SG

令和元年度　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　BEC（Business E-mail Compromise）に該当するものはどれか。

ア　巧妙なだましの手口を駆使し，取引先になりすまして偽の電子メールを送り，金銭をだまし取る。

イ　送信元を攻撃対象の組織のメールアドレスに詐称し，多数の実在しないメールアドレスに一度に大量の電子メールを送り，攻撃対象の組織のメールアドレスを故意にブラックリストに登録させて，利用を阻害する。

ウ　第三者からの電子メールが中継できるように設定されたメールサーバを，スパムメールの中継に悪用する。

エ　誹謗（ひぼう）中傷メールの送信元を攻撃対象の組織のメールアドレスに詐称し，組織の社会的な信用を大きく損なわせる。

問２　参加組織及びそのグループ企業において検知されたサイバー攻撃などの情報を，IPA が情報ハブになって集約し，参加組織間で共有する取組はどれか。

ア　CRYPTREC　　イ　CSIRT

ウ　J-CSIP　　エ　JISEC

問３　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，リスクを受容するプロセスに求められるものはどれか。

ア　受容するリスクについては，リスク所有者が承認すること

イ　受容するリスクを監視やレビューの対象外とすること

ウ　リスクの受容は，リスク分析前に行うこと

エ　リスクを受容するかどうかは，リスク対応後に決定すること

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 27000:2019（情報セキュリティマネジメントシステム－用語）において，不適合が発生した場合にその原因を除去し，再発を防止するためのものとして定義されているものはどれか。

ア　継続的改善　　イ　修正

ウ　是正処置　　エ　リスクアセスメント

問6　ネットワークカメラなどのIoT機器ではTCP 23番ポートへの攻撃が多い理由はどれか。

ア　TCP 23番ポートはIoT機器の操作用プロトコルで使用されており，そのプロトコルを用いると，初期パスワードを使って不正ログインが容易に成功し，不正にIoT機器を操作できることが多いから

イ　TCP 23番ポートはIoT機器の操作用プロトコルで使用されており，そのプロトコルを用いると，マルウェアを添付した電子メールをIoT機器に送信するという攻撃ができることが多いから

ウ　TCP 23番ポートはIoT機器へのメール送信用プロトコルで使用されており，そのプロトコルを用いると，初期パスワードを使って不正ログインが容易に成功し，不正にIoT機器を操作できることが多いから

エ　TCP 23番ポートはIoT機器へのメール送信用プロトコルで使用されており，そのプロトコルを用いると，マルウェアを添付した電子メールをIoT機器に送信するという攻撃ができることが多いから

問7　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，送信元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，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。

エ　電子メールを送信するサーバが，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。

問８　A 社では現在，インターネット上の Web サイトを内部ネットワークの PC 上の Web ブラウザから参照している。新たなシステムを導入し，DMZ 上に用意した VDI（Virtual Desktop Infrastructure）サーバに PC からログインし，インターネット上の Web サイトを VDI サーバ上の仮想デスクトップの Web ブラウザから参照するように変更する。この変更によって期待できるセキュリティ上の効果はどれか。

