SC

# 平成27年度　秋期
# 情報セキュリティスペシャリスト試験
# 午前Ⅱ　問題

| 試験時間 | 10:50 ～ 11:30（40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。試験時間中は，退室できません。
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25 |
|---|---|
| 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〕　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。

## 問題文中で共通に使用される表記ルール

各問題文中に注記がない限り，次の表記ルールが適用されているものとする。

| 試験問題での表記 | 規格・標準の名称 |
|---|---|
| JIS Q 9001 | JIS Q 9001:2008 |
| JIS Q 14001 | JIS Q 14001:2004 |
| JIS Q 15001 | JIS Q 15001:2006 |
| JIS Q 20000-1 | JIS Q 20000-1:2012 |
| JIS Q 20000-2 | JIS Q 20000-2:2013 |
| JIS Q 27000 | JIS Q 27000:2014 |
| JIS Q 27001 | JIS Q 27001:2014 |
| JIS Q 27002 | JIS Q 27002:2014 |
| JIS X 0160 | JIS X 0160:2012 |
| ISO 21500 | ISO 21500:2012 |
| ITIL | ITIL 2011 edition |
| PMBOK | PMBOK ガイド 第5版 |
| 共通フレーム | 共通フレーム 2013 |

問1　AESの暗号化方式を説明したものはどれか。

ア　鍵長によって，段数が決まる。
イ　段数は，6回以内の範囲で選択できる。
ウ　データの暗号化，復号，暗号化の順に3回繰り返す。
エ　同一の公開鍵を用いて暗号化を3回繰り返す。

問2　特定の認証局が発行したCRLに関する記述のうち，適切なものはどれか。

ア　CRLには，失効したディジタル証明書に対応する秘密鍵が登録される。
イ　CRLには，有効期限内のディジタル証明書のうち失効したディジタル証明書と失効した日時の対応が提示される。
ウ　CRLは，鍵の漏えい，破棄申請の状況をリアルタイムに反映するプロトコルである。
エ　有効期限切れで失効したディジタル証明書は，所有者が新たなディジタル証明書を取得するまでの間，CRLに登録される。

問３　ステートフルインスペクション方式のファイアウォールの特徴はどれか。

ア　Web ブラウザと Web サーバとの間に配置され，リバースプロキシサーバとして動作する方式であり，Web ブラウザから Web サーバへの通信に不正なデータがないかどうかを検査する。

イ　アプリケーションプロトコルごとにプロキシプログラムを用意する方式であり，クライアントからの通信を目的のサーバに中継する際に，不正なデータがないかどうかを検査する。

ウ　特定のアプリケーションプロトコルだけを通過させるゲートウェイソフトウェアを利用する方式であり，クライアントからのコネクションの要求を受け付けて，目的のサーバに改めてコネクションを要求することによって，アクセスを制御する。

エ　パケットフィルタリングを拡張した方式であり，過去に通過したパケットから通信セッションを認識し，受け付けたパケットを通信セッションの状態に照らし合わせて通過させるか遮断させるかを判断する。

問４　PC などに内蔵されるセキュリティチップ（TPM：Trusted Platform Module）がもつ機能はどれか。

ア　TPM 間での共通鍵の交換　　イ　鍵ペアの生成

ウ　ディジタル証明書の発行　　エ　ネットワーク経由の乱数送信

問5　ポリモーフィック型ウイルスの説明として，適切なものはどれか。

ア　インターネットを介して，攻撃者がPCを遠隔操作する。

イ　感染するごとにウイルスのコードを異なる鍵で暗号化し，コード自身を変化させることによって，同一のパターンで検知されないようにする。

ウ　複数のOSで利用できるプログラム言語でウイルスを作成することによって，複数のOS上でウイルスが動作する。

エ　ルートキットを利用してウイルスに感染していないように見せかけることによって，ウイルスを隠蔽する。

問6　ISO/IEC 15408を評価基準とする“ITセキュリティ評価及び認証制度”の説明として，適切なものはどれか。

ア　暗号モジュールに暗号アルゴリズムが適切に実装され，暗号鍵などが確実に保護されているかどうかを評価及び認証する制度

イ　主に無線LANにおいて，RADIUSなどと連携することで，認証されていない利用者を全て排除し，認証された利用者だけの通信を通過させることを評価及び認証する制度

