SG

平成30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1　サイバーレスキュー隊（J-CRAT）に関する記述として，適切なものはどれか。

ア　サイバーセキュリティ基本法に基づき内閣官房に設置されている。
イ　自社や顧客に関係した情報セキュリティインシデントに対応する企業内活動を担う。
ウ　情報セキュリティマネジメントシステム適合性評価制度を運営する。
エ　標的型サイバー攻撃の被害低減と攻撃連鎖の遮断を支援する活動を担う。

問2　リスク対応のうち，リスクの回避に該当するものはどれか。

ア　リスクが顕在化する可能性を低減するために，情報システムのハードウェア構成を冗長化する。
イ　リスクの顕在化に伴う被害からの復旧に掛かる費用を算定し，保険を掛ける。
ウ　リスクレベルが大きいと評価した情報システムを用いるサービスの提供をやめる。
エ　リスクレベルが小さいので特別な対応をとらないという意思決定をする。

問3　JIS Q 27000:2014（情報セキュリティマネジメントシステム－用語）におけるリスク評価についての説明として，適切なものはどれか。

ア　対策を講じることによって，リスクを修正するプロセス
イ　リスクとその大きさが受容可能か否かを決定するために，リスク分析の結果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　リスクの発見，認識及び記述を行うプロセス

問4　退職する従業員による不正を防ぐための対策のうち，IPA“組織における内部不正防止ガイドライン（第4版）”に照らして，適切なものはどれか。

ア　在職中に知り得た重要情報を退職後に公開しないように，退職予定者に提出させる秘密保持誓約書には，秘密保持の対象を明示せず，重要情報を客観的に特定できないようにしておく。

イ　退職後，同業他社に転職して重要情報を漏らすということがないように，職業選択の自由を行使しないことを明記した上で，具体的な範囲を設定しない包括的な競業避止義務契約を入社時に締結する。

ウ　退職者による重要情報の持出しなどの不正行為を調査できるように，従業員に付与した利用者IDや権限は退職後も有効にしておく。

エ　退職間際に重要情報の不正な持出しが行われやすいので，退職予定者に対する重要情報へのアクセスや媒体の持出しの監視を強化する。

問5　JIS Q 27000:2014（情報セキュリティマネジメントシステム－用語）及び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）における情報セキュリティ事象と情報セキュリティインシデントの関係のうち，適切なものはどれか。

ア　情報セキュリティ事象と情報セキュリティインシデントは同じものである。

イ　情報セキュリティ事象は情報セキュリティインシデントと無関係である。

ウ　単独又は一連の情報セキュリティ事象は，情報セキュリティインシデントに分類され得る。

エ　単独又は一連の情報セキュリティ事象は，全て情報セキュリティインシデントである。

問6　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）”を参考に，次の表に基づいて，情報資産の機密性を評価した。機密性が評価値 2 とされた情報資産とその判断理由として，最も適切な組みはどれか。

評価値	評価基準
2	法律で安全管理が義務付けられている，又は，漏えいすると取引先や顧客への大きな影響，自社への深刻若しくは大きな影響がある。
1	漏えいすると自社の事業に影響がある。
0	漏えいしても自社の事業に影響はない。

	情報資産	判断理由
ア	自社 EC サイト（電子データ）	DDoS 攻撃を受けて顧客からアクセスされなくなると，機会損失が生じて売上が減少する。
イ	自社 EC サイト（電子データ）	ディレクトリリスティングされると，廃版となった商品情報が EC サイト訪問者に勝手に閲覧される。
ウ	主力製品の設計図（電子データ）	責任者の承諾なく設計者によって無断で変更されると，製品の機能，品質，納期，製造工程に関する問題が生じ，損失が発生する。
エ	主力製品の設計図（電子データ）	不正アクセスによって外部に流出すると，技術やデザインによる製品の競争優位性が失われて，製品の売上が減少する。

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）でいう特権的アクセス権の管理について，情報システムの管理特権を利用した行為はどれか。

ア　許可を受けた営業担当者が，社外から社内の営業システムにアクセスし，業務を行う。

イ　経営者が，機密性の高い経営情報にアクセスし，経営の意思決定に生かす。

ウ　システム管理者が，業務システムのプログラムにアクセスし，バージョンアップを行う。

エ　来訪者が，デモンストレーション用のシステムにアクセスし，システム機能の確認を行う。

問8　JIS Q 27000:2014（情報セキュリティマネジメントシステム－用語）において，“エンティティは，それが主張するとおりのものであるという特性”と定義されているものはどれか。

