SG

平成31年度　春期
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〕　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1　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）において，トップマネジメントがマネジメントレビューで考慮しなければならない事項としている組合せとして，適切なものはどれか。

	マネジメントレビューで考慮しなければならない事項		
ア	前回までのマネジメントレビューの結果とった処置の状況	トップマネジメントが設定した情報セキュリティ目的	内部監査の結果
イ	前回までのマネジメントレビューの結果とった処置の状況	トップマネジメントが設定した情報セキュリティ目的	発生した不適合及び是正処置の状況
ウ	前回までのマネジメントレビューの結果とった処置の状況	内部監査の結果	発生した不適合及び是正処置の状況
エ	トップマネジメントが設定した情報セキュリティ目的	内部監査の結果	発生した不適合及び是正処置の状況

問2　JPCERT/CC “CSIRT ガイド（2015 年 11 月 26 日）” では，CSIRT を活動とサービス対象によって六つに分類しており，その一つにコーディネーションセンターがある。コーディネーションセンターの活動とサービス対象の組合せとして，適切なものはどれか。

	活動	サービス対象
ア	インシデント対応の中で，CSIRT 間の情報連携，調整を行う。	他の CSIRT
イ	インシデントの傾向分析やマルウェアの解析，攻撃の痕跡の分析を行い，必要に応じて注意を喚起する。	関係組織，国又は地域
ウ	自社製品の脆弱性に対応し，パッチ作成や注意喚起を行う。	自社製品の利用者
エ	組織内 CSIRT の機能の一部又は全部をサービスプロバイダとして，有償で請け負う。	顧客

問3　CRYPTREC の役割として，適切なものはどれか。

ア　外国為替及び外国貿易法で規制されている暗号装置の輸出許可申請を審査，承認する。

イ　政府調達において IT 関連製品のセキュリティ機能の適切性を評価，認証する。

ウ　電子政府での利用を推奨する暗号技術の安全性を評価，監視する。

エ　民間企業のサーバに対するセキュリティ攻撃を監視，検知する。

問４　JIS Q 27002:2014（情報セキュリティ管理策の実践のための規範）の“サポートユーティリティ”に関する例示に基づいて，サポートユーティリティと判断されるものはどれか。

ア　サーバ室の空調　　イ　サーバの保守契約
ウ　特権管理プログラム　　エ　ネットワーク管理者

問５　リスク対応のうち，リスクファイナンシングに該当するものはどれか。

ア　システムが被害を受けるリスクを想定して，保険を掛ける。
イ　システムの被害につながるリスクの顕在化を抑える対策に資金を投入する。
ウ　リスクが大きいと評価されたシステムを廃止し，新たなセキュアなシステムの構築に資金を投入する。
エ　リスクが顕在化した場合のシステムの被害を小さくする設備に資金を投入する。

問６　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“リスクレベル”の定義はどれか。

ア　脅威によって付け込まれる可能性のある，資産又は管理策の弱点
イ　結果とその起こりやすさの組合せとして表現される，リスクの大きさ
ウ　対応すべきリスクに付与する優先順位
エ　リスクの重大性を評価するために目安とする条件

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）では，リスクを運用管理することについて，アカウンタビリティ及び権限をもつ人又は主体を何と呼んでいるか。

ア　監査員　　イ　トップマネジメント
ウ　利害関係者　　エ　リスク所有者

問８　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）において，情報セキュリティ目的をどのように達成するかについて計画するとき，“実施事項”，“責任者”，“達成期限”のほかに，決定しなければならない事項として定められているものはどれか。

ア　“必要な資源”及び“結果の評価方法”
イ　“必要な資源”及び“適用する管理策”
ウ　“必要なプロセス”及び“結果の評価方法”
エ　“必要なプロセス”及び“適用する管理策”

問９　組織での情報資産管理台帳の記入方法のうち，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）”に照らして，適切なものはどれか。

