SG

平成30年度　秋期
情報セキュリティマネジメント試験
午前　問題

試験時間	9:30 ～ 11:00（1時間30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. **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50
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〕　秋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　組織的なインシデント対応体制の構築や運用を支援する目的でJPCERT/CCが作成したものはどれか。

ア　CSIRTマテリアル
イ　ISMSユーザーズガイド
ウ　証拠保全ガイドライン
エ　組織における内部不正防止ガイドライン

問２　JIS Q 27000:2014（情報セキュリティマネジメントシステム－用語）における，トップマネジメントに関する記述として，適切なものはどれか。

ア　ISMS適用範囲から独立した立場であることが求められる。
イ　企業の場合，ISMS適用範囲にかかわらず代表取締役でなければならない。
ウ　情報システム部門の長でなければならない。
エ　組織を指揮し，管理する人々の集まりとして複数名で構成されていてもよい。

問３　JIS Q 27017:2016（JIS Q 27002に基づくクラウドサービスのための情報セキュリティ管理策の実践の規範）が提供する“管理策及び実施の手引”の適用に関する記述のうち，適切なものはどれか。

ア　外部のクラウドサービスを利用し，かつ，別のクラウドサービスを他社に提供する事業者だけに適用できる。
イ　外部のクラウドサービスを利用する事業者と，クラウドサービスを他社に提供する事業者とのどちらにも適用できる。
ウ　外部のクラウドサービスを利用するだけであり，自らはクラウドサービスを他社に提供しない事業者には適用できない。
エ　外部のクラウドサービスを利用せず，自らクラウドサービスを他社に提供するだけの事業者には適用できない。

問4　安全・安心な IT 社会を実現するために創設された制度であり，IPA“中小企業の情報セキュリティ対策ガイドライン”に沿った情報セキュリティ対策に取り組むことを中小企業が自己宣言するものはどれか。

ア　ISMS 適合性評価制度
イ　IT セキュリティ評価及び認証制度
ウ　MyJVN
エ　SECURITY ACTION

問5　SaaS（Software as a Service）を利用するときの企業の情報セキュリティ管理に関する記述のうち，適切なものはどれか。

ア　システム運用を行わずに済み，障害時の業務手順やバックアップについての検討が不要である。
イ　システムのアクセス管理を行わずに済み，パスワードの初期化の手続や複雑性の要件を満たすパスワードポリシの検討が不要である。
ウ　システムの構築を行わずに済み，アプリケーションソフトウェア開発に必要な情報セキュリティ要件の定義やシステムログの保存容量の設計が不要である。
エ　システムの情報セキュリティ管理を行わずに済み，情報セキュリティ管理規程の策定や管理担当者の設置が不要である。

問6　JIS Q 27001:2014（情報セキュリティマネジメントシステム－要求事項）では，組織が情報セキュリティリスク対応のために適用する管理策などを記した適用宣言書の作成が要求されている。適用宣言書の作成に関する記述のうち，適切なものはどれか。

ア　承認された情報セキュリティリスク対応計画を基に，適用宣言書を作成する。
イ　情報セキュリティリスク対応に必要な管理策を JIS Q 27001:2014 附属書 A と比較した結果を基に，適用宣言書を作成する。
ウ　適用宣言書を作成後，その内容を基に情報セキュリティリスク対応の選択肢を選定する。
エ　適用宣言書を作成後，その内容を基に情報セキュリティリスクを特定する。

問7　JIS Q 27000:2014（情報セキュリティマネジメントシステム－用語）におけるリスク分析の定義はどれか。

ア　適切な管理策を採用し，リスクを修正するプロセス
イ　リスクが受容可能か又は許容可能かを決定するために，リスク及びその大きさをリスク基準と比較するプロセス
ウ　リスクの特質を理解し，リスクレベルを決定するプロセス
エ　リスクを発見，認識及び記述するプロセス

問８　JIS Q 27014:2015（情報セキュリティガバナンス）における，情報セキュリティガバナンスの範囲と IT ガバナンスの範囲に関する記述のうち，適切なものはどれか。