ア　真正性　　イ　信頼性　　ウ　責任追跡性　　エ　否認防止

問９　ネットワーク障害の発生時に，その原因を調べるために，ミラーポート及び LAN アナライザを用意して，LAN アナライザを使用できるようにしておくときに，留意することはどれか。

ア　LAN アナライザがパケットを破棄してしまうので，測定中は測定対象外のコンピュータの利用を制限しておく必要がある。

イ　LAN アナライザはネットワークを通過するパケットを表示できるので，盗聴などに悪用されないように注意する必要がある。

ウ　障害発生に備えて，ネットワーク利用者に対して LAN アナライザの保管場所と使用方法を周知しておく必要がある。

エ　測定に当たって，LAN ケーブルを一時的に抜く必要があるので，ネットワーク利用者に対して測定日を事前に知らせておく必要がある。

問10　SPF（Sender Policy Framework）の仕組みはどれか。

ア　電子メールを受信するサーバが，電子メールに付与されているディジタル署名を使って，送信元ドメインの詐称がないことを確認する。

イ　電子メールを受信するサーバが，電子メールの送信元のドメイン情報と，電子メールを送信したサーバの IP アドレスから，ドメインの詐称がないことを確認する。

ウ　電子メールを送信するサーバが，送信する電子メールの送信者の上司からの承認が得られるまで，一時的に電子メールの送信を保留する。

エ　電子メールを送信するサーバが，電子メールの宛先のドメインや送信者のメールアドレスを問わず，全ての電子メールをアーカイブする。

問11　UPSの導入によって期待できる情報セキュリティ対策としての効果はどれか。

ア　PCが電力線通信（PLC）からマルウェアに感染することを防ぐ。
イ　サーバと端末間の通信における情報漏えいを防ぐ。
ウ　電源の瞬断に起因するデータの破損を防ぐ。
エ　電子メールの内容が改ざんされることを防ぐ。

問12　WAFの説明はどれか。

ア　Web サイトに対するアクセス内容を監視し，攻撃とみなされるパターンを検知したときに当該アクセスを遮断する。
イ　Wi-Fi アライアンスが認定した無線 LAN の暗号化方式の規格であり，AES 暗号に対応している。
ウ　様々なシステムの動作ログを一元的に蓄積，管理し，セキュリティ上の脅威となる事象をいち早く検知，分析する。
エ　ファイアウォール機能を有し，マルウェア対策機能，侵入検知機能などの複数のセキュリティ機能を連携させ，統合的に管理する。

問13　サーバへの侵入を防止するのに有効な対策はどれか。

ア　サーバ上にあるファイルのフィンガプリントを保存する。
イ　サーバ上の不要なサービスを停止する。
ウ　サーバのバックアップを定期的に取得する。
エ　サーバを冗長化して耐故障性を高める。

問14　セキュリティバイデザインの説明はどれか。

ア　開発済みのシステムに対して，第三者の情報セキュリティ専門家が，脆弱性診断を行い，システムの品質及びセキュリティを高めることである。

イ　開発済みのシステムに対して，リスクアセスメントを行い，リスクアセスメント結果に基づいてシステムを改修することである。

ウ　システムの運用において，第三者による監査結果を基にシステムを改修することである。

エ　システムの企画・設計段階からセキュリティを確保する方策のことである。

問15　A 社では，インターネットを介して提供される複数のクラウドサービスを，共用 PC から利用している。共用 PC の利用者 ID は従業員の間で共用しているが，クラウドサービスの利用者 ID は従業員ごとに異なるものを使用している。クラウドサービスのパスワードの管理方法のうち，本人以外の者による不正なログインの防止の観点から，適切なものはどれか。

ア　各従業員が指紋認証で保護されたスマートフォンをもち，スマートフォン上の信頼できるパスワード管理アプリケーションに各自のパスワードを記録する。

イ　各従業員が複雑で推測が難しいパスワードを一つ定め，どのクラウドサービスでも，そのパスワードを設定する。

ウ　パスワードを共用 PC の Web ブラウザに記憶させ，次回以降に自動入力されるように設定する。

エ　パスワードを平文のテキストファイル形式で記録し，共用 PC の OS のデスクトップに保存する。

問16　ワームの検知方式の一つとして，検査対象のファイルから SHA-256 を使ってハッシュ値を求め，既知のワーム検体ファイルのハッシュ値のデータベースと照合する方式がある。この方式によって，検知できるものはどれか。

