SC

# 令和６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〕　秋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　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　RADIUS や Diameter が提供する AAA フレームワークの構成要素は，認証（Authentication），認可（Authorization）と，もう一つはどれか。

ア　Accounting　　イ　Activation

ウ　Audit　　エ　Augmented Reality

問２　AI による画像認識において，認識させる画像の中に人間には知覚できないノイズや微小な変化を含めることによって，AI アルゴリズムの特性を悪用し，誤認識させる攻撃はどれか。

ア　Adaptively Chosen Message 攻撃

イ　Adversarial Examples 攻撃

ウ　Distributed Reflection Denial of Service 攻撃

エ　Model Inversion 攻撃

問３　様々なサイバー攻撃手法を分類したナレッジベースはどれか。

ア　CVSS　　イ　MITRE ATT&CK

ウ　STIX/TAXII　　エ　サイバーキルチェーン

問４　NTP リフレクション攻撃の特徴はどれか。

ア　攻撃対象である NTP サーバに高頻度で時刻を問い合わせる。

イ　攻撃対象である NTP サーバの時刻情報を書き換える。

ウ　送信元を偽って，NTP サーバに echo request を送信する。

エ　送信元を偽って，NTP サーバにレスポンスデータが大きくなるリクエストを送信する。

問５　PQC（Post-Quantum Cryptography）はどれか。

ア　量子アニーリングマシンを用いて，回路サイズ，消費電力，処理速度を飛躍的に向上させた実装性能をもつ暗号方式

イ　量子コンピュータを用いて効率的に素因数分解を行うアルゴリズムによって，暗号を解読する技術

ウ　量子コンピュータを用いても解読が困難であり，安全性を保つことができる暗号方式

エ　量子通信路を用いた鍵配送システムを利用し，大容量のデータを高速に送受信する技術

問６　Smurf 攻撃はどれか。

ア　ICMP エコー要求パケットの送信元 IP アドレスに攻撃対象の IP アドレスを設定し，宛先にブロードキャストアドレスを設定して送信することによって攻撃対象を利用不能にさせる。

イ　送信元 IP アドレスに偽の IP アドレスを設定し，かつ，攻撃対象の受信可能範囲を超える大きなパケットを送信して攻撃対象を停止させる。

ウ　送信元 IP アドレスに偽の IP アドレスを設定した大量の SYN パケットを送信し，攻撃対象からの SYN-ACK パケットに対して SYN-ACK の応答を送信しないことによって攻撃対象のリソースを枯渇させる。

エ　ボットネットを使って多数の端末から攻撃対象のメールサーバに大量のなりすましメールを送信し，攻撃対象のメールサーバを停止させる。

問７　ある IdP（Identity Provider）は，パスキー（Passkey）認証をサポートしており，利用者 A は，この IdP の FIDO 認証器として，自分のスマートフォンの生体認証機能を登録してある。また，Web サーバ B は，この IdP を使ってログインが可能である。利用者 A の Web ブラウザから Web サーバ B にアクセスする際，利用者 A の生体情報を受信するもの，受信しないものの組合せのうち，適切なものはどれか。

| | 利用者 A の Web ブラウザ | Web サーバ B | IdP |
|---|---|---|---|
| ア | 受信しない | 受信しない | 受信しない |
| イ | 受信しない | 受信する | 受信する |
| ウ | 受信する | 受信しない | 受信しない |
| エ | 受信する | 受信する | 受信する |

問８　シングルサインオン（SSO）に関する記述のうち，適切なものはどれか。

ア　SAML 方式では，URL 形式の 1 人一つの利用者 ID を IdP（Identity Provider）で自動生成することによって，インターネット上の複数の Web サイトにおける SSO を実現する。

イ　エージェント方式では，クライアント PC に導入したエージェントが SSO の対象システムのログイン画面を監視し，ログイン画面が表示されたら認証情報を代行入力する。

ウ　代理認証方式では，SSO の対象サーバに SSO のモジュールを組み込む必要があり，システムの改修が必要となる。

エ　リバースプロキシ方式では，SSO を利用する全てのトラフィックがリバースプロキシサーバに集中する。

問９　量子暗号の特徴として，適切なものはどれか。

ア　暗号化と復号の処理を，量子コンピュータを用いて行うことができるので，従来のコンピュータでの処理に比べて大量のデータの秘匿を短時間で実現できる。

イ　共通鍵暗号方式であり，従来の情報の取扱量の最小単位であるビットの代わりに量子ビットを用いることによって，高速なデータ送受信が実現できる。

ウ　量子雑音を用いて共通鍵を生成し，公開鍵暗号方式で共有することによって，解読が困難な秘匿通信が実現できる。

エ　量子通信路を用いて安全に共有した乱数列を使い捨ての暗号鍵として用いることによって，原理的に第三者に解読されない秘匿通信が実現できる。

問10　電子メールの受信者側のメールサーバでの送信ドメイン認証が失敗したときの処理方針を，送信側のドメイン管理者が指定するための仕組みはどれか。

ア　DKIM　　イ　DMARC　　ウ　SMTP-AUTH　　エ　SPF

問11　SOAR（Security Orchestration, Automation and Response）の説明はどれか。

ア　脅威インテリジェンスの活用，セキュリティ運用の自動化及びインシデント対応の効率化を行う技術

イ　全ての利用者，デバイス，接続元を信頼できないものとして捉え，重要な情報資産やシステムに対するアクセスの正当性や安全性の検証を自動化することによって脅威を防ぐ考え方