ア　インターネット上の Web サイトから，内部ネットワークの PC へのマルウェアのダウンロードを防ぐ。

イ　インターネット上の Web サイト利用時に，MITB 攻撃による送信データの改ざんを防ぐ。

ウ　内部ネットワークの PC 及び仮想デスクトップの OS がボットに感染しなくなり，C&C サーバにコントロールされることを防ぐ。

エ　内部ネットワークの PC にマルウェアが侵入したとしても，他の PC に感染するのを防ぐ。

問９　JIS Q 27002:2014 には記載されていないが，JIS Q 27017:2016 において記載されている管理策はどれか。

ア　クラウドサービス固有の情報セキュリティ管理策

イ　事業継続マネジメントシステムにおける管理策

ウ　情報セキュリティガバナンスにおける管理策

エ　制御システム固有のサイバーセキュリティ管理策

問10　シャドーITに該当するものはどれか。

ア　IT製品やITを活用して地球環境への負荷を低減する取組

イ　IT 部門の許可を得ずに，従業員又は部門が業務に利用しているデバイスやクラウドサービス

ウ　攻撃対象者のディスプレイやキータイプを物陰から盗み見て，情報を盗み出す行為

エ　ネットワーク上のコンピュータに侵入する準備として，侵入対象の弱点を探るために組織や所属する従業員の情報を収集すること

問11　ステガノグラフィはどれか。

ア　画像などのデータの中に，秘密にしたい情報を他者に気付かれることなく埋め込む。

イ　検索エンジンの巡回ロボットに Web ページの閲覧者とは異なる内容を応答し，該当 Web ページの検索順位が上位に来るようにする。

ウ　検査対象の製品に，問題を引き起こしそうな JPEG 画像などのテストデータを送信し読み込ませて，製品の応答や挙動から脆弱性を検出する。

エ　コンピュータには認識できないほどゆがんだ文字を画像として表示し，利用者に文字を認識させて入力させることによって，利用者が人であることを確認する。

問12　セキュアハッシュ関数 SHA-256 を用いてファイル A 及びファイル B のハッシュ値を算出すると，どちらも全く同じ次に示すハッシュ値 n（16 進数で示すと 64 桁）となった。この結果から考えられることとして，適切なものはどれか。

ハッシュ値 n：86620f2f 152524d7 dbed4bcb b8119bb6 d493f734 0b4e7661 88565353 9e6d2074

ア　ファイル A とファイル B の各内容を変更せずに再度ハッシュ値を算出すると，ファイル A とファイル B のハッシュ値が異なる。

イ　ファイル A とファイル B のハッシュ値 n のデータ量は 64 バイトである。

ウ　ファイル A とファイル B を連結させたファイル C のハッシュ値の桁数は 16 進数で示すと 128 桁である。

エ　ファイル A の内容とファイル B の内容は同じである。

問13　インターネットバンキングでの MITB 攻撃による不正送金について，対策として用いられるトランザクション署名の説明はどれか。

ア　携帯端末からの送金取引の場合，金融機関から携帯端末の登録メールアドレスに送金用のワンタイムパスワードを送信する。

イ　特定認証業務の認定を受けた認証局が署名したディジタル証明書をインターネットバンキングでの利用者認証に用いることによって，ログインパスワードが漏えいした際の不正ログインを防止する。

ウ　利用者が送金取引時に，送金処理を行う PC とは別のデバイスに振込先口座番号などの取引情報を入力して表示された値をインターネットバンキングに送信する。

エ　ログイン時に，送金処理を行う PC とは別のデバイスによって，一定時間だけ有効なログイン用のワンタイムパスワードを算出し，インターネットバンキングに送信する。

問14　WAF におけるフォールスポジティブに該当するものはどれか。

ア　HTML の特殊文字“<”を検出したときに通信を遮断するように WAF を設定した場合，“<”などの数式を含んだ正当な HTTP リクエストが送信されたとき，WAF が攻撃として検知し，遮断する。

イ　HTTP リクエストのうち，RFC などに仕様が明確に定義されておらず，Web アプリケーションソフトウェアの開発者が独自の仕様で追加したフィールドについては WAF が検査しないという仕様を悪用して，攻撃の命令を埋め込んだ HTTP リクエストが送信されたとき，WAF が遮断しない。

ウ　HTTP リクエストのパラメタとして許可する文字列以外を検出したときに通信を遮断するように WAF を設定した場合，許可しない文字列を含んだ不正な HTTP リクエストが送信されたとき，WAF が攻撃として検知し，遮断する。

エ　悪意のある通信を正常な通信と見せかけ，HTTP リクエストを分割して送信されたとき，WAF が遮断しない。

問15　ボットネットにおいて C&C サーバが担う役割はどれか。

ア　遠隔操作が可能なマルウェアに，情報収集及び攻撃活動を指示する。

イ　攻撃の踏み台となった複数のサーバからの通信を制御して遮断する。

ウ　電子商取引事業者などに，偽のディジタル証明書の発行を命令する。

エ　不正な Web コンテンツのテキスト，画像及びレイアウト情報を一元的に管理する。

問16　攻撃者が用意したサーバ X の IP アドレスが，A 社 Web サーバの FQDN に対応する IP アドレスとして，B 社 DNS キャッシュサーバに記憶された。これによって，意図せずサーバ X に誘導されてしまう利用者はどれか。ここで，A 社，B 社の各従業員は自社の DNS キャッシュサーバを利用して名前解決を行う。