ア　情報セキュリティガバナンスの範囲と IT ガバナンスの範囲は重複する場合がある。

イ　情報セキュリティガバナンスの範囲と IT ガバナンスの範囲は重複せず，それぞれが独立している。

ウ　情報セキュリティガバナンスの範囲は IT ガバナンスの範囲に包含されている。

エ　情報セキュリティガバナンスの範囲は IT ガバナンスの範囲を包含している。

問９　IPA“中小企業の情報セキュリティ対策ガイドライン（第 2.1 版）”に記載されている，基本方針，対策基準，実施手順から成る組織の情報セキュリティポリシに関する記述のうち，適切なものはどれか。

ア　基本方針と対策基準は適用範囲を経営者とし，実施手順は適用範囲を経営者を除く従業員として策定してもよい。

イ　組織の規模が小さい場合は，対策基準と実施手順を併せて 1 階層とし，基本方針を含めて 2 階層の文書構造として策定してもよい。

ウ　組織の取り扱う情報資産としてシステムソフトウェアが複数存在する場合は，その違いに応じて，複数の基本方針，対策基準及び実施手順を策定する。

エ　初めに具体的な実施手順を策定し，次に実施手順の共通原則を対策基準としてまとめて，最後に，対策基準の運用に必要となる基本方針を策定する。

問10　情報セキュリティ管理を推進する取組みａ～ｄのうち，IPA“中小企業の情報セキュリティ対策ガイドライン（第 2.1 版）”において，経営者がリーダシップを発揮し自ら行うべき取組みとして示されているものだけを全て挙げた組合せはどれか。

〔情報セキュリティ管理を推進する取組み〕

a　情報セキュリティ監査の目的を有効かつ効率的に達成するために，監査計画を立案する。

b　情報セキュリティ対策の有効性を維持するために，対策を定期又は随時に見直す。

c　情報セキュリティ対策を組織的に実施する意思を明確に示すために，方針を定める。

d　情報セキュリティの新たな脅威に備えるために，最新動向を収集する。

ア　a，b，c　　イ　a，b，d　　ウ　a，c，d　　エ　b，c，d

問11　情報の取扱基準の中で，社外秘情報の持出しを禁じ，周知した上で，従業員に情報を不正に持ち出された場合に，“社外秘情報とは知らなかった”という言い訳をさせないことが目的の一つになっている対策はどれか。

ア　権限がない従業員が文書にアクセスできないようにするペーパレス化

イ　従業員との信頼関係の維持を目的にした職場環境の整備

ウ　従業員に対する電子メールの外部送信データ量の制限

エ　情報の管理レベルについてのラベル付け

問12　軽微な不正や犯罪を放置することによって，より大きな不正や犯罪が誘発されるという理論はどれか。

ア　環境設計による犯罪予防理論
イ　日常活動理論
ウ　不正のトライアングル理論
エ　割れ窓理論

問13　ゼロデイ攻撃の特徴はどれか。

ア　脆弱性に対してセキュリティパッチが提供される前に当該脆弱性を悪用して攻撃する。
イ　特定のWebサイトに対し，日時を決めて，複数台のPCから同時に攻撃する。
ウ　特定のターゲットに対し，フィッシングメールを送信して不正サイトに誘導する。
エ　不正中継が可能なメールサーバを見つけて，それを踏み台にチェーンメールを大量に送信する。

問14　ボットネットにおけるC&Cサーバの役割として，適切なものはどれか。

ア　Webサイトのコンテンツをキャッシュし，本来のサーバに代わってコンテンツを利用者に配信することによって，ネットワークやサーバの負荷を軽減する。

イ　外部からインターネットを経由して社内ネットワークにアクセスする際に，CHAPなどのプロトコルを用いることによって，利用者認証時のパスワードの盗聴を防止する。

ウ　外部からインターネットを経由して社内ネットワークにアクセスする際に，チャレンジレスポンス方式を採用したワンタイムパスワードを用いることによって，利用者認証時のパスワードの盗聴を防止する。