ア　ワーム検体と同一のワーム
イ　ワーム検体と特徴あるコード列が同じワーム
ウ　ワーム検体とファイルサイズが同じワーム
エ　ワーム検体の亜種に該当するワーム

問17　A 社では，利用しているソフトウェア製品の脆弱性に対して，ベンダから提供された最新のセキュリティパッチを適用することを決定した。ソフトウェア製品がインストールされている組織内の PC やサーバについて，セキュリティパッチの適用漏れを防ぎたい。そのために有効なものはどれか。

ア　ソフトウェア製品の脆弱性の概要や対策の情報が蓄積された脆弱性対策情報データベース（JVN iPedia）
イ　ソフトウェア製品の脆弱性の特性や深刻度を評価するための基準を提供する共通脆弱性評価システム（CVSS）
ウ　ソフトウェア製品のソースコードを保存し，ソースコードへのアクセス権と変更履歴を管理するソースコード管理システム
エ　ソフトウェア製品の名称やバージョン，それらが導入されている機器の所在，IP アドレスを管理する IT 資産管理システム

問18　社内ネットワークとインターネットの接続点に，ステートフルインスペクション機能をもたない，静的なパケットフィルタリング型のファイアウォールを設置している。このネットワーク構成において，社内の PC からインターネット上の SMTP サーバに電子メールを送信できるようにするとき，ファイアウォールで通過を許可する TCP パケットのポート番号の組合せはどれか。ここで，SMTP 通信には，デフォルトのポート番号を使うものとする。

	送信元	宛先	送信元 ポート番号	宛先 ポート番号
ア	PC	SMTP サーバ	25	1024 以上
	SMTP サーバ	PC	1024 以上	25
イ	PC	SMTP サーバ	110	1024 以上
	SMTP サーバ	PC	1024 以上	110
ウ	PC	SMTP サーバ	1024 以上	25
	SMTP サーバ	PC	25	1024 以上
エ	PC	SMTP サーバ	1024 以上	110
	SMTP サーバ	PC	110	1024 以上

問19　内閣は，2015 年 9 月にサイバーセキュリティ戦略を定め，その目的達成のための施策の立案及び実施に当たって，五つの基本原則に従うべきとした。その基本原則に含まれるものはどれか。

ア　サイバー空間が一部の主体に占有されることがあってはならず，常に参加を求める者に開かれたものでなければならない。

イ　サイバー空間上の脅威は，国を挙げて対処すべき課題であり，サイバー空間における秩序維持は国家が全て代替することが適切である。

ウ　サイバー空間においては，安全確保のために，発信された情報を全て検閲すべきである。

エ　サイバー空間においては，情報の自由な流通を尊重し，法令を含むルールや規範を適用してはならない。

問20　ドメイン名ハイジャックを可能にする手口はどれか。

ア　PC と Web サーバとの通信を途中で乗っ取り，不正にデータを窃取する。

イ　Web サーバに，送信元を偽装したリクエストを大量に送信して，Web サービスを停止させる。

ウ　Web ページにアクセスする際の URL に余分なドットやスラッシュなどを含め，アクセスが禁止されているディレクトリにアクセスする。

エ　権威 DNS サーバに登録された情報を不正に書き換える。

問21　ドライブバイダウンロード攻撃に該当するものはどれか。

ア　PC 内のマルウェアを遠隔操作して，PC のハードディスクドライブを丸ごと暗号化する。

イ　外部ネットワークからファイアウォールの設定の誤りを突いて侵入し，内部ネットワークにあるサーバのシステムドライブにルートキットを仕掛ける。

ウ　公開 Web サイトにおいて，スクリプトを Web ページ中の入力フィールドに入力し，Web サーバがアクセスするデータベース内のデータを不正にダウンロードする。

