SC

平成29年度　秋期
情報処理安全確保支援士試験
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〕　秋の情報処理安全確保支援士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　CRL（Certificate Revocation List）に掲載されるものはどれか。

ア　有効期限切れになったディジタル証明書の公開鍵
イ　有効期限切れになったディジタル証明書のシリアル番号
ウ　有効期限内に失効したディジタル証明書の公開鍵
エ　有効期限内に失効したディジタル証明書のシリアル番号

問２　PKI を構成する OCSP を利用する目的はどれか。

ア　誤って破棄してしまった秘密鍵の再発行処理の進捗状況を問い合わせる。
イ　ディジタル証明書から生成した鍵情報の交換が OCSP クライアントとレスポンダの間で失敗した際，認証状態を確認する。
ウ　ディジタル証明書の失効情報を問い合わせる。
エ　有効期限が切れたディジタル証明書の更新処理の進捗状況を確認する。

問３　標準化団体 OASIS が，Web サイト間で認証，属性及び認可の情報を安全に交換するために策定したフレームワークはどれか。

ア　SAML　　イ　SOAP　　ウ　XKMS　　エ　XML Signature

問4　ハッシュ関数の性質の一つである衝突発見困難性に関する記述のうち，適切なものはどれか。

ア　SHA-256 の衝突発見困難性を示す，ハッシュ値が一致する二つのメッセージの探索に要する最大の計算量は，256 の 2 乗である。

イ　SHA-256 の衝突発見困難性を示す，ハッシュ値の元のメッセージの探索に要する最大の計算量は，2 の 256 乗である。

ウ　衝突発見困難性とは，ハッシュ値が与えられたときに，元のメッセージの探索に要する計算量が大きいことによる，探索の困難性のことである。

エ　衝突発見困難性とは，ハッシュ値が一致する二つのメッセージの探索に要する計算量が大きいことによる，探索の困難性のことである。

問5　情報セキュリティにおけるエクスプロイトコードの説明はどれか。

ア　同じセキュリティ機能をもつ製品に乗り換える場合に，CSV など他の製品に取り込むことができる形式でファイルを出力するプログラム

イ　コンピュータに接続されたハードディスクなどの外部記憶装置や，その中に保存されている暗号化されたファイルなどを閲覧，管理するソフトウェア

ウ　セキュリティ製品を設計する際の早い段階から実際に動作する試作品を作成し，それに対する利用者の反応を見ながら徐々に完成に近づける開発手法

エ　ソフトウェアやハードウェアの脆弱性を利用するために作成されたプログラム

問６　DNS に対するカミンスキー攻撃（Kaminsky's attack）への対策はどれか。

ア　DNS キャッシュサーバと権威 DNS サーバとの計 2 台の冗長構成とすることによって，過負荷によるサーバダウンのリスクを大幅に低減させる。

イ　SPF（Sender Policy Framework）を用いて MX レコードを認証することによって，電子メールの送信元ドメインが詐称されていないかどうかを確認する。

ウ　問合せ時の送信元ポート番号をランダム化することによって，DNS キャッシュサーバに偽の情報がキャッシュされる確率を大幅に低減させる。

エ　プレースホルダを用いたエスケープ処理を行うことによって，不正な SQL 構文による DNS リソースレコードの書換えを防ぐ。

問７　DoS 攻撃の一つである Smurf 攻撃はどれか。

ア　ICMP の応答パケットを攻撃対象に大量に送り付ける。

イ　TCP 接続要求である SYN パケットを攻撃対象に大量に送り付ける。

ウ　サイズが大きい UDP パケットを攻撃対象に大量に送り付ける。

エ　サイズが大きい電子メールや大量の電子メールを攻撃対象に送り付ける。

問８　暗号化装置において暗号化処理時に消費電力を測定するなどして，当該装置内部の秘密情報を推定する攻撃はどれか。

ア　キーロガー　　イ　サイドチャネル攻撃

ウ　スミッシング　　エ　中間者攻撃

問9　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 クライアントと 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 クライアントからの通信を目的の Web サーバに中継する際に，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ソフトウェア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，通信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するかを判断する。