ウ　情報技術に関連した製品のセキュリティ機能の適切性，確実性を第三者機関が評価し，その結果を公的に認証する制度

エ　情報セキュリティマネジメントシステムが，基準にのっとり，適切に組織内に構築，運用されていることを評価及び認証する制度

問7　特定の情報資産の漏えいに関するリスク対応のうち，リスク回避に該当するものはどれか。

ア　外部の者が侵入できないように，入退室をより厳重に管理する。

イ　情報資産を外部のデータセンタに預託する。

ウ　情報の新たな収集を禁止し，収集済みの情報を消去する。

エ　情報の重要性と対策費用を勘案し，あえて対策をとらない。

問8　水飲み場型攻撃（Watering Hole Attack）の手口はどれか。

ア　アイコンを文書ファイルのものに偽装した上で，短いスクリプトを埋め込んだショートカットファイル（LNK ファイル）を電子メールに添付して標的組織の従業員に送信する。

イ　事務連絡などのやり取りを行うことで，標的組織の従業員の気を緩めさせ，信用させた後，攻撃コードを含む実行ファイルを電子メールに添付して送信する。

ウ　標的組織の従業員が頻繁にアクセスする Web サイトに攻撃コードを埋め込み，標的組織の従業員がアクセスしたときだけ攻撃が行われるようにする。

エ　ミニブログのメッセージにおいて，ドメイン名を短縮してリンク先の URL を分かりにくくすることによって，攻撃コードを埋め込んだ Web サイトに標的組織の従業員を誘導する。

問9　不正が発生する際には“不正のトライアングル”の 3 要素全てが存在すると考えられている。“不正のトライアングル”の構成要素の説明のうち，適切なものはどれか。

ア　“機会”とは，情報システムなどの技術や物理的な環境及び組織のルールなど，内部者による不正行為の実行を可能，又は容易にする環境の存在である。

イ　“情報と伝達”とは，必要な情報が識別，把握及び処理され，組織内外及び関係者相互に正しく伝えられるようにすることである。

ウ　“正当化”とは，ノルマによるプレッシャーなどのことである。

エ　“動機”とは，良心のかしゃくを乗り越える都合の良い解釈や他人への責任転嫁など，内部者が不正行為を自ら納得させるための自分勝手な理由付けである。

問10　ICMP Flood 攻撃に該当するものはどれか。

ア　HTTP GET コマンドを繰り返し送ることによって，攻撃対象のサーバにコンテンツ送信の負荷を掛ける。

イ　ping コマンドを用いて大量の要求パケットを発信することによって，攻撃対象のサーバに至るまでの回線を過負荷にしてアクセスを妨害する。

ウ　コネクション開始要求に当たる SYN パケットを大量に送ることによって，攻撃対象のサーバに，接続要求ごとに応答を返すための過大な負荷を掛ける。

エ　大量の TCP コネクションを確立することによって，攻撃対象のサーバに接続を維持させ続けてリソースを枯渇させる。

問11　VLAN機能をもった1台のレイヤ3スイッチに複数のPCを接続している。スイッチのポートをグループ化して複数のセグメントに分けると，セグメントを分けない場合に比べて，どのようなセキュリティ上の効果が得られるか。