ア　A 社 Web サーバにアクセスしようとする A 社従業員
イ　A 社 Web サーバにアクセスしようとする B 社従業員
ウ　B 社 Web サーバにアクセスしようとする A 社従業員
エ　B 社 Web サーバにアクセスしようとする B 社従業員

問17　PC とサーバとの間で IPsec による暗号化通信を行う。通信データの暗号化アルゴリズムとして AES を使うとき，用いるべき鍵はどれか。

ア　PC だけが所有する秘密鍵
イ　PC とサーバで共有された共通鍵
ウ　PC の公開鍵
エ　サーバの公開鍵

問18　WPA3 はどれか。

ア　HTTP 通信の暗号化規格
イ　TCP/IP 通信の暗号化規格
ウ　Web サーバで使用するディジタル証明書の規格
エ　無線 LAN のセキュリティ規格

問19　リバースブルートフォース攻撃に該当するものはどれか。

ア　攻撃者が何らかの方法で事前に入手した利用者 ID とパスワードの組みのリストを使用して，ログインを試行する。

イ　パスワードを一つ選び，利用者 ID として次々に文字列を用意して総当たりにログインを試行する。

ウ　利用者 ID，及びその利用者 ID と同一の文字列であるパスワードの組みを次々に生成してログインを試行する。

エ　利用者 ID を一つ選び，パスワードとして次々に文字列を用意して総当たりにログインを試行する。

問20　ディジタル署名に用いる鍵の組みのうち，適切なものはどれか。

	ディジタル署名の作成に用いる鍵	ディジタル署名の検証に用いる鍵
ア	共通鍵	秘密鍵
イ	公開鍵	秘密鍵
ウ	秘密鍵	共通鍵
エ	秘密鍵	公開鍵

問21　情報セキュリティにおいてバックドアに該当するものはどれか。

ア　アクセスする際にパスワード認証などの正規の手続が必要な Web サイトに，当該手続を経ないでアクセス可能な URL

イ　インターネットに公開されているサーバの TCP ポートの中からアクティブになっているポートを探して，稼働中のサービスを特定するためのツール

ウ　ネットワーク上の通信パケットを取得して通信内容を見るために設けられたスイッチの LAN ポート

エ　プログラムが確保するメモリ領域に，領域の大きさを超える長さの文字列を入力してあふれさせ，ダウンさせる攻撃

問22　マルウェアの動的解析に該当するものはどれか。

ア　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　検体をサンドボックス上で実行し，その動作や外部との通信を観測する。

ウ　検体をネットワーク上の通信データから抽出し，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23　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24　リスクベース認証に該当するものはどれか。

ア　インターネットバンキングでの取引において，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。

イ　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。

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25　攻撃者が，多数のオープンリゾルバに対して，“あるドメイン”の実在しないランダムなサブドメインを多数問い合わせる攻撃（ランダムサブドメイン攻撃）を仕掛け，多数のオープンリゾルバが応答した。このときに発生する事象はどれか。