エ　利用者が公開 Web サイトを閲覧したときに，その利用者の意図にかかわらず，PC にマルウェアをダウンロードさせて感染させる。

問22　バイオメトリクス認証システムの判定しきい値を変化させるとき，FRR（本人拒否率）と FAR（他人受入率）との関係はどれか。

ア　FRR と FAR は独立している。

イ　FRR を減少させると，FAR は減少する。

ウ　FRR を減少させると，FAR は増大する。

エ　FRR を増大させると，FAR は増大する。

問23　マルウェアの動的解析に該当するものはどれか。

ア　解析対象となる検体のハッシュ値を計算し，オンラインデータベースに登録された既知のマルウェアのハッシュ値のリストと照合してマルウェアを特定する。

イ　サンドボックス上で検体を実行し，その動作や外部との通信を観測する。

ウ　ネットワーク上の通信データから検体を抽出し，さらに，逆コンパイルして取得したコードから検体の機能を調べる。

エ　ハードディスク内のファイルの拡張子とファイルヘッダの内容を基に，拡張子が偽装された不正なプログラムファイルを検出する。

問24　メッセージが改ざんされていないかどうかを確認するために，そのメッセージから，ブロック暗号を用いて生成することができるものはどれか。

ア　PKI　　イ　パリティビット

ウ　メッセージ認証符号　　エ　ルート証明書

問25　リスクベース認証に該当するものはどれか。

ア　インターネットからの全てのアクセスに対し，トークンで生成されたワンタイムパスワードを入力させて認証する。

イ　インターネットバンキングでの連続する取引において，取引の都度，乱数表の指定したマス目にある英数字を入力させて認証する。

ウ　利用者の IP アドレスなどの環境を分析し，いつもと異なるネットワークからのアクセスに対して追加の認証を行う。

エ　利用者の記憶，持ち物，身体の特徴のうち，必ず二つ以上の方式を組み合わせて認証する。

問26　暗号アルゴリズムの危殆化を説明したものはどれか。

ア　外国の輸出規制によって，十分な強度をもつ暗号アルゴリズムを実装した製品が利用できなくなること

イ　鍵の不適切な管理によって，鍵が漏えいする危険性が増すこと

ウ　計算能力の向上などによって，鍵の推定が可能になり，暗号の安全性が低下すること

エ　最高性能のコンピュータを用い，膨大な時間とコストを掛けて暗号強度をより確実なものにすること

問27　暗号解読の手法のうち，ブルートフォース攻撃はどれか。

ア　与えられた１組の平文と暗号文に対し，総当たりで鍵を割り出す。

イ　暗号化関数の統計的な偏りを線形関数によって近似して解読する。

ウ　暗号化装置の動作を電磁波から解析することによって解読する。

エ　異なる二つの平文とそれぞれの暗号文の差分を観測して鍵を割り出す。

問28　電子メールの本文を暗号化するために使用される方式はどれか。

ア　BASE64　　イ　GZIP　　ウ　PNG　　エ　S/MIME

問29　ディジタル証明書をもつ A 氏が，B 商店に対して電子メールを使って商品を注文するときに，A 氏は自分の秘密鍵を用いてディジタル署名を行い，B 商店は A 氏の公開鍵を用いて署名を確認する。この手法によって実現できることはどれか。ここで，A 氏の秘密鍵は A 氏だけが使用できるものとする。

ア　A 氏から B 商店に送られた注文の内容が，第三者に漏れないようにできる。
イ　A 氏から発信された注文が，B 商店に届くようにできる。
ウ　B 商店から A 氏への商品販売が許可されていることを確認できる。
エ　B 商店に届いた注文が，A 氏からの注文であることを確認できる。

問30　PKI（公開鍵基盤）において，認証局が果たす役割の一つはどれか。

ア　共通鍵を生成する。
イ　公開鍵を利用してデータを暗号化する。
ウ　失効したディジタル証明書の一覧を発行する。
エ　データが改ざんされていないことを検証する。

問31　サイバーセキュリティ基本法の説明はどれか。

ア　国民は，サイバーセキュリティの重要性に関する関心と理解を深め，その確保に必要な注意を払うよう努めるものとすると規定している。
イ　サイバーセキュリティに関する国及び情報通信事業者の責務を定めたものであり，地方公共団体や教育研究機関についての言及はない。
ウ　サイバーセキュリティに関する国及び地方公共団体の責務を定めたものであり，民間事業者が努力すべき事項についての規定はない。
エ　地方公共団体を“重要社会基盤事業者”と位置づけ，サイバーセキュリティ関連施策の立案・実施に責任を負う者であると規定している。

問32　記憶媒体を介して，企業で使用されているコンピュータにマルウェアを侵入させ，そのコンピュータの記憶内容を消去した者を処罰の対象とする法律はどれか。

ア　刑法　　イ　製造物責任法
ウ　不正アクセス禁止法　　エ　プロバイダ責任制限法

問33　個人情報保護委員会“個人情報の保護に関する法律についてのガイドライン（通則編）平成29年3月一部改正”に，要配慮個人情報として例示されているものはどれか。