エ　侵入して乗っ取ったコンピュータに対して，他のコンピュータへの攻撃などの不正な操作をするよう，外部から命令を出したり応答を受け取ったりする。

問15　マルウェアWanna Cryptor（WannaCry）に関する記述として，適切なものはどれか。

ア　SMBv1の脆弱(ぜい)性を悪用するなどして感染し，PC内のデータを暗号化してデータの復号のための金銭を要求したり，他のPCに感染を拡大したりする。

イ　ファイル共有など複数の感染経路を使って大量のPCに感染を拡大し，さらにPC内の電子メールアドレスを収集しながらインターネット経由で感染を拡大する。

ウ　ランダムにIPアドレスを選んでデータベースの脆弱性を悪用した攻撃を行うことによって多数のPCに感染を拡大し，ネットワークトラフィックを増大させる。

エ　利用者が電子メールに添付されたVBScriptファイルを実行すると感染し，PC内のパスワードを攻撃者のWebサイトへ送信したり，マルウェア付きの電子メールを他者へばらまいたりする。

問16　業務への利用には，会社の情報システム部門の許可が本来は必要であるのに，その許可を得ずに勝手に利用されるデバイスやクラウドサービス，ソフトウェアを指す用語はどれか。

ア　シャドーIT　　イ　ソーシャルエンジニアリング
ウ　ダークネット　　エ　バックドア

問17　セキュアブートの説明はどれか。

ア　BIOS にパスワードを設定し，PC 起動時に BIOS のパスワード入力を要求することによって，OS の不正な起動を防ぐ技術
イ　HDD にパスワードを設定し，PC 起動時に HDD のパスワード入力を要求することによって，OS の不正な起動を防ぐ技術
ウ　PC の起動時に OS やドライバのディジタル署名を検証し，許可されていないものを実行しないようにすることによって，OS 起動前のマルウェアの実行を防ぐ技術
エ　マルウェア対策ソフトをスタートアッププログラムに登録し，OS 起動時に自動的にマルウェアスキャンを行うことによって，マルウェアの被害を防ぐ技術

問18　インターネットと社内サーバの間にファイアウォールが設置されている環境で，時刻同期の通信プロトコルを用いて社内サーバの時刻をインターネット上の時刻サーバの正確な時刻に同期させる。このとき，ファイアウォールで許可すべき時刻サーバとの間の通信プロトコルはどれか。

ア　FTP（TCP，ポート番号 21）
イ　NTP（UDP，ポート番号 123）
ウ　SMTP（TCP，ポート番号 25）
エ　SNMP（TCP 及び UDP，ポート番号 161 及び 162）

問19　利用者 PC がボットに感染しているかどうかを hosts ファイルの改ざんの有無で確認するとき，hosts ファイルが改ざんされていないと判断できる設定内容はどれか。ここで，hosts ファイルの設定内容は 1 行だけであり，利用者及びシステム管理者は，これまでに hosts ファイルを変更していないものとする。

	設定内容	説明
ア	127.0.0.1　a.b.com	a.b.com は利用者 PC の OS 提供元の FQDN を示す。
イ	127.0.0.1　c.d.com	c.d.com は利用者 PC の製造元の FQDN を示す。
ウ	127.0.0.1　e.f.com	e.f.com はウイルス定義ファイルの提供元の FQDN を示す。
エ	127.0.0.1　localhost	localhost は利用者 PC 自体を示す。

問20　公衆無線 LAN のアクセスポイントを設置するときのセキュリティ対策と効果の組みのうち，適切なものはどれか。

	セキュリティ対策	効果
ア	MAC アドレスフィルタリングを設定する。	正規の端末の MAC アドレスに偽装した攻撃者の端末からの接続を遮断し，利用者のなりすましを防止する。
イ	SSID を暗号化する。	SSID を秘匿して，SSID の盗聴を防止する。
ウ	自社がレジストラに登録したドメインを，アクセスポイントの SSID に設定する。	正規のアクセスポイントと同一の SSID を設定した，悪意のあるアクセスポイントの設置を防止する。
エ	同一のアクセスポイントに無線で接続している端末同士の通信を，アクセスポイントで遮断する。	同一のアクセスポイントに無線で接続している他の端末に，公衆無線 LAN の利用者がアクセスポイントを経由して無断でアクセスすることを防止する。