ア　様々な情報が混在し，重要度を一律に評価できないドキュメントファイルは，企業の存続を左右しかねない情報や個人情報を含む場合だけ台帳に記入する。
イ　時間経過に伴い重要度が変化する情報資産は，重要度が確定してから，又は組織で定めた未記入措置期間が経過してから，台帳に記入する。
ウ　情報資産を紙媒体と電子データの両方で保存している場合は，いずれか片方だけを台帳に記入する。
エ　利用しているクラウドサービスに保存している情報資産を含めて，台帳に記入する。

問10　DNS キャッシュポイズニングに該当するものはどれか。

ア　HTML メールの本文にリンクを設定し，表示文字列は，有名企業の DNS サーバに登録されているドメイン名を含むものにして，実際のリンク先は攻撃者の Web サイトに設定した上で，攻撃対象に送り，リンク先を開かせる。

イ　PC が問合せを行う DNS キャッシュサーバに偽の DNS 応答を送ることによって，偽のドメイン情報を注入する。

ウ　Unicode を使って偽装したドメイン名を DNS サーバに登録しておき，さらに，そのドメインを含む情報をインターネット検索結果の上位に表示させる。

エ　WHOIS データベースサービスを提供するサーバを DoS 攻撃して，WHOIS データベースにあるドメインの DNS 情報を参照できないようにする。

問11　SPF（Sender Policy Framework）を利用する目的はどれか。

ア　HTTP 通信の経路上での中間者攻撃を検知する。

イ　LAN への PC の不正接続を検知する。

ウ　内部ネットワークへの侵入を検知する。

エ　メール送信者のドメインのなりすましを検知する。

問12　ファイルの属性情報として，ファイルに対する読取り，書込み，実行の権限を独立に設定できる OS がある。この 3 種類の権限は，それぞれに 1 ビットを使って許可，不許可を設定する。この 3 ビットを 8 進数表現 0 ～ 7 の数字で設定するとき，次の試行結果から考えて，適切なものはどれか。

〔試行結果〕

① 0 を設定したら，読取り，書込み，実行ができなくなってしまった。

② 3 を設定したら，読取りと書込みはできたが，実行ができなかった。

③ 7 を設定したら，読取り，書込み，実行ができるようになった。

ア　2 を設定すると，読取りと実行ができる。

イ　4 を設定すると，実行だけができる。

ウ　5 を設定すると，書込みだけができる。

エ　6 を設定すると，読取りと書込みができる。

問13　入室時と退室時に ID カードを用いて認証を行い，入退室を管理する。このとき，入室時の認証に用いられなかった ID カードでの退室を許可しない，又は退室時の認証に用いられなかった ID カードでの再入室を許可しないコントロールを行う仕組みはどれか。

ア　TPMOR（Two Person Minimum Occupancy Rule）

イ　アンチパスバック

ウ　インターロックゲート

エ　パニックオープン

問14　PCI DSS v3.2.1 において，取引承認を受けた後の加盟店及びサービスプロバイダにおけるカードセキュリティコードの取扱方法の組みのうち，適切なものはどれか。ここで，用語の定義は次のとおりとする。

〔用語の定義〕

加盟店とは，クレジットカードを商品又はサービスの支払方法として取り扱う事業体をいう。

サービスプロバイダとは，他の事業体の委託でカード会員データの処理，保管，伝送に直接関わる事業体をいう。イシュア（クレジットカード発行や発行サービスを行う事業体）は除く。

カードセキュリティコードには，カード表面又は署名欄に印字されている，3 桁又は 4 桁の数値がある。

	加盟店におけるカードセキュリティコードの取扱方法	サービスプロバイダにおけるカードセキュリティコードの取扱方法
ア	暗号化して加盟店内に保管する。	暗号化してサービスプロバイダのシステム内に保管する。
イ	平文で加盟店内に保管する。	保管しない。
ウ	保管しない。	平文でサービスプロバイダのシステム内に保管する。
エ	保管しない。	保管しない。