ア　“あるドメイン”を管理する権威 DNS サーバに対して負荷が掛かる。

イ　“あるドメイン”を管理する権威 DNS サーバに登録されている DNS 情報が改ざんされる。

ウ　オープンリゾルバが保持する DNS キャッシュに不正な値を注入される。

エ　オープンリゾルバが保持するゾーン情報を不正に入手される。

問26　手順に示す電子メールの送受信によって得られるセキュリティ上の効果はどれか。

〔手順〕

(1) 送信者は，電子メールの本文を共通鍵暗号方式で暗号化し（暗号文），その共通鍵を受信者の公開鍵を用いて公開鍵暗号方式で暗号化する（共通鍵の暗号化データ）。

(2) 送信者は，暗号文と共通鍵の暗号化データを電子メールで送信する。

(3) 受信者は，受信した電子メールから取り出した共通鍵の暗号化データを，自分の秘密鍵を用いて公開鍵暗号方式で復号し，得た共通鍵で暗号文を復号する。

ア　送信者による電子メールの送達確認

イ　送信者のなりすましの検出

ウ　電子メールの本文の改ざん箇所の修正

エ　電子メールの本文の内容の漏えいの防止

問27　クレジットカードなどのカード会員データのセキュリティ強化を目的として制定され，技術面及び運用面の要件を定めたものはどれか。

ア　ISMS 適合性評価制度　　イ　PCI DSS

ウ　特定個人情報保護評価　　エ　プライバシーマーク制度

問28　電子メールをドメイン A の送信者がドメイン B の宛先に送信するとき，送信者をドメイン A のメールサーバで認証するためのものはどれか。

ア　APOP　　イ　POP3S　　ウ　S/MIME　　エ　SMTP-AUTH

問29　ハニーポットの説明はどれか。

ア　サーバやネットワークを実際の攻撃に近い手法で検査することによって，もし実際に攻撃があった場合の被害の範囲を予測する。

イ　社内ネットワークに接続しようとする PC を，事前に検査専用のネットワークに接続させ，セキュリティ状態を検査することによって，安全ではない PC の接続を防ぐ。

ウ　保護された領域で，検査対象のプログラムを動作させることによって，その挙動からマルウェアを検出して，隔離及び駆除を行う。

エ　わざと侵入しやすいように設定した機器やシステムをインターネット上に配置することによって，攻撃手法やマルウェアの振る舞いなどの調査と研究に利用する。

問30　Web サーバの検査におけるポートスキャナの利用目的はどれか。

ア　Web サーバで稼働しているサービスを列挙して，不要なサービスが稼働していないことを確認する。

イ　Web サーバの利用者 ID の管理状況を運用者に確認して，情報セキュリティポリシからの逸脱がないことを調べる。

ウ　Web サーバへのアクセスの履歴を解析して，不正利用を検出する。

エ　正規の利用者 ID でログインし，Web サーバのコンテンツを直接確認して，コンテンツの脆弱性を検出する。

問31　企業において業務で使用されているコンピュータに，記憶媒体を介してマルウェアを侵入させ，そのコンピュータのデータを消去した者がいたとき，その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32　技術者の活動に関係する法律のうち，罰則規定のないものはどれか。

ア　公益通報者保護法　　イ　個人情報保護法
ウ　特許法　　エ　不正競争防止法

問33　シュリンクラップ契約において，ソフトウェアの使用許諾契約が成立するのはどの時点か。

ア　購入したソフトウェアの代金を支払った時点
イ　ソフトウェアの入った DVD-ROM を受け取った時点
ウ　ソフトウェアの入った DVD-ROM の包装を解いた時点
エ　ソフトウェアを PC にインストールした時点

問34　A 社は，B 社と著作物の権利に関する特段の取決めをせず，A 社の要求仕様に基づいて，販売管理システムのプログラム作成を B 社に委託した。この場合のプログラム著作権の原始的帰属に関する記述のうち，適切なものはどれか。

ア　A 社と B 社が話し合って帰属先を決定する。
イ　A 社と B 社の共有帰属となる。
ウ　A 社に帰属する。
エ　B 社に帰属する。

問35　A 社は，A 社で使うソフトウェアの開発作業を B 社に実施させる契約を，B 社と締結した。締結した契約が労働者派遣であるものはどれか。

ア　A 社監督者が，B 社の雇用する労働者に，業務遂行に関する指示を行い，A 社の開発作業を行わせる。
イ　B 社監督者が，B 社の雇用する労働者に指示を行って成果物を完成させ，A 社監督者が成果物の検収作業を行う。
ウ　B 社の雇用する労働者が，A 社の依頼に基づいて，B 社指示の下で B 社所有の機材・設備を使用し，開発作業を行う。
エ　B 社の雇用する労働者が，B 社監督者の業務遂行に関する指示の下，A 社施設内で開発作業を行う。

問36　常時 10 名以上の従業員を有するソフトウェア開発会社が，社内の情報セキュリティ管理を強化するために，秘密情報を扱う担当従業員の扱いを見直すこととした。労働法に照らし，適切な行為はどれか。