問21　APT の説明はどれか。

ア　攻撃者が DoS 攻撃及び DDoS 攻撃を繰り返し，長期間にわたり特定組織の業務を妨害すること

イ　攻撃者が興味本位で場当たり的に，公開されている攻撃ツールや脆弱性検査ツールを悪用した攻撃を繰り返すこと

ウ　攻撃者が特定の目的をもち，標的となる組織の防御策に応じて複数の攻撃方法を組み合わせ，気付かれないよう執拗に攻撃を繰り返すこと

エ　攻撃者が不特定多数への感染を目的として，複数の攻撃方法を組み合わせたマルウェアを継続的にばらまくこと

問22　A 社の Web サーバは，サーバ証明書を使って TLS 通信を行っている。PC から A 社の Web サーバへの TLS を用いたアクセスにおいて，当該 PC がサーバ証明書を入手した後に，認証局の公開鍵を利用して行う動作はどれか。

ア　暗号化通信に利用する共通鍵を，認証局の公開鍵を使って復号する。

イ　暗号化通信に利用する共通鍵を生成し，認証局の公開鍵を使って暗号化する。

ウ　サーバ証明書の正当性を，認証局の公開鍵を使って検証する。

エ　利用者が入力して送付する秘匿データを，認証局の公開鍵を使って暗号化する。

問23　従量課金制のクラウドサービスにおける EDoS（Economic Denial of Service，又は Economic Denial of Sustainability）攻撃の説明はどれか。

ア　カード情報の取得を目的に，金融機関が利用しているクラウドサービスに侵入する攻撃
イ　課金回避を目的に，同じハードウェア上に構築された別の仮想マシンに侵入し，課金機能を利用不可にする攻撃
ウ　クラウドサービス利用者の経済的な損失を目的に，リソースを大量消費させる攻撃
エ　パスワード解析を目的に，クラウドサービス環境のリソースを悪用する攻撃

問24　伝達したいメッセージを画像データなどのコンテンツに埋め込み，埋め込んだメッセージの存在を秘匿する技術はどれか。

ア　CAPTCHA　　イ　クリックジャッキング
ウ　ステガノグラフィ　　エ　ストレッチング

問25　アプリケーションソフトウェアにディジタル署名を施す目的はどれか。

ア　アプリケーションソフトウェアの改ざんを利用者が検知できるようにする。
イ　アプリケーションソフトウェアの使用を特定の利用者に制限する。
ウ　アプリケーションソフトウェアの著作権が作成者にあることを証明する。
エ　アプリケーションソフトウェアの利用者による修正や改変を不可能にする。