問15　IPS の説明はどれか。

ア　Web サーバなどの負荷を軽減するために，暗号化や復号の処理を高速に行う専用ハードウェア

イ　サーバやネットワークへの侵入を防ぐために，不正な通信を検知して遮断する装置

ウ　システムの脆弱性を見つけるために，疑似的に攻撃を行い侵入を試みるツール

エ　認可されていない者による入室を防ぐために，指紋，虹彩などの生体情報を用いて本人認証を行うシステム

問16　特定のサービスやシステムから流出した認証情報を攻撃者が用いて，認証情報を複数のサービスやシステムで使い回している利用者のアカウントへのログインを試みる攻撃はどれか。

ア　パスワードリスト攻撃　　イ　ブルートフォース攻撃

ウ　リバースブルートフォース攻撃　　エ　レインボー攻撃

問17　社内 PC からインターネットに通信するとき，パケット中にある社内 PC のプライベート IP アドレスとポート番号の組合せを，ファイアウォールのインターネット側の IP アドレスとポート番号の組合せに変換することによって，インターネットからは分からないように社内 PC のプライベート IP アドレスを隠蔽することが可能なものはどれか。

ア　BGP　　イ　IP マスカレード

ウ　OSPF　　エ　フラグメンテーション

問18　ペネトレーションテストに該当するものはどれか。

ア　検査対象の実行プログラムの設計書，ソースコードに着目し，開発プロセスの各工程にセキュリティ上の問題がないかどうかをツールや目視で確認する。

イ　公開 Web サーバの各コンテンツファイルのハッシュ値を管理し，定期的に各ファイルから生成したハッシュ値と一致するかどうかを確認する。

ウ　公開 Web サーバや組織のネットワークの脆弱性を探索し，サーバに実際に侵入できるかどうかを確認する。

エ　内部ネットワークのサーバやネットワーク機器の IPFIX 情報から，各 PC の通信に異常な振る舞いがないかどうかを確認する。

問19　PC への侵入に成功したマルウェアがインターネット上の指令サーバと通信を行う場合に，宛先ポートとして使用される TCP ポート番号 80 に関する記述のうち，適切なものはどれか。

ア　DNS のゾーン転送に使用されることから，通信がファイアウォールで許可されている可能性が高い。

イ　Web サイトの HTTPS 通信での閲覧に使用されることから，マルウェアと指令サーバとの間の通信が侵入検知システムで検知される可能性が低い。

ウ　Web サイトの閲覧に使用されることから，通信がファイアウォールで許可されている可能性が高い。

エ　ドメイン名の名前解決に使用されることから，マルウェアと指令サーバとの間の通信が侵入検知システムで検知される可能性が低い。

問20　無線 LAN を利用できる者を限定したいとき，アクセスポイントへの第三者による無断接続の防止に最も効果があるものはどれか。

ア　MAC アドレスフィルタリングを設定する。
イ　SSID には英数字を含む 8 字以上の文字列を設定する。
ウ　セキュリティ方式に WEP を使用し，十分に長い事前共有鍵を設定する。
エ　セキュリティ方式に WPA2-PSK を使用し，十分に長い事前共有鍵を設定する。

問21　Web サイトで利用される CAPTCHA に該当するものはどれか。

ア　人からのアクセスであることを確認できるよう，アクセスした者に応答を求め，その応答を分析する仕組み
イ　不正な SQL 文をデータベースに送信しないよう，Web サーバに入力された文字列をプレースホルダに割り当てて SQL 文を組み立てる仕組み
ウ　利用者が本人であることを確認できるよう，Web サイトから一定時間ごとに異なるパスワードを要求する仕組み
エ　利用者が本人であることを確認できるよう，乱数を Web サイト側で生成して利用者に送り，利用者側でその乱数を鍵としてパスワードを暗号化し，Web サイトに送り返す仕組み

問22　利用者 PC の内蔵ストレージが暗号化されていないとき，攻撃者が利用者 PC から内蔵ストレージを抜き取り，攻撃者が用意した PC に接続して内蔵ストレージ内の情報を盗む攻撃の対策に該当するものはどれか。