ア　就業規則に業務上知り得た秘密の漏えい禁止の一般的な規定があるときに，担当従業員の職務に即して秘密の内容を特定する個別合意を行う。

イ　就業規則には業務上知り得た秘密の漏えい禁止の規定がないときに，漏えい禁止と処分の規定を従業員の意見を聴かずに就業規則に追加する。

ウ　情報セキュリティ事故を起こした場合の処分について，担当従業員との間で，就業規則よりも処分の内容を重くした個別合意を行う。

エ　情報セキュリティに関連する規定は就業規則に記載してはいけないので，就業規則に規定を設けずに，各従業員と個別合意を行う。

問37　入出金管理システムから出力された入金データファイルを，売掛金管理システムが読み込んでマスタファイルを更新する。入出金管理システムから売掛金管理システムに受け渡されたデータの正確性及び網羅性を確保するコントロールはどれか。

ア　売掛金管理システムにおける入力データと出力結果とのランツーランコントロール

イ　売掛金管理システムのマスタファイル更新におけるタイムスタンプ機能

ウ　入金額及び入金データ件数のコントロールトータルのチェック

エ　入出金管理システムへの入力のエディットバリデーションチェック

問38　金融庁“財務報告に係る内部統制の評価及び監査の基準（平成 23 年）”に基づいて，内部統制の基本的要素を，統制環境，リスクの評価と対応，統制活動，情報と伝達，モニタリング，IT への対応の六つに分類したときに，統制活動に該当するものはどれか。

ア　経営者が自らの意思としての経営方針を全社的に明示していること
イ　情報システムの故障・不具合に備えて保険契約に加入しておくこと
ウ　内部監査部門が定期的に業務監査を実施すること
エ　発注業務と検収業務をそれぞれ別の者に担当させること

問39　データの生成から入力，処理，出力，活用までのプロセス，及び組み込まれているコントロールを，システム監査人が書面上で又は実際に追跡する技法はどれか。

ア　インタビュー法　　イ　ウォークスルー法
ウ　監査モジュール法　　エ　ペネトレーションテスト法

問40　アクセス制御を監査するシステム監査人の行為のうち，適切なものはどれか。

ア　ソフトウェアに関するアクセス制御の管理台帳を作成し，保管した。
イ　データに関するアクセス制御の管理規程を閲覧した。
ウ　ネットワークに関するアクセス制御の管理方針を制定した。
エ　ハードウェアに関するアクセス制御の運用手続を実施した。

問41　IT サービスマネジメントにおいて，“サービスに対する計画外の中断”，“サービスの品質の低下”，又は“顧客へのサービスにまだ影響していない事象”を何というか。

ア　インシデント　　イ　既知の誤り
ウ　変更要求　　エ　問題

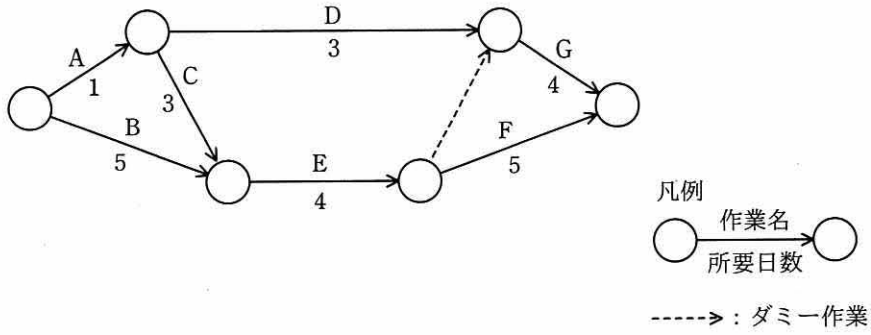
問42　ヒューマンエラーに起因する障害を発生しにくくする方法に，エラープルーフ化がある。運用作業におけるエラープルーフ化の例として，最も適切なものはどれか。

ア　画面上の複数のウィンドウを同時に使用する作業では，ウィンドウを間違えないようにウィンドウの背景色をそれぞれ異なる色にする。
イ　長時間に及ぶシステム監視作業では，疲労が蓄積しないように，2 時間おきに交代で休憩を取得する体制にする。
ウ　ミスが発生しやすい作業について，過去に発生したヒヤリハット情報を共有して同じミスを起こさないようにする。
エ　臨時の作業を行う際にも落ち着いて作業ができるように，臨時の作業の教育や訓練を定期的に行う。