問26　データベースで管理されるデータの暗号化に用いることができ，かつ，暗号化と復号とで同じ鍵を使用する暗号方式はどれか。

ア　AES　　イ　PKI　　ウ　RSA　　エ　SHA-256

問27　暗号方式に関する説明のうち，適切なものはどれか。

ア　共通鍵暗号方式で相手ごとに秘密の通信をする場合，通信相手が多くなるに従って，鍵管理の手間が増える。

イ　共通鍵暗号方式を用いて通信を暗号化するときには，送信者と受信者で異なる鍵を用いるが，通信相手にそれぞれの鍵を知らせる必要はない。

ウ　公開鍵暗号方式で通信文を暗号化して内容を秘密にした通信をするときには，復号鍵を公開することによって，鍵管理の手間を減らす。

エ　公開鍵暗号方式では，署名に用いる鍵を公開しておく必要がある。

問28　共通脆弱性評価システム（CVSS）の特徴として，適切なものはどれか。

ア　CVSS v2 と CVSS v3 は，脆弱性の深刻度の算出方法が同じであり，どちらのバージョンで算出しても同じ値になる。

イ　情報システムの脆弱性の深刻度に対するオープンで汎用的な評価手法であり，特定ベンダに依存しない評価方法を提供する。

ウ　脆弱性の深刻度を 0 から 100 の数値で表す。

エ　脆弱性を評価する基準は，現状評価基準と環境評価基準の二つである。

問29　SSH の説明はどれか。

ア　MIME を拡張した電子メールの暗号化とディジタル署名に関する標準

イ　オンラインショッピングで安全にクレジットカード決済を行うための仕様

ウ　共通鍵暗号技術と公開鍵暗号技術を併用した電子メールの暗号化，復号の機能をもつ電子メールソフト

エ　リモートログインやリモートファイルコピーのセキュリティを強化したプロトコル，及びそのプロトコルを実装したコマンド

問30　WAF（Web Application Firewall）におけるブラックリスト又はホワイトリストに関する記述のうち，適切なものはどれか。

ア　ブラックリストは，脆弱性がある Web サイトの IP アドレスを登録したものであり，該当する IP アドレスからの通信を遮断する。

イ　ブラックリストは，問題がある通信データパターンを定義したものであり，該当する通信を遮断する。

ウ　ホワイトリストは，暗号化された受信データをどのように復号するかを定義したものであり，復号鍵が登録されていないデータを遮断する。

エ　ホワイトリストは，脆弱性がない Web サイトの FQDN を登録したものであり，登録がない Web サイトへの通信を遮断する。

問31　サイバーセキュリティ基本法において定められたサイバーセキュリティ戦略本部は，どの機関に置かれているか。

ア　経済産業省　　イ　国家安全保障会議

ウ　国会　　エ　内閣

問32　不正アクセス禁止法で規定されている，“不正アクセス行為を助長する行為の禁止”規定によって規制される行為はどれか。

ア　正当な理由なく他人の利用者 ID とパスワードを第三者に提供する。
イ　他人の利用者 ID とパスワードを不正に入手する目的でフィッシングサイトを開設する。
ウ　不正アクセスを目的とし，他人の利用者 ID とパスワードを不正に入手する。
エ　不正アクセスを目的とし，不正に入手した他人の利用者 ID とパスワードを PC に保管する。

問33　電子署名法に関する記述のうち，適切なものはどれか。

ア　電子署名には，電磁的記録ではなく，かつ，コンピュータで処理できないものも含まれる。
イ　電子署名には，民事訴訟法における押印と同様の効力が認められる。
ウ　電子署名の認証業務を行うことができるのは，政府が運営する認証局に限られる。
エ　電子署名は共通鍵暗号技術によるものに限られる。

問34　Webページの著作権に関する記述のうち，適切なものはどれか。

ア　営利目的ではなく趣味として，個人が開設し，公開しているWebページに他人の著作物を無断掲載しても，私的使用であるから著作権の侵害にならない。

イ　作成したプログラムをインターネット上でフリーウェアとして公開した場合，公開されたプログラムは，著作権法で保護されない。

ウ　試用期間中のシェアウェアを使用して作成したデータを，試用期間終了後もWebページに掲載することは，著作権の侵害になる。

エ　特定の分野ごとにWebページのURLを収集し，独自の解釈を付けたリンク集は，著作権法で保護され得る。

問35　ボリュームライセンス契約の説明はどれか。

ア　企業などソフトウェアの大量購入者向けに，インストールできる台数をあらかじめ取り決め，マスタが提供される契約

イ　使用場所を限定した契約であり，特定の施設の中であれば台数や人数に制限なく使用が許される契約

ウ　ソフトウェアをインターネットからダウンロードしたとき画面に表示される契約内容に同意するを選択することによって，使用が許される契約

エ　標準の使用許諾条件を定め，その範囲で一定量のパッケージの包装を解いたときに，権利者と購入者との間に使用許諾契約が自動的に成立したとみなす契約

問36　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（平成 23 年）”における IT の統制目標の一つである“信頼性”はどれか。

ア　情報が，関連する法令や会計基準，社内規則などに合致して処理されること
イ　情報が，正当な権限を有する者以外に利用されないように保護されていること
ウ　情報が，組織の意思・意図に沿って承認され，漏れなく正確に記録・処理されること
エ　情報が，必要とされるときに利用可能であること

問37　JIS Q 27001:2014（情報セキュリティマネジメントシステム－要求事項）に基づいて ISMS 内部監査を行った結果として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　USB メモリの使用を，定められた手順に従って許可していた。
イ　個人情報の誤廃棄事故を主務官庁などに，規定されたとおりに報告していた。
ウ　マルウェアスキャンでスパイウェアが検知され，駆除されていた。
エ　リスクアセスメントを実施した後に，リスク受容基準を決めた。