ア　内蔵ストレージにインストールした OS の利用者アカウントに対して，ログインパスワードを設定する。

イ　内蔵ストレージに保存したファイルの読取り権限を，ファイルの所有者だけに付与する。

ウ　利用者 PC 上で HDD パスワードを設定する。

エ　利用者 PC に BIOS パスワードを設定する。

問23　A 氏から B 氏に電子メールを送る際の S/MIME の利用に関する記述のうち，適切なものはどれか。

ア　A 氏は B 氏の公開鍵を用いることなく，B 氏だけが閲覧可能な暗号化電子メールを送ることができる。

イ　B 氏は受信した電子メールに記載されている内容が事実であることを，公的機関に問い合わせることによって確認できる。

ウ　B 氏は受信した電子メールに記載されている内容は A 氏が署名したものであり，第三者による改ざんはないことを確認できる。

エ　万一，マルウェアに感染したファイルを添付して送信した場合に B 氏が添付ファイルを開いても，B 氏の PC がマルウェアに感染することを防ぐことができる。

問24　XML 署名を利用することによってできることはどれか。

ア　TLS において，HTTP 通信の暗号化及び署名の付与に利用することによって，通信経路上での XML ファイルの盗聴を防止する。

イ　XML と JavaScript がもつ非同期の HTTP 通信機能を使い，Web ページの内容を動的に書き換えた上で署名を付与することによって，対話型の Web ページを作成する。

ウ　XML 文書全体に対する単一の署名だけではなく，文書の一部に対して署名を付与する部分署名や多重署名などの複雑な要件に対応する。

エ　隠したい署名データを画像データの中に埋め込むことによって，署名の存在自体を外から判別できなくする。

問25　データベースのアカウントの種類とそれに付与する権限の組合せのうち，情報セキュリティ上，適切なものはどれか。

	アカウントの種類	レコードの更新権限	テーブルの作成・削除権限
ア	データ構造の定義用アカウント	有	無
イ	データ構造の定義用アカウント	無	有
ウ	データの入力・更新用アカウント	有	有
エ	データの入力・更新用アカウント	無	有

問26　メッセージ認証符号の利用目的に該当するものはどれか。

ア　メッセージが改ざんされていないことを確認する。

イ　メッセージの暗号化方式を確認する。

ウ　メッセージの概要を確認する。

エ　メッセージの秘匿性を確保する。

問27　楕円曲線暗号の特徴はどれか。

ア　RSA 暗号と比べて，短い鍵長で同レベルの安全性が実現できる。
イ　共通鍵暗号方式であり，暗号化や復号の処理を高速に行うことができる。
ウ　総当たりによる解読が不可能なことが，数学的に証明されている。
エ　データを秘匿する目的で用いる場合，復号鍵を秘密にしておく必要がない。

問28　OpenPGP や S/MIME において用いられるハイブリッド暗号方式の特徴はどれか。

ア　暗号通信方式として IPsec と TLS を選択可能にすることによって利用者の利便性を高める。
イ　公開鍵暗号方式と共通鍵暗号方式を組み合わせることによって鍵管理コストと処理性能の両立を図る。
ウ　複数の異なる共通鍵暗号方式を組み合わせることによって処理性能を高める。
エ　複数の異なる公開鍵暗号方式を組み合わせることによって安全性を高める。

問29　利用者 PC 上の SSH クライアントからサーバに公開鍵認証方式で SSH 接続するとき，利用者のログイン認証時にサーバが使用する鍵と SSH クライアントが使用する鍵の組みはどれか。

ア　サーバに登録された SSH クライアントの公開鍵と，利用者 PC 上の SSH クライアントの公開鍵
イ　サーバに登録された SSH クライアントの公開鍵と，利用者 PC 上の SSH クライアントの秘密鍵
ウ　サーバに登録された SSH クライアントの秘密鍵と，利用者 PC 上の SSH クライアントの公開鍵
エ　サーバに登録された SSH クライアントの秘密鍵と，利用者 PC 上の SSH クライアントの秘密鍵

