SC

令和７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注意してください。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〕　春期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　DRDoS 攻撃に該当するものはどれか。

ア　サーバの可用性を脅かす脆弱性が発見されてから対策が提供されるまでの間に，その脆弱性を攻撃者が悪用することによって，標的のサーバのリソースを枯渇させ，利用を妨害する。

イ　最初の接続要求（SYN）パケットを繰り返し送信することによって，標的のサーバの利用可能なメモリを枯渇させ，利用を妨害する。

ウ　多数の DNS サーバに対して送信元の IP アドレスを標的の IP アドレスに偽装したリクエストを送信し，それらのサーバの応答パケットによって，標的のサーバのリソースを枯渇させ，利用を妨害する。

エ　多数の HTTP リクエストを長期間掛けて送信し続けることによって，標的の Web サーバのセッションを占有し，利用を妨害する。

問２　シングルサインオンの実装方式の一つである SAML 認証の特徴として，適切なものはどれか。

ア　IdP（Identity Provider）が利用者認証を行い，認証成功後に発行されるアサーションを SP（Service Provider）が検証し，問題がなければクライアントは SP にアクセスできるようになる。

イ　Web サーバに導入されたエージェントが認証サーバと連携して利用者認証を行い，クライアントは認証成功後に発行される cookie を使用して SP にアクセスできるようになる。

ウ　認証サーバは Kerberos プロトコルを使って利用者認証を行い，クライアントは認証成功後に発行されるチケットを使用して SP にアクセスできるようになる。

エ　リバースプロキシで利用者認証が行われ，クライアントは認証成功後にリバースプロキシ経由で SP にアクセスできるようになる。

問３　SHA-512/256 の説明はどれか。

ア　入力データに SHA-256 に基づいたハッシュ関数を 1 回適用し，256 ビットの値を出力した後，512 ビットに拡張して出力する。

イ　入力データに SHA-256 に基づいたハッシュ関数を 512 回繰り返し適用し，256 ビットの値を出力する。

ウ　入力データに SHA-512 に基づいたハッシュ関数を 1 回適用し，512 ビットの値を出力した後，256 ビットに切り詰めて出力する。

エ　入力データに SHA-512 に基づいたハッシュ関数を 256 回繰り返し適用し，512 ビットの値を出力する。

問４　DNS に対するカミンスキー攻撃への対策はどれか。

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 を用いて DNS リソース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　SQL 文の組立てにプレースホルダを用いることによって，不正な SQL 文による DNS リソースレコードの書換えを防ぐ。

エ　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。

問５　クリプトジャッキングに該当するものはどれか。

ア　PC に不正アクセスし，その PC のリソースを利用して，暗号資産のマイニングを行う攻撃

イ　暗号資産取引所の Web サイトに不正ログインを繰り返し，取引所の暗号資産を盗む攻撃

ウ　巧妙に細工した電子メールのやり取りによって，企業の担当者をだまし，攻撃者の用意した暗号資産口座に送金させる攻撃

エ　マルウェア感染した PC に制限を掛けて利用できないようにし，その制限の解除と引換えに暗号資産を要求する攻撃

問６　デ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 で利用するデジタル証明書の規格は，ITU-T X.400 で標準化されている。

イ　TLS において，デジタル証明書は，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ジタル証明書は，申請者の秘密鍵に対して認証局がデ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ジタル署名したデジタル証明書を発行する。

問７　マルウェア Mirai の動作はどれか。

ア　IoT 機器などで動作する Web サーバプログラムの脆弱性を悪用して感染を広げ，Web ページを改ざんし，決められた日時に特定の IP アドレスに対して DDoS 攻撃を行う。

イ　Web サーバプログラムの脆弱性を悪用して企業の Web ページに不正な JavaScript を挿入し，当該 Web ページを閲覧した利用者を不正な Web サイトへと誘導する。

ウ　ファイル共有ソフトを使っている PC 内でマルウェアの実行ファイルを利用者が誤って実行すると，PC 内の情報をインターネット上の Web サイトにアップロードして不特定多数の人に公開する。