問38　外部委託管理の監査に関する記述のうち，最も適切なものはどれか。

ア　請負契約においては，委託側の事務所で作業を行っている受託側要員のシステムへのアクセスについて，アクセス管理が妥当かどうかを，委託側が監査できるように定める。

イ　請負契約においては，受託側要員に対する委託側責任者の指揮命令が行われていることを，委託側で監査する。

ウ　外部委託で開発した業務システムの品質管理状況は，委託側で監査せず，受託側で監査する。

エ　機密性が高い業務システムの開発を外部に委託している場合は，自社開発に切り替えるよう，監査結果の報告において改善勧告する。

問39　システム監査において，電子文書の真正性の検証に電子証明書が利用できる公開鍵証明書取得日，電子署名生成日及び検証日の組合せはどれか。

なお，公開鍵証明書の有効期間は 4 年間とし，当該期間中の公開鍵証明書の更新や失効は考慮しない前提とする。

	公開鍵証明書取得日	電子署名生成日	検証日
ア	2012 年 3 月 1 日	2014 年 8 月 1 日	2018 年 12 月 1 日
イ	2014 年 1 月 1 日	2016 年 12 月 1 日	2018 年 2 月 1 日
ウ	2015 年 4 月 1 日	2015 年 5 月 1 日	2018 年 12 月 1 日
エ	2016 年 8 月 1 日	2014 年 7 月 1 日	2018 年 3 月 1 日

問40　合意されたサービス提供時間が 7:00～19:00 であるシステムにおいて，ある日の 16:00 にシステム障害が発生し，サービスが停止した。修理は 21:00 まで掛かり，当日中にサービスは再開できなかった。当日のサービスは予定どおり 7:00 から開始され，サービス提供の時間帯にサービスの計画停止は行っていない。この日の可用性は何%か。ここで，可用性は小数点以下を切り捨てるものとする。

ア　25　　イ　60　　ウ　64　　エ　75

問41　IT サービスマネジメントにおいて，SMS（サービスマネジメントシステム）の効果的な計画立案，運用及び管理を確実にするために，SLA やサービスカタログを文書化し，維持しなければならないのは誰か。

ア　経営者　　イ　顧客
ウ　サービス提供者　　エ　利用者

問42　IT サービスマネジメントにおいて，一次サポートグループが二次サポートグループにインシデントの解決を依頼することを何というか。ここで，一次サポートグループは，インシデントの初期症状のデータを収集し，利用者との継続的なコミュニケーションのための，コミュニケーションの役割を果たすグループであり，二次サポートグループは，専門的技能及び経験をもつグループである。

ア　回避策　　イ　継続的改善
ウ　段階的取扱い　　エ　予防処置

問43　ソフトウェア開発プロジェクトにおいて WBS（Work Breakdown Structure）を使用する目的として，適切なものはどれか。

ア　開発の期間と費用がトレードオフの関係にある場合に，総費用の最適化を図る。
イ　作業の順序関係を明確にして，重点管理すべきクリティカルパスを把握する。
ウ　作業の日程を横棒（バー）で表して，作業の開始時点や終了時点，現時点の進捗を明確にする。
エ　作業を階層的に詳細化して，管理可能な大きさに細分化する。

問44　信頼性設計に関する記述のうち，フェールセーフの説明はどれか。

ア　故障が発生した場合，一部のサービスレベルを低下させても，システムを縮退して運転を継続する設計のこと
イ　システムに冗長な構成を組み入れ，故障が発生した場合，自動的に待機系に切り替えて運転を継続する設計のこと
ウ　システムの一部が故障しても，危険が生じないような構造や仕組みを導入する設計のこと
エ　人間が誤った操作や取扱いができないような構造や仕組みを，システムに対して考慮する設計のこと

問45　データベースの監査ログを取得する目的として，適切なものはどれか。

ア　権限のない利用者のアクセスを拒否する。
イ　チェックポイントからのデータ復旧に使用する。
ウ　データの不正な書換えや削除を事前に検知する。
エ　問題のあるデータベース操作を事後に調査する。

問46　TCP/IP ネットワークのトランスポート層におけるポート番号の説明として，適切なものはどれか。

ア　LAN において NIC（ネットワークインタフェースカード）を識別する情報
イ　TCP/IP ネットワークにおいてホストを識別する情報
ウ　TCP や UDP においてアプリケーションを識別する情報
エ　レイヤ 2 スイッチのポートを識別する情報