問30　侵入者やマルウェアの挙動を調査するために，意図的に脆弱性をもたせたシステム又はネットワークはどれか。

ア　DMZ　　イ　SIEM
ウ　ハニーポット　　エ　ボットネット

問31　JIS Q 15001:2017（個人情報保護マネジメントシステム－要求事項）に関する記述のうち，適切なものはどれか。

ア　開示対象個人情報は，保有個人データとは別に定義されており，保有期間によらず全ての個人情報が該当すると定められている。
イ　規格文書の構成は，JIS Q 27001:2014 と異なり，マネジメントシステム規格に共通的に用いられる章立てが採用されていない。
ウ　特定の機微な個人情報が定義されており，労働組合への加盟といった情報が例として挙げられている。
エ　本人から書面に記載された個人情報を直接取得する場合には，利用目的などをあらかじめ書面によって本人に明示し，同意を得なければならないと定められている。

問32　“政府機関等の情報セキュリティ対策のための統一基準（平成 30 年度版）”に関する説明として，適切なものはどれか。

ア　機密性，完全性及び可用性それぞれの観点による情報の格付の区分を定義している。
イ　個人情報保護法に基づいて制定されたものである。
ウ　適用範囲は，全ての政府機関及び全ての民間企業としている。
エ　不正アクセス禁止法に基づいて制定されたものである。

問33　企業が，“特定電子メールの送信の適正化等に関する法律”における特定電子メールに該当する広告宣伝メールを送信する場合に関する記述のうち，適切なものはどれか。

ア　SMS で送信する場合はオプトアウト方式を利用する。
イ　オプトイン方式，オプトアウト方式のいずれかを選択する。
ウ　原則としてオプトアウト方式を利用する。
エ　原則としてオプトイン方式を利用する。

問34　個人情報保護委員会“特定個人情報の適正な取扱いに関するガイドライン（事業者編）平成 30 年 9 月 28 日最終改正”及びその“Q&A”によれば，事業者によるファイル作成が**禁止されている場合**はどれか。

なお，“Q&A”とは“「特定個人情報の適正な取扱いに関するガイドライン（事業者編）」及び「（別冊）金融業務における特定個人情報の適正な取扱いに関するガイドライン」に関する Q&A 平成 30 年 9 月 28 日更新”のことである。

ア　システム障害に備えた特定個人情報ファイルのバックアップファイルを作成する場合
イ　従業員の個人番号を利用して業務成績を管理するファイルを作成する場合
ウ　税務署に提出する資料間の整合性を確認するために個人番号を記載した明細表などチェック用ファイルを作成する場合
エ　保険契約者の死亡保険金支払に伴う支払調書ファイルを作成する場合

問35　著作者人格権に該当するものはどれか。

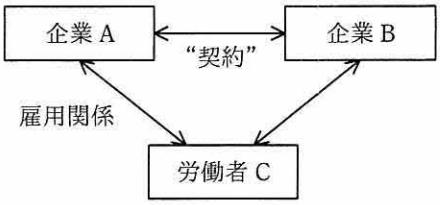
ア　印刷，撮影，複写などの方法によって著作物を複製する権利

イ　公衆からの要求に応じて自動的にサーバから情報を送信する権利

ウ　著作物の複製物を公衆に貸し出す権利

エ　自らの意思に反して著作物を変更，切除されない権利

問36　図は，企業と労働者の関係を表している。企業 B と労働者 C の関係に関する記述のうち，適切なものはどれか。



ア　“契約”が請負契約で，企業 A が受託者，企業 B が委託者であるとき，企業 B と労働者 C との間には，指揮命令関係が生じる。

イ　“契約”が出向にかかわる契約で，企業 A が企業 B に労働者 C を出向させたとき，企業 B と労働者 C との間には指揮命令関係が生じる。

ウ　“契約”が労働者派遣契約で，企業 A が派遣元，企業 B が派遣先であるとき，企業 B と労働者 C の間にも，雇用関係が生じる。

エ　“契約”が労働者派遣契約で，企業 A が派遣元，企業 B が派遣先であるとき，企業 B に労働者 C が出向しているといえる。

問37　経営者が社内のシステム監査人の外観上の独立性を担保するために講じる措置として，最も適切なものはどれか。

ア　システム監査人にITに関する継続的学習を義務付ける。
イ　システム監査人に必要な知識や経験を定めて公表する。
ウ　システム監査人の監査技法研修制度を設ける。
エ　システム監査人の所属部署を内部監査部門とする。