ア　医療従事者が診療の過程で知り得た診療記録などの情報
イ　国籍や外国人であるという法的地位の情報
ウ　宗教に関する書籍の購買や貸出しに係る情報
エ　他人を被疑者とする犯罪捜査のために取調べを受けた事実

問34　A社が著作権を保有しているプログラムで実現している機能と，B社のプログラムが同じ機能をもつとき，A社に対するB社の著作権侵害に関する記述のうち，適切なものはどれか。

ア　A社のソースコードを無断で使用して，同じソースコードの記述で機能を実現しても，A社公表後1年未満にB社がプログラムを公表すれば，著作権侵害とならない。
イ　A社のソースコードを無断で使用して，同じソースコードの記述で機能を実現しても，プログラム名称を別名称にすれば，著作権侵害とならない。
ウ　A社のソースコードを無断で使用していると，著作権の存続期間内は，著作権侵害となる。
エ　同じ機能を実現しているのであれば，ソースコードの記述によらず，著作権侵害となる。

問35　不正競争防止法で禁止されている行為はどれか。

ア　競争相手に対抗するために，特定商品の小売価格を安価に設定する。
イ　自社製品を扱っている小売業者に，指定した小売価格で販売するよう指示する。
ウ　他社のヒット商品と商品名や形状は異なるが同等の機能をもつ商品を販売する。
エ　広く知られた他人の商品の表示に，自社の商品の表示を類似させ，他人の商品と誤認させて商品を販売する。

問36　労働者派遣法に照らして，派遣先の対応として，適切なものはどれか。ここで，派遣労働者は期間制限の例外に当たらないものとする。

ア　業務に密接に関連した教育訓練を，同じ業務を行う派遣先の正社員と派遣労働者がいる職場で，正社員だけに実施した。
イ　工場で 3 年間働いていた派遣労働者を，今年から派遣を受け入れ始めた本社で正社員として受け入れた。
ウ　事業環境に特に変化がなかったので，特段の対応をせず，同一工場内において派遣労働者を 4 年間継続して受け入れた。
エ　ソフトウェア開発業務なので，派遣契約では特に期間制限を設けないルールとした。

問37　複数のシステム間でのデータ連携において，送信側システムで集計した送信データの件数の合計と，受信側システムで集計した受信データの件数の合計を照合して確認するためのコントロールはどれか。

ア　アクセスコントロール　　イ　エディットバリデーションチェック
ウ　コントロールトータルチェック　　エ　チェックデジット

問38　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）に準拠してISMSを運用している場合，内部監査について順守すべき要求事項はどれか。

ア　監査員にはISMS認証機関が認定する研修の修了者を含まなければならない。
イ　監査責任者は代表取締役が任命しなければならない。
ウ　監査範囲はJIS Q 27001に規定された管理策に限定しなければならない。
エ　監査プログラムは前回までの監査結果を考慮しなければならない。

問39　システム監査において，監査証拠となるものはどれか。

ア　システム監査チームが監査意見を取りまとめるためのミーティングの議事録
イ　システム監査チームが監査報告書に記載した指摘事項
ウ　システム監査チームが作成した個別監査計画書
エ　システム監査チームが被監査部門から入手したシステム運用記録

問40　システム監査実施における被監査部門の行為として，適切なものはどれか。

ア　監査部門から提出を要求された証憑（ひょう）の中で存在しないものがあれば，過去に遡って作成する。
イ　監査部門から要求されたアンケート調査に回答し，監査の実施に先立って監査部門に送付する。
ウ　システム監査で調査すべき監査項目を自ら整理してチェックリストを作成し，それに基づく監査の実施を依頼する。
エ　被監査部門の情報システムが抱えている問題を基にして，自ら監査テーマを設定する。

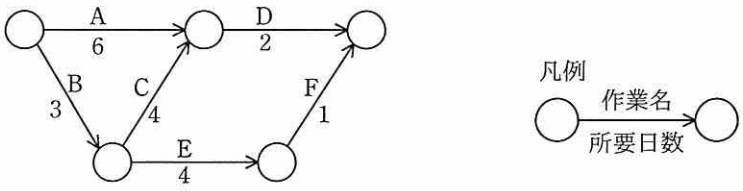
問41　事業継続計画（BCP）について監査を実施した結果，適切な状況と判断されるものはどれか。

ア　従業員の緊急連絡先リストを作成し，最新版に更新している。
イ　重要書類は複製せずに1か所で集中保管している。
ウ　全ての業務について，優先順位なしに同一水準のBCPを策定している。
エ　平時にはBCPを従業員に非公開としている。