エ　ランダムな宛先 IP アドレスを使用して IoT 機器などに感染を広げるとともに，C&C サーバからの指令に従って標的に対して DDoS 攻撃を行う。

問８　サイバー攻撃における，コネクトバックの説明はどれか。

ア　PC をマルウェアに感染させてスクリーンロックしたり，ファイルを暗号化したりして使用不能にし，逆に復号することと引換えに金銭を要求する。

イ　一見すると有益なソフトウェアと見せかけて，逆にマルウェアを利用者の PC にシェルを用いて利用者が気付かないうちにインストールさせる。

ウ　侵害したシステムから攻撃者のサーバに対して通信を開始する。

エ　製品，ソフトウェアなどを分解又は解析し，その仕組み，仕様，構成部品を明らかにしてバックドアを仕込む。

問９　公開鍵基盤における CPS（Certification Practice Statement）はどれか。

ア　認証局が発行するデジタル証明書の所有者が策定したセキュリティ宣言

イ　認証局でのデジタル証明書発行手続を代行する事業者が策定したセキュリティ宣言

ウ　認証局の認証業務の運用などに関する詳細を規定した文書

エ　認証局を監査する第三者機関の運用などに関する詳細を規定した文書

問10　JIS Q 27000:2019（情報セキュリティマネジメントシステム―用語）の用語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付け込まれる可能性がある，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11　“政府情報システムのためのセキュリティ評価制度（ISMAP）”の説明はどれか。

ア　個人情報の取扱いについて政府が求める保護措置を講じる体制を整備している事業者などを評価して，適合を示すマークを付与し，個人情報を取り扱う政府情報システムの運用について，当該マークを付与された者への委託を認める制度

イ　個人データを海外に移転する際に，移転先の国の政府が定めた情報システムのセキュリティ基準を評価して，日本が求めるセキュリティ水準が確保されている場合には，本人の同意なく移転できるとする制度

ウ　政府が求めるセキュリティ要求を満たしているクラウドサービスをあらかじめ評価，登録することによって，政府のクラウドサービス調達におけるセキュリティ水準の確保を図る制度

エ　プライベートクラウドの情報セキュリティ全般に関するマネジメントシステムの規格にパブリッククラウドサービスに特化した管理策を追加した国際規格を基準にして，政府情報システムにおける情報セキュリティ管理体制を評価する制度

問12　NIST“サイバーセキュリティフレームワーク（CSF） 2.0”のコアには，機能が六つある。IDENTIFY, PROTECT, DETECT, RESPOND, RECOVER と，あと一つはどれか。

ア　CONTROL　　イ　DIRECT　　ウ　GOVERN　　エ　MANAGE

問13　IoC（Indicator of Compromise）に該当するものはどれか。

ア　JVN上で公開されている，あるソフトウェアに関する脆弱性情報
イ　ある認証局が公開している公開鍵証明書の失効リスト
ウ　あるネットワーク機器のログに残されたC&Cサーバとの通信履歴
エ　あるファイアウォールに設定されたパケットフィルタリングルール

問14　サイドチャネル攻撃の手法であるタイミング攻撃の対策として，最も適切なものはどれか。

ア　演算アルゴリズムに処理を追加して，秘密情報の違いによって演算の処理時間に差異が出ないようにする。
イ　コンデンサを挿入して，電力消費量が時間的に均一になるようにする。
ウ　ハードウェアを自ら診断することによって故障を検出する機構，及び故障を検出したら秘密情報を破壊する機構を設ける。
エ　保護層を備えて，内部のデータが不正に書き換えられないようにする。

問15　マルウェア感染の調査対象のPCに対して，電源を切る前に全ての証拠保全を行いたい。ARPキャッシュを取得した後に保全すべき情報のうち，最も優先して保全すべきものはどれか。

ア　調査対象のPCで動的に追加されたルーティングテーブル
イ　調査対象のPCに増設されたHDDにある個人情報を格納したテキストファイル
ウ　調査対象のPCのVPN接続情報を記録しているVPNサーバ内のログ
エ　調査対象のPCのシステムログファイル