問43　プロジェクトライフサイクルの一般的な特性はどれか。

ア　開発要員数は，プロジェクト開始時が最多であり，プロジェクトが進むにつれて減少し，完了に近づくと再度増加する。
イ　ステークホルダがコストを変えずにプロジェクトの成果物に対して及ぼすことができる影響の度合いは，プロジェクト完了直前が最も大きくなる。
ウ　プロジェクトが完了に近づくほど，変更やエラーの修正がプロジェクトに影響する度合いは小さくなる。
エ　リスクは，プロジェクトが完了に近づくにつれて減少する。

問44　あるプロジェクトの日程計画をアローダイアグラムで示す。クリティカルパスはどれか。



ア　A, C, E, F　　イ　A, D, G

ウ　B, E, F　　エ　B, E, G

問45　Web システムの性能指標のうち，応答時間の説明はどれか。

ア　Web ブラウザに表示された問合せボタンが押されてから，Web ブラウザが結果を表示し始めるまでの時間

イ　Web ブラウザを起動してから，最初に表示するようにあらかじめ設定した Web ページの全てのデータ表示が完了するまでの時間

ウ　サーバ側のトランザクション処理が完了してから，Web ブラウザが結果を表示し始めるまでの時間

エ　ダウンロードを要求してから，ダウンロードが完了するまでの時間

問46　データベースのトランザクションに関する記述のうち，適切なものはどれか。

ア　他のトランザクションにデータを更新されないようにするために，テーブルに対するロックをアプリケーションプログラムが解放した。

イ　トランザクション障害が発生したので，異常終了したトランザクションをDBMSがロールフォワードした。

ウ　トランザクションの更新結果を確定するために，トランザクションをアプリケーションプログラムがロールバックした。

エ　複数のトランザクション間でデッドロックが発生したので，トランザクションをDBMSがロールバックした。

問47　PCが，Webサーバ，メールサーバ，他のPCなどと通信を始める際に，通信相手のIPアドレスを問い合わせる仕組みはどれか。

ア　ARP（Address Resolution Protocol）

イ　DHCP（Dynamic Host Configuration Protocol）

ウ　DNS（Domain Name System）

エ　NAT（Network Address Translation）

問48　RPAを活用することによって業務の改善を図ったものはどれか。

ア　果物の出荷検査のために，画像解析によって大きさや形が規格外の果物をふるい落とす装置を導入し，検査速度を向上させた。

イ　事務職員が人手で行っていた定型的かつ大量のコピー&ペースト作業をソフトウェアによって自動化し，作業時間の短縮と作業精度の向上を実現させた。

ウ　倉庫での作業従事者にパワーアシストスーツを着用させ，身体の不調で病欠する従業員の割合を低減させた。

エ　ビッグデータを用いてあらかじめ解析した結果から，タクシーの需要が多いと見込まれる地域を日ごとに特定し，タクシーの空車の割合を低減させた。

問49　情報システムを取得するための提案依頼書（RFP）の作成と提案依頼に当たって，取得者であるユーザ企業側の対応のうち，適切なものはどれか。

ア　RFP 作成の手間を省くために，要求事項の記述は最小限にとどめる。曖昧な点や不完全な点があれば，供給者であるベンダ企業から取得者に都度確認させる。

イ　取得者であるユーザ企業側では，事前に実現性の確認を行わずに，要求事項が実現可能かどうかの調査や検討は供給者であるベンダ企業側に任せる。

ウ　複数の要求事項がある場合，重要な要求とそうでない要求の区別がつくようにRFP 作成時点で重要度を設定しておく。

エ　要求事項は機能を記述するのではなく，極力，具体的な製品名や実現手段を細かく指定する。

問50　アンケートの自由記述欄に記入された文章における単語の出現頻度などを分析する手法はどれか。

ア　アクセスログ分析　　イ　シックスシグマ

ウ　テキストマイニング　　エ　マーケットバスケット分析

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。