問10　ディジタル証明書に関する記述のうち，適切なものはどれか。

ア　S/MIME や TLS で利用するディジタル証明書の規格は，ITU-T X.400 で標準化されている。

イ　ディジタル証明書は，TLS プロトコルにおいて通信データの暗号化のための鍵交換や通信相手の認証に利用されている。

ウ　認証局が発行するディジタル証明書は，申請者の秘密鍵に対して認証局がディジタル署名したものである。

エ　ルート認証局は，下位の認証局の公開鍵にルート認証局の公開鍵でディジタル署名したディジタル証明書を発行する。

問11　不適合への対応のうち，JIS Q 27000:2014（情報セキュリティマネジメントシステム－用語）の“是正処置”の定義はどれか。

ア　不適合によって起こった結果に対処するための処置
イ　不適合の原因を除去し，再発を防止するための処置
ウ　不適合の性質及び対応結果について文書化するための処置
エ　不適合を除去するための処置

問12　JIS Q 27000:2014（情報セキュリティマネジメントシステム－用語）における情報セキュリティリスクに関する記述のうち，適切なものはどれか。

ア　脅威とは，一つ以上の要因によって悪用される可能性がある，資産又は管理策の弱点のことである。
イ　脆弱性とは，システム又は組織に損害を与える可能性がある，望ましくないインシデントの潜在的な原因のことである。
ウ　リスク対応とは，リスクの大きさが，受容可能か又は許容可能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のことである。
エ　リスク特定とは，リスクを発見，認識及び記述するプロセスのことであり，リスク源，事象，それらの原因及び起こり得る結果の特定が含まれる。

問13　基本評価基準，現状評価基準，環境評価基準の三つの基準で情報システムの脆弱性の深刻度を評価するものはどれか。

ア　CVSS　　イ　ISMS　　ウ　PCI DSS　　エ　PMS

問14　攻撃者が，Web アプリケーションのセッションを乗っ取り，そのセッションを利用してアクセスした場合でも，個人情報の漏えいなどに被害が拡大しないようにするために，重要な情報の表示などをする画面の直前で Web アプリケーションが追加的に行う対策として，最も適切なものはどれか。

ア　Web ブラウザとの間の通信を暗号化する。
イ　発行済セッション ID を Cookie に格納する。
ウ　発行済セッション ID を HTTP レスポンスボディ中のリンク先の URI のクエリ文字列に設定する。
エ　パスワードによる利用者認証を行う。

問15　スパムメールの対策として，宛先ポート番号 25 の通信に対して ISP が実施する OP25B の例はどれか。

ア　ISP 管理外のネットワークからの通信のうち，スパムメールのシグネチャに該当するものを遮断する。
イ　動的 IP アドレスを割り当てたネットワークから ISP 管理外のネットワークへの直接の通信を遮断する。
ウ　メール送信元のメールサーバについて DNS の逆引きができない場合，そのメールサーバからの通信を遮断する。
エ　メール不正中継の脆弱性をもつメールサーバからの通信を遮断する。

問16　外部から侵入されたサーバ及びそのサーバに接続されていた記憶媒体を調査対象としてディジタルフォレンジックスを行うことになった。まず，稼働状態にある調査対象サーバや記憶媒体などから表に示す a～d のデータを証拠として保全する。保全の順序のうち，最も適切なものはどれか。

	証拠として保全するデータ
a	遠隔にあるログサーバに記録された調査対象サーバのアクセスログ
b	調査対象サーバにインストールされていた会計ソフトのインストール用 CD
c	調査対象サーバのハードディスク上の表計算ファイル
d	調査対象サーバのルーティングテーブルの状態