問16　OAuth 2.0 に関する記述のうち，適切なものはどれか。

ア　認可を行うためのプロトコルであり，認可サーバが，アクセスしてきた者が利用者（リソースオーナー）本人であるかどうかを確認するためのものである。

イ　認可を行うためのプロトコルであり，認可サーバが，利用者（リソースオーナー）の許可を得て，サービス（クライアント）に対し，適切な権限を付与するためのものである。

ウ　認証を行うためのプロトコルであり，認証サーバが，アクセスしてきた者が利用者（リソースオーナー）本人であるかどうかを確認するためのものである。

エ　認証を行うためのプロトコルであり，認証サーバが，利用者（リソースオーナー）の許可を得て，サービス（クライアント）に対し，適切な権限を付与するためのものである。

問17　ISP が，OP25B を導入する目的の一つはどれか。

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18　イーサネットにおいて，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，宛先 MAC アドレスの全てのビットが 1 である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　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　Web ページ内の HTML フォームに入力されたデータが Web サーバに送られる際には，HTTP プロトコルの GET メソッド又は POST メソッドを用いたリクエストメッセージが使用される。このとき，入力されたデータはリクエストメッセージのどの部分に含まれるか。ここで，HTTP のバージョンは HTTP/1.1 とし，リクエストメッセージは，リクエスト行，ヘッダー，メッセージボディの順で構成されているものとする。

	GET メソッドが使用される場合	POST メソッドが使用される場合
ア	リクエスト行	ヘッダー
イ	リクエスト行	メッセージボディ
ウ	ヘッダー	ヘッダー
エ	ヘッダー	メッセージボディ

問21　“従業員”表に対して，SQL 文を実行して得られる結果はどれか。ここで，実線の下線は主キーを表し，表中の NULL は値が存在しないことを表す。

従業員

従業員コード	上司	従業員名
S001	NULL	A
S002	S001	B
S003	S001	C
S004	S003	D
S005	NULL	E
S006	S005	F
S007	S006	G

〔SQL 文〕

```
SELECT 従業員コード FROM 従業員 X
    WHERE NOT EXISTS
        (SELECT * FROM 従業員 Y WHERE X.従業員コード = Y.上司)
```

ア

従業員コード
S001
S003
S005
S006

イ

従業員コード
S001
S005

ウ

従業員コード
S002
S004
S007

エ

従業員コード
S003
S006

問22　アジャイル開発のプロジェクトで，ソースコードの品質を向上させるために，バグ，コードの重複，脆弱性につながるコードを自動で検出することができる OSS のツールを導入したい。導入する OSS として，最も適切なものはどれか。

ア　Git　　イ　Jenkins　　ウ　Snort　　エ　SonarQube

問23　アジャイル開発手法の一つであるスクラムを適用したソフトウェア開発プロジェクトにおいて，KPT 手法を用いてレトロスペクティブを行った。KPT における三つの視点の組みはどれか。

ア　Kaizen, Persona, Try　　イ　Keep, Problem, Try
ウ　Knowledge, Persona, Test　　エ　Knowledge, Practice, Team

問24　サービス提供時間帯が毎日 6 時 ～ 20 時のシステムにおいて，ある月の停止時間，修復時間及びシステムメンテナンス時間は次のとおりであった。この月のサービス可用性は何%か。ここで，1 か月の稼働日数は 30 日であって，サービス可用性（%）は小数第 2 位を四捨五入するものとする。

〔停止時間，修復時間及びシステムメンテナンス時間〕
・システム障害によるサービス提供時間内の停止時間：7 時間
・システム障害への対処に要したサービス提供時間外の修復時間：3 時間
・サービス提供時間外のシステムメンテナンス時間：8 時間

ア　95.7　　イ　97.6　　ウ　98.3　　エ　99.0

問25　金融庁“財務報告に係る内部統制の評価及び監査に関する実施基準（令和 5 年）”によれば，“記録した取引に漏れ，重複がないこと”は，組織目標を達成するための IT の統制目標のうち，どれに含まれるか。

ア　可用性　　イ　機密性　　ウ　準拠性　　エ　信頼性

〔 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。