問38　ソフトウェア開発プロセスにおけるセキュリティを確保するための取組について，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）の附属書Aの管理策に照らして監査を行った。判明した状況のうち，監査人が監査報告書に指摘事項として記載すべきものはどれか。

ア　ソフトウェア開発におけるセキュリティ機能の試験は，開発期間が終了した後に実施している。
イ　ソフトウェア開発は，セキュリティ確保に配慮した開発環境において行っている。
ウ　ソフトウェア開発を外部委託している場合，外部委託先による開発活動の監督・監視において，セキュリティ確保の観点を考慮している。
エ　パッケージソフトウェアを活用した開発において，セキュリティ確保の観点から，パッケージソフトウェアの変更は必要な変更に限定している。

問39　システム監査報告書に記載する指摘事項に関する説明のうち，適切なものはどれか。

ア　監査証拠による裏付けの有無にかかわらず，監査人が指摘事項とする必要があると判断した事項を記載する。

イ　監査人が指摘事項とする必要があると判断した事項のうち，監査対象部門の責任者が承認した事項を記載する。

ウ　調査結果に事実誤認がないことを監査対象部門に確認した上で，監査人が指摘事項とする必要があると判断した事項を記載する。

エ　不備の内容や重要性は考慮せず，全てを漏れなく指摘事項として記載する。

問40　経済産業省“情報セキュリティ監査基準 実施基準ガイドライン（Ver1.0）”における，情報セキュリティ対策の適切性に対して一定の保証を付与することを目的とする監査（保証型の監査）と情報セキュリティ対策の改善に役立つ助言を行うことを目的とする監査（助言型の監査）の実施に関する記述のうち，適切なものはどれか。

ア　同じ監査対象に対して情報セキュリティ監査を実施する場合，保証型の監査から手がけ，保証が得られた後に助言型の監査に切り替えなければならない。

イ　情報セキュリティ監査において，保証型の監査と助言型の監査は排他的であり，監査人はどちらで監査を実施するかを決定しなければならない。

ウ　情報セキュリティ監査を保証型で実施するか助言型で実施するかは，監査要請者のニーズによって決定するのではなく，監査人の責任において決定する。

エ　不特定多数の利害関係者の情報を取り扱う情報システムに対しては，保証型の監査を定期的に実施し，その結果を開示することが有用である。

問41　あるデータセンタでは，受発注管理システムの運用サービスを提供している。次の受発注管理システムの運用中の事象において，インシデントに該当するものはどれか。

〔受発注管理システムの運用中の事象〕

夜間バッチ処理において，注文トランザクションデータから注文書を出力するプログラムが異常終了した。異常終了を検知した運用担当者から連絡を受けた保守担当者は，緊急出社してサービスを回復し，後日，異常終了の原因となったプログラムの誤りを修正した。

ア　異常終了の検知　　イ　プログラムの誤り

ウ　プログラムの異常終了　　エ　保守担当者の緊急出社

問42　システム運用におけるデータの取扱いに関する記述のうち，最も適切なものはどれか。

ア　エラーデータの修正は，データの発生元で行うものと，システムの運用者が所属する運用部門で行うものに分けて実施する。

イ　原始データの信ぴょう性のチェック及び原始データの受渡しの管理は，システムの運用者が所属する運用部門が担当するのが良い。

ウ　データの発生元でエラーデータを修正すると時間が掛かるので，エラーデータの修正はできるだけシステムの運用者が所属する運用部門に任せる方が良い。

エ　入力データのエラー検出は，データを処理する段階で行うよりも，入力段階で行った方が検出及び修正の作業効率が良い。

問43　組織が実施する作業を，プロジェクトと定常業務の二つに類別するとき，プロジェクトに該当するものはどれか。

ア　企業の経理部門が行っている，月次・半期・年次の決算処理
イ　金融機関の各支店が行っている，個人顧客向けの住宅ローンの貸付け
ウ　精密機器の製造販売企業が行っている，製品の取扱方法に関する問合せへの対応
エ　地方公共団体が行っている，庁舎の建替え