ア　a → c → d → b

イ　b → c → a → d

ウ　c → a → d → b

エ　d → c → a → b

問17　無線 LAN の情報セキュリティ対策に関する記述のうち，適切なものはどれか。

ア　EAP では，クライアント PC とアクセスポイントとの間で，あらかじめ登録した共通鍵による暗号化通信を実現できる。

イ　RADIUS では，クライアント PC とアクセスポイントとの間で公開鍵暗号方式による暗号化通信を実現できる。

ウ　SSID は，クライアント PC ごとの秘密鍵を定めたものであり，公開鍵暗号方式による暗号化通信を実現できる。

エ　WPA2-Enterprise では，IEEE 802.1X の規格に沿った利用者認証及び動的に配布される暗号化鍵を用いた暗号化通信を実現できる。

問18　ルータで接続された二つのセグメント間でのコリジョンの伝搬とブロードキャストフレームの中継について，適切な組合せはどれか。

	コリジョンの伝搬	ブロードキャストフレームの中継
ア	伝搬しない	中継しない
イ	伝搬しない	中継する
ウ	伝搬する	中継しない
エ	伝搬する	中継する

問19　1台のサーバと複数台のクライアントが，100Mビット／秒のLANで接続されている。業務のピーク時には，クライアント1台につき1分当たり600kバイトのデータをサーバからダウンロードする。このとき，同時使用してもピーク時に業務を滞りなく遂行できるクライアント数は何台までか。ここで，LANの伝送効率は50%，サーバ及びクライアント内の処理時間は無視できるものとし，1Mビット／秒＝10^6ビット／秒，1kバイト＝1,000バイトとする。

ア　10　　イ　625　　ウ　1,250　　エ　5,000

問20　ネットワークに接続されているホストのIPアドレスが198.51.100.90で，サブネットマスクが255.255.255.224のとき，ホストアドレスはどれか。

ア　10　　イ　26　　ウ　90　　エ　212

問21　ビッグデータの解析に利用されるニューラルネットワークに関する記述のうち，適切なものはどれか。

ア　誤差逆伝播法（バックプロパゲーション）は，ニューラルネットワーク全体の重みを調整する手法であり，調整作業は入力層から出力層に向かって行われる。

イ　サポートベクタマシンは機械学習に必要な機能を実現する装置のことであり，ニューラルネットワークで大量計算する際に利用される。

ウ　深層学習（ディープラーニング）に用いられるニューラルネットワークは，入力層と出力層の間に複数の中間層をもつモデルが利用される。

エ　中間層を増やしたニューラルネットワークによる訓練データを用いた学習は，訓練データ以外の未知のデータに対しても高精度な正解が導け，これを過学習（オーバフィッティング）という。

問22　JIS X 25010:2013（システム及びソフトウェア製品の品質要求及び評価（SQuaRE）－システム及びソフトウェア品質モデル）におけるシステムの利用時の品質特性に“満足性”がある。“満足性”の品質副特性の一つである“実用性”の説明はどれか。

ア　個人的なニーズを満たすことから利用者が感じる喜びの度合い

イ　利用者がシステム又はソフトウェアを利用するときの快適さに満足する度合い

ウ　利用者又は他の利害関係者がもつ，製品又はシステムが意図したとおりに動作するという確信の度合い

エ　利用の結果及び利用の影響を含め，利用者が把握した目標の達成状況によって得られる利用者の満足の度合い

問23　企業間で，商用目的で締結されたソフトウェアの開発請負契約書に著作権の帰属が記載されていない場合，著作権の帰属先として，適切なものはどれか。

ア　請負人，注文者のどちらにも帰属しない。
イ　請負人と注文者が共有する。
ウ　請負人に帰属する。
エ　注文者に帰属する。

問24　情報システムの設計のうち，フェールソフトの考え方を適用した例はどれか。

ア　UPS を設置することによって，停電時に手順どおりにシステムを停止できるようにする。
イ　制御プログラムの障害時に，システムの暴走を避け，安全に運転を停止できるようにする。
ウ　ハードウェアの障害時に，パフォーマンスは低下するが，構成を縮小して運転を続けられるようにする。
エ　利用者の誤操作や誤入力を未然に防ぐことによって，システムの誤動作を防止できるようにする。

問25　株式会社の内部監査におけるシステム監査を，システム監査基準（平成 16 年）に基づいて実施する場合の監査責任者及びメンバに関する記述のうち，適切なものはどれか。

ア　あるメンバを，当該メンバが過去に在籍していた部門に対する監査に従事させる場合，一定の期間を置く。

イ　監査責任者は，当該株式会社の株主に限る。

ウ　監査部門の在籍期間について，メンバの場合は制限がないが，監査責任者の場合は会社法における監査役の任期を下回ってはならない。

エ　メンバの給与その他の報酬の水準は，監査部門に在籍中は引き下げてはならない。

〔 メ モ 用 紙 〕

〔 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。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。
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。