理層の業務から機能を抽出し，機能をエンティティとする。次に，機能の相互関係に基づいてリレーションを定義する。さらに，全社の帳票類を調査整理し，正規化された項目に基づいて属性を定義し，全社のデータモデルとする。

イ　企業の全体像を把握するため，基本的なエンティティだけを抽出し，それらの相互間のリレーションを含めて，鳥瞰図を作成する。次に，エンティティを詳細化し，すべてのリレーションを明確にしたものを全社のデータモデルとする。

ウ　業務層の現状システムを分析し，エンティティとリレーションを抽出する。それぞれについて適切な属性を定め，これらを基に E-R 図を作成し，それを抽象化して，全社のデータモデルを作成する。

エ　全社のデータとその処理過程を分析し，重要な処理を行っている業務を基本エンティティとする。次に，基本エンティティ相互のデータの流れをリレーションとしてとらえ，適切な識別名を与える。さらに，基本エンティティと関係あるデータを属性とし，全社のデータモデルを作成する。

問 30　市場販売目的のソフトウェア開発の際に，研究開発費として費用処理するものはどれか。

ア　外部から購入したソフトウェアに著しい改良を加え，販売用のソフトウェア製品とするときに要した開発費用

イ　研究開発費で開発されたソフトウェア製品に，引き続き軽微な機能を追加したときの費用

ウ　既に販売中のソフトウェア製品に不具合が発見されたとき，その修正にかかわる設計変更及び開発に要した費用

エ　ソフトウェア製品を販売する際に，顧客特有の機能の追加開発やカスタマイズに要した費用

問 31　キャッシュフロー計算書において，営業活動によるキャッシュフローに表示されるものはどれか。ここで，キャッシュフロー計算書は，間接法を採用しているものとする。

ア　棚卸資産減少額　　イ　短期借入金返済

ウ　配当金支払額　　エ　有形固定資産売却収入

問 32　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　KJ 法　　イ　クロスセクション法
ウ　シナリオライティング法　　エ　デルファイ法

問 33　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 34　ある会社の生産計画部では，毎月 25 日に次の手続で翌月の計画生産量を決定している。8 月分の計画生産量を求める式はどれか。

〔手続〕
(1) 当月末の予想在庫量を，前月末の実在庫量と当月の計画生産量と予想販売量から求める。
(2) 当月末の予想在庫量と，翌月分の予想販売量から，翌月末の予想在庫量が翌々月から 3 か月間の予想販売量と等しくなるように翌月の計画生産量を決定する。

I6	6 月末実在庫量				
I7	7 月末予想在庫量	P7	7 月分計画生産量	S7	7 月分予想販売量
I8	8 月末予想在庫量	P8	8 月分計画生産量	S8	8 月分予想販売量
				S9	9 月分予想販売量
				S10	10 月分予想販売量
				S11	11 月分予想販売量

In：n 月の月末在庫量　　Pn：n 月の生産量　　Sn：n 月の販売量

ア　I6＋P7－S7＋S8　　イ　S8＋S9＋S10＋S11－I7
ウ　S8＋S9＋S10＋S11－I8　　エ　S9＋S10＋S11－I7

問 35　ディジタルディバイドを説明したものはどれか。

ア　PC や IT を利用する能力や機会の違いによって，経済的，又は社会的な格差が生じること

イ　インターネットなどを活用することによって，住民が直接，政府や自治体の政策に参画できること

ウ　国民のだれもが，地域の格差なく，妥当な料金で平等に利用できる通信及び放送サービスのこと

エ　市民生活のイベント又は企業活動の分野ごとに，すべてのサービスを 1 か所で提供すること

問 36　法人が作成し，公開，発売したソフトウェアの著作権の権利期間は公開から何年か。

ア　15　　イ　20　　ウ　30　　エ　50

問 37　著作者人格権に関する記述のうち，適切なものはどれか。

ア　著作権は著作時点で発生するが，著作者人格権は実名登録時点で発生する。

イ　著作者人格権は著作者に専属し，他者には譲渡できないものである。

ウ　著作物を公表する権利及び複製する権利は，著作者人格権に含まれる。

エ　翻訳権を与えた場合，著作者人格権の同一性保持権も譲渡することになる。

問 38　下請代金支払遅延等防止法において，下請業者から受領したプログラムの返品を禁止しているのは，どの場合か。

ア　委託内容の一部を受領したが，下請業者の要員不足が原因で開発が遅れている旨の説明を受けた。

イ　親事業者と顧客との間の委託内容が変更になり，既に受領していたプログラムが不要になった。

ウ　開発途上で発生した仕様変更の内容，対価などを下請業者と合意していたが，受領したプログラムには仕様変更が反映されていなかった。

エ　ほとんど発生しないバグが，受領時の通常のテストでは発見できず，受領後 5 か月経過した時点で発見された。

問 39　不正競争防止法で保護されるものはどれか。

ア　特許権を取得した発明

イ　頒布されている独自のシステム開発手順書

ウ　秘密として管理している事業活動用の非公開の顧客名簿

エ　秘密としての管理を行っていない，自社システムを開発するために重要な設計書

問 40　製造物責任法（PL 法）に関する記述のうち，適切なものはどれか。

ア　製造物の欠陥の原因となった製造過程における過失を被害者が証明できなければ，製造者に責任を負わせることはできない。

イ　製造物の単なる輸入業者は，責任の主体とはならない。

ウ　製造物を引き渡した時点から 5 年を過ぎて事故が発生した場合，製造者に責任を負わせることはできない。

エ　製造物を引き渡した時点の科学又は技術では欠陥を認識できなかった場合，その欠陥によって被害が発生しても，製造者に責任を負わせることはできない。

問 41　“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 42　“システム監査基準”の報告基準で定めている事項はどれか。