問44　クライアントサーバシステムの特徴として，適切なものはどれか。

ア　クライアントとサーバが協調して，目的の処理を遂行する分散処理形態であり，サービスという概念で機能を分割し，サーバがサービスを提供する。
イ　クライアントとサーバが協調しながら共通のデータ資源にアクセスするために，システム構成として密結合システムを採用している。
ウ　クライアントは，多くのサーバからの要求に対して，互いに協調しながら同時にサービスを提供し，サーバからのクライアント資源へのアクセスを制御する。
エ　サービスを提供するクライアント内に設置するデータベースも，規模に対応して柔軟に拡大することができる。

問45　トランザクション T_1 が更新中のデータを，トランザクション T_2 が参照しようとしたとき，更新と参照の処理結果を矛盾させないようにするための DBMS の機能はどれか。

ア　最適化　　イ　参照制約
ウ　排他制御　　エ　副問合せ

問46　PC を使って電子メールの送受信を行う際に，電子メールの送信とメールサーバからの電子メールの受信に使用するプロトコルの組合せとして，適切なものはどれか。

	送信プロトコル	受信プロトコル
ア	IMAP4	POP3
イ	IMAP4	SMTP
ウ	POP3	IMAP4
エ	SMTP	IMAP4

問47　BPO の説明はどれか。

ア　災害や事故で被害を受けても，重要事業を中断させない，又は可能な限り中断期間を短くする仕組みを構築すること

イ　社内業務のうちコアビジネスでない事業に関わる業務の一部又は全部を，外部の専門的な企業に委託すること

ウ　製品の基準生産計画，部品表及び在庫情報を基に，資材の所要量と必要な時期を求め，これを基準に資材の手配，納入の管理を支援する生産管理手法のこと

エ　プロジェクトを，戦略との適合性や費用対効果，リスクといった観点から評価を行い，情報化投資のバランスを管理し，最適化を図ること

問48　2種類のIT機器a，bの購入を検討している。それぞれの耐用年数を考慮して投資の回収期間を設定し，この投資で得られる利益の全額を投資額の回収に充てることにした。a，b それぞれにおいて，設定した回収期間で投資額を回収するために最低限必要となる年間利益に関する記述のうち，適切なものはどれか。ここで，年間利益は毎年均等とし，回収期間における利率は考慮しないものとする。

	a	b
投資額（万円）	90	300
回収期間（年）	3	5

ア　aとbは同額の年間利益が必要である。

イ　aはbの2倍の年間利益が必要である。

ウ　bはaの1.5倍の年間利益が必要である。

エ　bはaの2倍の年間利益が必要である。

問49　RFI に回答した各ベンダに対して RFP を提示した。今後のベンダ選定に当たって，公正に手続を進めるためにあらかじめ実施しておくことはどれか。

ア　RFI の回答内容の評価が高いベンダに対して，選定から外れたときに備えて，再提案できる救済措置を講じておく。

イ　現行のシステムを熟知したベンダに対して，RFP の要求事項とは別に，そのベンダを選定しやすいように評価を高くしておく。

ウ　提案の評価基準や要求事項の適合度への重み付けをするルールを設けるなど，選定の基準や手順を確立しておく。

エ　ベンダ選定から契約締結までの期間を短縮するために，RFP を提示した全ベンダに内示書を発行して，契約書や作業範囲記述書の作成を依頼しておく。

問50　企業が社会的責任を果たすために実施すべき施策のうち，環境対策の観点から実施するものはどれか。

ア　株主に対し，企業の経営状況の透明化を図る。

イ　グリーン購入に向けて社内体制を整備する。

ウ　災害時における従業員のボランティア活動を支援する制度を構築する。

エ　社内に倫理ヘルプラインを設置する。

〔 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。