ア　スイッチが，PCから送出されるICMPパケットを全て遮断するので，PC間のマルウェア感染のリスクを低減できる。

イ　スイッチが，PCからのブロードキャストパケットの到達範囲を制限するので，アドレス情報の不要な流出のリスクを低減できる。

ウ　スイッチが，PCのMACアドレスから接続可否を判別するので，PCの不正接続のリスクを低減できる。

エ　スイッチが，物理ポートごとに，決まったIPアドレスのPC接続だけを許可するので，PCの不正接続のリスクを低減できる。

問12　クロスサイトスクリプティングによる攻撃を防止する対策はどれか。

ア　WebサーバにSNMPエージェントを常駐稼働させ，Webサーバの負荷状態を監視する。

イ　Webサーバの OS のセキュリティパッチについて，常に最新のものを適用する。

ウ　Webサイトへのデータ入力について，許容範囲を超えた大きさのデータの書込みを禁止する。

エ　Webサイトへの入力データを表示するときに，HTMLで特別な意味をもつ文字のエスケープ処理を行う。

問13　Web サーバが HTTPS 通信の応答で Cookie に Secure 属性を設定したときのブラウザの処理はどれか。

ア　ブラウザは，Cookie の“Secure=”に続いて指定された時間を参照し，指定された時間を過ぎている場合にその Cookie を削除する。

イ　ブラウザは，Cookie の“Secure=”に続いて指定されたホスト名を参照し，指定されたホストにその Cookie を送信する。

ウ　ブラウザは，Cookie の“Secure”を参照し，HTTPS 通信時だけその Cookie を送信する。

エ　ブラウザは，Cookie の“Secure”を参照し，ブラウザの終了時にその Cookie を削除する。

問14　テンペスト（TEMPEST）攻撃を説明したものはどれか。

ア　故意に暗号化演算を誤動作させて正しい処理結果との差異を解析する。

イ　処理時間の差異を計測し解析する。

ウ　処理中に機器から放射される電磁波を観測し解析する。

エ　チップ内の信号線などに探針を直接当て，処理中のデータを観測し解析する。

問15　脆弱性検査で，対象ホストに対してポートスキャンを行った。対象ポートの状態を判定する方法のうち，適切なものはどれか。

ア　対象ポートに SYN パケットを送信し，対象ホストから“RST/ACK”パケットを受信するとき，接続要求が許可されたと判定する。

イ　対象ポートに SYN パケットを送信し，対象ホストから“SYN/ACK”パケットを受信するとき，接続要求が中断又は拒否されたと判定する。

ウ　対象ポートに UDP パケットを送信し，対象ホストからメッセージ“port unreachable”を受信するとき，対象ポートが閉じていると判定する。

エ　対象ポートに UDP パケットを送信し，対象ホストからメッセージ“port unreachable”を受信するとき，対象ポートが開いていると判定する。

問16　ダウンローダ型マルウェアが内部ネットワークの PC に感染したとき，そのマルウェアによってインターネット経由で他のマルウェアがダウンロードされることを防ぐ対策として，最も有効なものはどれか。

ア　URL フィルタを用いてインターネット上の危険な Web サイトへの接続を遮断する。

イ　インターネットから内部ネットワークに向けた要求パケットによる不正侵入行為を IPS で破棄する。

ウ　スパムメール対策サーバでインターネットからのスパムメールを拒否する。

エ　メールフィルタで他サイトへの不正メール発信を遮断する。

問17　OAuth 2.0 において，Web サービス A の利用者 C が，Web サービス B にリソース D を所有している。利用者 C の承認の下，Web サービス A が，リソース D への限定的なアクセス権限を取得するときのプロトコル OAuth 2.0 の動作はどれか。

ア　Web サービス A が，アクセストークンを発行する。
イ　Web サービス A が，利用者 C のディジタル証明書を Web サービス B に送信する。
ウ　Web サービス B が，アクセストークンを発行する。
エ　Web サービス B が，利用者 C のディジタル証明書を Web サービス A に送信する。

