SC

平成31年度　春期
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〕　春の情報処理安全確保支援士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　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 OCSP 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 サイトなどを運営するオンラインビジネスパートナ間で認証，属性及び認可の情報を安全に交換するために策定したものはどれか。

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発見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発見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，元のメッセージの発見に要する計算量が大きいことによる，発見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発見に要する計算量が大きいことによる，発見の困難性のことである。

問５　仮想通貨環境において，報酬を得るために行われるクリプトジャッキングはどれか。

ア　他人の PC 又はサーバに侵入して計算資源を不正に利用し，台帳への追記の計算を行う。

イ　他人の PC 又はサーバに保存された顧客情報を不正に取得して，販売する。

ウ　他人の PC 又はサーバのキーボードからの入力値を不正に取得して，攻撃者のサーバに送信する。

エ　他人の PC 又はサーバのファイルを暗号化して利用できなくし，警告文を表示して報酬を要求する。

問6　DoS 攻撃の一つである Smurf 攻撃はどれか。

ア　ICMP の応答パケットを大量に発生させ，それが攻撃対象に送られるようにする。

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7　サイドチャネル攻撃に該当するものはどれか。

ア　暗号化装置における暗号化処理時の消費電力などの測定や統計処理によって，当該装置内部の秘密情報を推定する攻撃

イ　攻撃者が任意に選択した平文とその平文に対応した暗号文から数学的手法を用いて暗号鍵を推測し，同じ暗号鍵を用いて作成された暗号文を解読する攻撃

ウ　操作中の人の横から，入力操作の内容を観察することによって，利用者 ID とパスワードを盗み取る攻撃

エ　無線 LAN のアクセスポイントを不正に設置し，チャネル間の干渉を発生させることによって，通信を妨害する攻撃

問８　インターネットバンキングサービスを提供する Web サイトを利用する際に，トランザクション署名の機能をもつハードウェアトークンを利用する。次の処理を行うとき，(4)によってできることはどれか。ここで，ハードウェアトークンは利用者ごとに異なり，本人だけが利用する。

〔処理〕

(1) ハードウェアトークンに振込先口座番号と振込金額を入力し，メッセージ認証符号（MAC）を生成する。

(2) Web サイトの振込処理画面に振込先口座番号，振込金額及び(1)で生成された MAC を入力し，Web サイトに送信する。

(3) Web サイトでは，本人に発行したハードウェアトークンと同じ処理手順によって振込先口座番号と振込金額から MAC を生成する。

(4) Web サイトでは，(2)で入力された MAC と，(3)で生成した MAC を比較する。

ア　通信経路において盗聴されていないことを確認できる。

イ　通信経路における盗聴者を特定できる。

ウ　振込先口座番号と振込金額が改ざんされていないことを確認できる。

エ　振込先口座番号と振込金額の改ざんされた箇所を訂正できる。

問9　総務省及び経済産業省が策定した“電子政府における調達のために参照すべき暗号のリスト（CRYPTREC 暗号リスト）”に関する記述のうち，適切なものはどれか。

ア　CRYPTREC 暗号リストにある運用監視暗号リストとは，運用監視システムにおける利用実績が十分であると判断され，電子政府において利用を推奨する暗号技術のリストである。

イ　CRYPTREC 暗号リストにある証明書失効リストとは，政府共用認証局が公開している，危殆化した暗号技術のリストである。

ウ　CRYPTREC 暗号リストにある推奨候補暗号リストとは，安全性及び実装性能が確認され，今後，電子政府推奨暗号リストに掲載される可能性がある暗号技術のリストである。

エ　CRYPTREC 暗号リストにある電子政府推奨暗号リストとは，互換性維持目的に限った継続利用を推奨する暗号技術のリストである。

問10　クロスサイトリクエストフォージェリ攻撃の対策として，**効果がない**ものはどれか。

ア　Web サイトでの決済などの重要な操作の都度，利用者のパスワードを入力させる。

イ　Web サイトへのログイン後，毎回異なる値を HTTP レスポンスに含め，Web ブラウザからのリクエストごとに送付されるその値を，Web サーバ側で照合する。

ウ　Web ブラウザからのリクエスト中の Referer によって正しいリンク元からの遷移であることを確認する。

エ　Web ブラウザからのリクエストを Web サーバで受け付けた際に，リクエストに含まれる“<”や“>”などの特殊文字を，タグとして認識されない“<”や“>”などの文字列に置き換える。

問11　DNS キャッシュポイズニング攻撃に対して有効な対策はどれか。

ア　DNS サーバにおいて，侵入したマルウェアをリアルタイムに隔離する。

イ　DNS 問合せに使用する DNS ヘッダ内の ID を固定せずにランダムに変更する。

ウ　DNS 問合せに使用する送信元ポート番号を 53 番に固定する。

エ　外部からの DNS 問合せに対しては，宛先ポート番号 53 のものだけに応答する。

問12　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，スイッチのポートをセグメントに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 アドレスをもつ PC の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13　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 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装するための規格である。

イ　RADIUS 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装するための規格である。

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装するための規格で規定されている。

エ　WPA2-Enterprise 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装するための方式である。