ア　監査報告書の管理体制　　イ　監査報告書の提出期限

ウ　監査報告書の保存期間　　エ　監査報告に基づく改善指導

問 43　システム監査で利用する統計的サンプリング法に関する記述のうち，適切なものはどれか。

ア　サンプルの抽出に無作為抽出法を用い，サンプルの監査結果に基づく母集団に関する結論を出すに当たって，確率論の考え方を用いる。

イ　抽出されるサンプル数は，統計的サンプリングと非統計的サンプリングの選択を決定付ける重要な判断基準である。

ウ　抽出するサンプルを統計的に決定する手法ではなく，サンプルに対して監査手続を実施した結果を統計的に評価する方法である。

エ　無作為抽出法を用いるだけではなく，システム監査人が経験的判断を加味して，サンプルを抽出する。

問 44　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シミュレートし，本番データと異なるデータを使って処理手続や処理論理をテストする方法

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枠組みの中で，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組み込んで実データを処理する方法

問 45　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など，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，問題に対する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 46　監査証拠の評価のうち，適切なものはどれか。

ア　被監査部門以外の第三者から入手した文書は，被監査部門から入手した同種の文書よりも監査証拠としての証明力が強い。

イ　被監査部門から入手した内部証拠は，そのコントロールが適切でない場合でも，監査証拠としての証明力が強い。

ウ　被監査部門に作成させた出力帳票は，システム監査人の立会いの下で被監査部門の担当者に端末を操作させて入手したデータよりも，監査証拠としての証明力が強い。

エ　被監査部門に対するヒアリングの内容は，被監査部門から入手した複数文書の突き合わせ結果よりも監査証拠としての証明力が強い。

問 47　システム監査の特質はどれか。

ア　システム監査が内部監査として行われる場合であっても，監査人は経営者から独立していなければならない。

イ　システム監査は，監査対象から独立した立場で行う情報システムの監査であり，システムの企画・開発・運用・保守に責任を負う。

ウ　システム監査は，業務監査の一環として行ってはならない。

エ　システム監査は，原則として，情報システムが“システム管理基準”に準拠しているかどうかを確かめる。

問 48　システム開発の基本設計工程におけるデザインレビューについてシステム監査を行った結果，指摘事項となる状況はどれか。

ア　レビュー対象の基本設計書を，レビュー参加者に事前配付している。

イ　レビューの結果をレビュー結果記録表に記録し，保管している。

ウ　レビューの参加者を，基本設計担当者，詳細設計担当者，及び開発チームリーダの 3 者としている。

エ　レビューは，設計担当者が説明してレビューメンバが質問するウォークスルー方式で行っている。

問 49　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　データの更新時にユーザ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。

イ　データベースの障害回復手段が組み込まれているかどうか。

ウ　データベースの利用効率が適切であるかどうか。

エ　データ領域の使用中領域と拡張用領域のバランスが適切であるかどうか。

問 50　“ISMS 認証基準”の詳細管理策を基に設定した，ノート型 PC に対する物理的安全対策の妥当性を確認するための監査手続はどれか。

ア　オフィス内を視察し，不在者のノート型 PC が施錠されたキャビネットに保管されていることを確認する。

イ　教育計画及び教育記録を閲覧し，ノート型 PC の安全管理についての社員教育が適切に行われていることを確認する。

ウ　実際にノート型 PC を操作して，パスワードを入力しないと起動できない仕組みになっていることを確認する。

エ　ノート型 PC の管理ルールを調べ，社外に持ち出す場合には申請書を提示し，セキュリティ管理者の許可を得るルールになっていることを確認する。

問 51　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 52　システム監査と情報セキュリティ監査における監査対象を説明したものはどれか。

ア　システム監査では情報システムにかかわらない文書情報を対象に含めないが，情報セキュリティ監査では含める。

イ　システム監査と情報セキュリティ監査は，ともにすべての情報資産を対象とする。

ウ　情報セキュリティ監査では情報システムにかかわる人を対象に含めないが，システム監査では含める。

エ　情報セキュリティ監査は情報システムを対象としないが，システム監査は対象とする。

問 53　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。

監査リスク ＝ 固有リスク×統制リスク×発見リスク

ア　外部証拠の入手範囲の拡大　　イ　各種規程類の確認範囲の拡大

ウ　監査期間の短縮　　エ　試査範囲の縮小

問 54　情報セキュリティ監査基準の位置付けはどれか。

ア　監査人が監査上の判断の尺度として用いるべき基準である。

イ　情報資産を保護するためのベストプラクティスをまとめたものである。

ウ　情報セキュリティ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　組織体が効果的な情報セキュリティマネジメント体制を構築し，適切なコントロールを整備，運用するための実践規範である。

問 55　JIS Q 9001（ISO 9001）の内部監査とシステム監査の関係はどれか。

ア　ISO 9001 の内部監査は，ソフトウェア製品の供給者が利用者に対して製品の品質を保証するために行うもので，システム監査よりも対象範囲が広い。

イ　ソフトウェア製品の開発プロジェクトを対象とするシステム監査が，ISO 9001 の内部監査に相当する。

ウ　ソフトウェア製品の利用者に対して監査報告を行うという点で，システム監査と ISO 9001 の内部監査は共通している。

エ　ソフトウェアの品質確保の観点から行うシステム監査は，ISO 9001 の内部監査に相当する場合がある。