問42　サービスデスク組織の構造とその特徴のうち，ローカルサービスデスクのものはどれか。

ア　サービスデスクを1拠点又は少数の場所に集中することによって，サービス要員を効率的に配置したり，大量のコールに対応したりすることができる。
イ　サービスデスクを利用者の近くに配置することによって，言語や文化が異なる利用者への対応，専門要員によるVIP対応などができる。
ウ　サービス要員が複数の地域や部門に分散していても，通信技術の利用によって単一のサービスデスクであるかのようにサービスが提供できる。
エ　分散拠点のサービス要員を含めた全員を中央で統括して管理することによって，統制のとれたサービスが提供できる。

問43　図のアローダイアグラムにおいて，プロジェクト全体の期間を短縮するために，作業 A ～ E の幾つかを 1 日ずつ短縮する。プロジェクト全体の期間を 2 日短縮できる作業の組みはどれか。



ア　A，C，E　　イ　A，D　　ウ　B，C，E　　エ　B，D

問44　磁気ディスクの耐障害性に関する説明のうち，RAID 5 に該当するものはどれか。

ア　最低でも 3 台の磁気ディスクが必要となるが，いずれか 1 台の磁気ディスクが故障しても全データを復旧することができる。

イ　最低でも 4 台の磁気ディスクが必要となるが，いずれか 2 台の磁気ディスクが故障しても全データを復旧することができる。

ウ　複数台の磁気ディスクに同じデータを書き込むので，いずれか 1 台の磁気ディスクが故障しても影響しない。

エ　複数台の磁気ディスクにデータを分散して書き込むので，磁気ディスクのいずれか 1 台が故障すると全データを復旧できない。

問45　PaaS 型サービスモデルの特徴はどれか。

ア　利用者は，サービスとして提供される OS やストレージに対する設定や変更をして利用することができるが，クラウドサービス基盤を変更したり拡張したりすることはできない。

イ　利用者は，サービスとして提供される OS やデータベースシステム，プログラム言語処理系などを組み合わせて利用することができる。

ウ　利用者は，サービスとして提供されるアプリケーションを利用することができるが，自らアプリケーションを開発することはできない。

エ　利用者は，ネットワークを介してサービスとして提供される端末のデスクトップ環境を利用することができる。

問46　DBMS において，複数のトランザクション処理プログラムが同一データベースを同時に更新する場合，論理的な矛盾を生じさせないために用いる技法はどれか。

ア　再編成　　イ　正規化

ウ　整合性制約　　エ　排他制御

問47　電子メールのヘッダフィールドのうち，SMTP でメッセージが転送される過程で削除されるものはどれか。

ア　Bcc　　イ　Date　　ウ　Received　　エ　X-Mailer

問48　IT アウトソーシングの活用に当たって，委託先決定までの計画工程，委託先決定からサービス利用開始までの準備工程，委託先が提供するサービスを発注者が利用する活用工程の三つに分けたとき，発注者が活用工程で行うことはどれか。

ア　移行計画やサービス利用におけるコミュニケーションプランを委託先と決定する。

イ　移行ツールのテストやサービス利用テストなど，一連のテストを委託先と行う。

ウ　稼働状況を基にした実績報告や利用者評価を基に，改善案を委託先と取りまとめる。

エ　提案依頼書を作成，提示して委託候補先から提案を受ける。

問49　CSR 調達に該当するものはどれか。

ア　コストを最小化するために，最も安価な製品を選ぶ。

イ　災害時に調達が不可能となる事態を避けるために，複数の調達先を確保する。

ウ　自然環境，人権などへの配慮を調達基準として示し，調達先に遵守を求める。

エ　物品の購買に当たって EDI を利用し，迅速かつ正確な調達を行う。

問50　製造原価明細書から損益計算書を作成したとき，売上総利益は何千円か。

単位　千円

製造原価明細書

材料費	400
労務費	300
経　費	200
当期総製造費用	□
期首仕掛品棚卸高	150
期末仕掛品棚卸高	250
当期製品製造原価	□

単位　千円

損益計算書

売上高	1,000
売上原価	
期首製品棚卸高	120
当期製品製造原価	□
期末製品棚卸高	70
売上原価	□
売上総利益	□

ア　150　　イ　200　　ウ　310　　エ　450

〔 メ モ 用 紙 〕

〔 メ モ 用 紙 〕

〔 メ モ 用 紙 〕

6. 退室可能時間に途中で退室する場合には，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。