問14　インターネットサービスプロバイダ（ISP）が，OP25B を導入する目的はどれか。

ア　ISP 管理外のネットワークに対する ISP 管理下のネットワークからの ICMP パケットによる DDoS 攻撃を遮断する。

イ　ISP 管理外のネットワークに向けて ISP 管理下のネットワークから送信されるスパムメールを制限する。

ウ　ISP 管理下のネットワークに対する ISP 管理外のネットワークからの ICMP パケットによる DDoS 攻撃を遮断する。

エ　ISP 管理下のネットワークに向けて ISP 管理外のネットワークから送信されるスパムメールを制限する。

問15　SPF（Sender Policy Framework）によるドメイン認証を実施する場合，SPFの導入時に，電子メール送信元アドレスのドメイン所有者側で行う必要がある設定はどれか。

ア　DNSサーバにSPFレコードを登録する。
イ　DNSの問合せで使用するポート番号を変更する。
ウ　メールサーバにディジタル証明書を導入する。
エ　メールサーバのTCPポート25番を利用不可にする。

問16　内部ネットワーク上のPCからインターネット上のWebサイトを参照するときは，DMZ上のVDI（Virtual Desktop Infrastructure）サーバにログインし，VDIサーバ上のWebブラウザを必ず利用するシステムを導入する。インターネット上のWebサイトから内部ネットワーク上のPCへのマルウェアの侵入，及びインターネット上のWebサイトへのPC内のファイルの流出を防止する効果を得るために必要な条件はどれか。

ア　PCとVDIサーバ間は，VDIの画面転送プロトコル及びファイル転送を利用する。
イ　PCとVDIサーバ間は，VDIの画面転送プロトコルだけを利用する。
ウ　VDIサーバが，プロキシサーバとしてHTTP通信を中継する。
エ　VDIサーバが，プロキシサーバとしてVDIの画面転送プロトコルだけを中継する。

問17　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18　無線 LAN の隠れ端末問題の説明として，適切なものはどれか。

ア　アクセスポイントが SSID ステルス機能を用いてビーコン信号を止めることによって，端末から利用可能な SSID が分からなくなる問題

イ　端末がアクセスポイントとは通信できるが，他の端末のキャリアを検出できない状況にあり，送信フレームが衝突を起こしやすくなる問題

ウ　端末が別のアクセスポイントとアソシエーションを確立することによって，その端末が元のアクセスポイントからは見えなくなる問題

エ　複数の端末が同時にフレームを送信したとき，送信した端末が送信フレームの衝突を検出できない問題

問19　シリアル回線で使用するものと同じデータリンクのコネクション確立やデータ転送を，LAN 上で実現するプロトコルはどれか。

ア　MPLS　　イ　PPP　　ウ　PPPoE　　エ　PPTP

問20　ネットワーク管理プロトコルである SNMPv3 で使われる PDU のうち，事象の発生をエージェントが自発的にマネージャに知らせるために使用するものはどれか。ここで，エージェントとはエージェント相当のエンティティ，マネージャとはマネージャ相当のエンティティを指す。

ア　GetRequest-PDU　　イ　Response-PDU
ウ　SetRequest-PDU　　エ　SNMPv2-Trap-PDU

問21　次の表において，“在庫”表の製品番号に参照制約が定義されているとき，その参照制約によって拒否される可能性がある操作はどれか。ここで，実線の下線は主キーを，破線の下線は外部キーを表す。

在庫（在庫管理番号，製品番号，在庫量）
製品（製品番号，製品名，型，単価）

ア　“在庫”表の行削除　　イ　“在庫”表の表削除
ウ　“在庫”表への行追加　　エ　“製品”表への行追加

問22　問題を引き起こす可能性があるデータを大量に入力し，そのときの応答や挙動を監視することによって，ソフトウェアの脆弱性を検出するテスト手法はどれか。

ア　限界値分析　　イ　実験計画法　　ウ　ファジング　　エ　ロードテスト

問23　マッシュアップに該当するものはどれか。

ア　既存のプログラムから，そのプログラムの仕様を導き出す。
イ　既存のプログラムを部品化し，それらの部品を組み合わせて，新規プログラムを開発する。
ウ　クラスライブラリを利用して，新規プログラムを開発する。
エ　公開されている複数のサービスを利用して，新たなサービスを提供する。

問24　データの追加・変更・削除が，少ないながらも一定の頻度で行われるデータベースがある。このデータベースのフルバックアップを磁気テープに取得する時間間隔を今までの 2 倍にした。このとき，データベースのバックアップ又は復旧に関する記述のうち，適切なものはどれか。

ア　復旧時に行うログ情報の反映の平均処理時間が約 2 倍になる。
イ　フルバックアップ取得 1 回当たりの磁気テープ使用量が約 2 倍になる。
ウ　フルバックアップ取得 1 回当たりの磁気テープ使用量が約半分になる。
エ　フルバックアップ取得の平均処理時間が約 2 倍になる。

問25　システム監査における監査調書の説明として，適切なものはどれか。

ア　監査対象部門が，監査報告後に改善提案への対応方法を記入したもの
イ　監査対象部門が，予備調査前に当該部門の業務内容をとりまとめたもの
ウ　監査人が，実施した監査のプロセスを記録したもの
エ　監査人が，年度の監査計画を監査対象ごとに詳細化して作成したもの

〔 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。