問18　DNS の MX レコードで指定するものはどれか。

ア　宛先ドメインへの電子メールを受け付けるメールサーバ
イ　エラーが発生したときの通知先のメールアドレス
ウ　複数の DNS サーバが動作しているときのマスタ DNS サーバ
エ　メーリングリストを管理しているサーバ

問19　スパニングツリープロトコルの機能を説明したものはどれか。

ア　MAC アドレスを見て，フレームを廃棄するか中継するかを決める。
イ　一定時間通信が行われていない MAC アドレスを，MAC アドレステーブルから消去する。
ウ　経路が複数存在する場合，アプリケーションやアドレスごとに経路を振り分けて，負荷を分散する。
エ　複数のブリッジ間で情報を交換し合い，ループ発生の検出や障害発生時の迂回ルート決定を行う。

問20　ファイル転送プロトコル TFTP を FTP と比較したときの記述として，適切なものはどれか。

ア　暗号化を用いてセキュリティ機能を強化したファイル転送プロトコル
イ　インターネットからのファイルのダウンロード用に特化したファイル転送プロトコル
ウ　テキストデータの転送を効率的に行うためにデータ圧縮機能を追加したファイル転送プロトコル
エ　ユーザ認証を省略し UDP を用いる，簡素化されたファイル転送プロトコル

問21　データウェアハウスを構築するために，業務システムごとに異なっているデータ属性やコード体系を統一する処理はどれか。

ア　ダイス　　イ　データクレンジング
ウ　ドリルダウン　　エ　ロールアップ

問22　ソフトウェア開発・保守の工程において，リポジトリを構築する理由として，最も適切なものはどれか。

ア　各工程で検出した不良を管理することが可能になり，ソフトウェアの品質分析が容易になる。
イ　各工程での作業手順を定義することが容易になり，開発・保守時の作業ミスを防止することができる。
ウ　各工程での作業予定と実績を関連付けて管理することが可能になり，作業の進捗管理が容易になる。
エ　各工程での成果物を一元管理することによって，開発・保守作業の効率が良くなり，用語の統一もできる。

問23　特許権に関する記述のうち，適切なものはどれか。

ア　A 社が特許を出願するよりも前に B 社が独自に開発して日本国内で発売した製品は，A 社の特許権の侵害にならない。

イ　組込み機器におけるハードウェアは特許権で保護されるが，ソフトウェアは保護されない。

ウ　審査を受けて特許権を取得した後に，特許権が無効となることはない。

エ　先行特許と同一の技術であっても，独自に開発した技術であれば特許権の侵害にならない。

問24　入出力データの管理方針のうち，適切なものはどれか。

ア　出力帳票の受渡しは授受管理表などを用いて確実に行い，情報の重要度によっては業務部門の管理者に手渡しする。

イ　出力帳票の利用状況を定期的に点検し，利用されていないと判断したものは，情報システム部門の判断で出力を停止する。

ウ　チェックによって発見された入力データの誤りは，情報システム部門の判断で修正する。

エ　入力原票や EDI 受信ファイルなどの取引情報は，機密性を確保するために，データをシステムに取り込んだら速やかに廃棄する。

問25　システム監査における監査証拠の説明のうち，適切なものはどれか。

ア　監査人が収集又は作成する資料であり，監査報告書に記載する監査意見や指摘事項は，その資料によって裏付けられていなければならない。

イ　監査人が当初設定した監査手続を記載した資料であり，監査人はその資料に基づいて監査を実施しなければならない。

ウ　機密性の高い情報が含まれている資料であり，監査人は監査報告書の作成後，速やかに全てを処分しなければならない。

エ　被監査部門が監査人に提出する資料であり，監査人が自ら作成する資料は含まれない。

〔 メ モ 用 紙 〕

6. **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。
7. 問題冊子の余白などは，適宜利用して構いません。
8. 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。
9. 試験終了後，この問題冊子は持ち帰ることができます。
10. 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。
11. 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。
12. 午後Ⅰ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。