問47　データサイエンティストの主要な役割はどれか。

ア　監査対象から独立的かつ客観的立場のシステム監査の専門家として情報システムを総合的に点検及び評価し，組織体の長に助言及び勧告するとともにフォローアップする。
イ　情報科学についての知識を有し，ビジネス課題を解決するためにビッグデータを意味ある形で使えるように分析システムを実装・運用し，課題の解決を支援する。
ウ　多数のコンピュータをスイッチやルータなどのネットワーク機器に接続し，コンピュータ間でデータを高速に送受信するネットワークシステムを構築する。
エ　プロジェクトを企画・実行する上で，予算管理，進捗管理，人員配置やモチベーション管理，品質コントロールなどについて重要な決定権をもち，プロジェクトにおける総合的な責任を負う。

問48　ディジタルディバイドの解消のために取り組むべきことはどれか。

ア　IT 投資額の見積りを行い，投資目的に基づいて効果目標を設定して，効果目標ごとに目標達成の可能性を事前に評価すること

イ　IT の活用による家電や設備などの省エネルギー化及びテレワークなどによる業務の効率向上によって，エネルギー消費を削減すること

ウ　情報リテラシの習得機会を増やしたり，情報通信機器や情報サービスが一層利用しやすい環境を整備したりすること

エ　製品や食料品などの製造段階から最終消費段階又は廃棄段階までの全工程について，IC タグを活用して流通情報を追跡可能にすること

問49　企画，要件定義，システム開発，ソフトウェア実装，ハードウェア実装，保守から成る一連のプロセスにおいて，要件定義プロセスで実施すべきものはどれか。

ア　システムに関わり合いをもつ利害関係者の種類を識別し，利害関係者のニーズ及び要望並びに課せられる制約条件を識別する。

イ　事業の目的，目標を達成するために必要なシステム化の方針，及びシステムを実現するための実施計画を立案する。

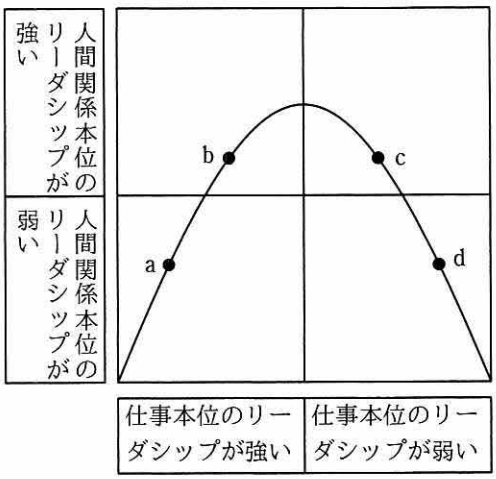
ウ　目的とするシステムを得るために，システムの機能及び能力を定義し，システム方式設計によってハードウェア，ソフトウェアなどによる実現方式を確立する。

エ　利害関係者の要件を満足するソフトウェア製品又はソフトウェアサービスを得るための，方式設計と適格性の確認を実施する。

問50　リーダシップのスタイルは，その組織の状況に合わせる必要がある。組織の状況とリーダシップのスタイルの関係に次のことが想定できるとすると，スポーツチームの監督のリーダシップのスタイルのうち，図中のｄと考えられるものはどれか。

〔組織の状況とリーダシップのスタイルの関係〕

組織は発足当時，構成員や仕組みの成熟度が低いので，リーダが仕事本位のリーダシップで引っ張っていく。成熟度が上がるにつれ，リーダと構成員の人間関係が培われ，仕事本位から人間関係本位のリーダシップに移行していく。更に成熟度が進むと，構成員は自主的に行動できるようになり，仕事本位，人間関係本位のリーダシップがいずれも弱まっていく。



ア　うるさく言うのも半分くらいで勝てるようになってきた。

イ　勝つためには選手と十分に話し合って戦略を作ることだ。

ウ　勝つためには選手に戦術の立案と実行を任せることだ。

エ　選手をきちんと管理することが勝つための条件だ。

〔 メ モ 用 紙 〕

〔 メ モ 用 紙 〕

〔 メ モ 用 紙 〕

6. 退室可能時間中に退室する場合は，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 ～ 10:50

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。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。
9. 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。
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。