ウ　組織間でサイバー攻撃に関する情報を効率的に交換するために，脅威情報構造化記述形式で記述された情報の交換を自動化するためのプロトコル仕様

エ　ファイアウォール，マルウェア対策製品，侵入検知製品など複数のセキュリティ製品のログの集約及び相関分析を自動化するための専用装置

問12　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，数式を入力する Web サイトに“<”を数式の一部として含んだ 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に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ータ中に許可しない文字列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パラメータ中に含んだ不正な 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13　インラインモードで動作するアノマリ型 IPS はどれか。

ア　IPS が監視対象の通信経路を流れる全ての通信パケットを経路外からキャプチャできるように通信経路上のスイッチのミラーポートに接続される。異常な通信を定義し，それと合致する通信を不正と判断して遮断する。

イ　IPS が監視対象の通信経路を流れる全ての通信パケットを経路外からキャプチャできるように通信経路上のスイッチのミラーポートに接続される。通常時の通信を定義し，それから外れた通信を不正と判断して遮断する。

ウ　IPS が監視対象の通信を通過させるように通信経路上に設置される。異常な通信を定義し，それと合致する通信を不正と判断して遮断する。

エ　IPS が監視対象の通信を通過させるように通信経路上に設置される。通常時の通信を定義し，それから外れた通信を不正と判断して遮断する。

問14　クリックジャッキング攻撃に有効な対策はどれか。

ア　cookie に，HttpOnly 属性を設定する。
イ　cookie に，Secure 属性を設定する。
ウ　HTTP レスポンスヘッダーに，Strict-Transport-Security を設定する。
エ　HTTP レスポンスヘッダーに，X-Frame-Options を設定する。

問15　DTLS の特徴はどれか。

ア　IP パケットの暗号化を可能としている。
イ　PPP で接続する際のチャレンジレスポンス認証機能をイーサネット上の通信に提供している。
ウ　TCP のペイロードデータの暗号強度を TLS よりも強化している。
エ　UDP のペイロードデータの暗号化を可能としている。

問16　利用者 A が所有するリソース B が，Web サービス C 上にある。OAuth 2.0 において，利用者 A の認可の下，Web サービス D からリソース B への限定されたアクセスを可能にするときのプロトコルの動作はどれか。ここで Web サービス C は，認可サーバを兼ねているものとする。

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

問17　利用者認証情報を管理するサーバ1台と複数のアクセスポイントで構成された無線LAN環境を実現したい。PCが無線LAN環境に接続するときの利用者認証とアクセス制御に，IEEE 802.1XとRADIUSを利用する場合の標準的な方法はどれか。

ア　PCにはIEEE 802.1Xのサプリカントを実装し，かつ，RADIUSクライアントの機能をもたせる。
イ　アクセスポイントにはIEEE 802.1Xのオーセンティケータを実装し，かつ，RADIUSクライアントの機能をもたせる。
ウ　アクセスポイントにはIEEE 802.1Xのサプリカントを実装し，かつ，RADIUSサーバの機能をもたせる。
エ　サーバにはIEEE 802.1Xのオーセンティケータを実装し，かつ，RADIUSサーバの機能をもたせる。

問18　ネットワーク層のパケットを対象としてIPパケットでカプセル化し，トンネリングを行えるプロトコルはどれか。

ア　IPsec　　イ　L2TP　　ウ　PPTP　　エ　RSTP

問19　IPv4におけるICMPのメッセージに関する説明として，適切なものはどれか。

ア　送信元が設定したソースルーティングが失敗した場合は，Echo Replyを返す。
イ　転送されてきたデータグラムを受信したルータが，そのネットワークの最適なルータを送信元に通知して経路の変更を要請するには，Redirectを返す。
ウ　フラグメントの再組立て中にタイムアウトが発生した場合は，データグラムを破棄してParameter Problemを返す。
エ　ルータでメッセージを転送する際に，送信元が設定したTTLが0になった場合は，Destination Unreachableを返す。

問20　ネットワーク機器間の光ファイバを使った通信を分岐させてネットワーク上のトラフィックを取り出し，セキュリティ装置で監視したい。ネットワークから信号を光学的に分岐させて取り出す装置はどれか。

ア　ネットワークタップ　　イ　波長分割多重装置
ウ　ルータ　　エ　レイヤー2スイッチ

問21　関係モデルにおける外部キーに関する記述のうち，適切なものはどれか。

ア　外部キーの値は，その関係の中で一意でなければならない。
イ　外部キーは，それが参照する候補キーと比較可能でなくてもよい。
ウ　参照先の関係に，参照元の外部キーの値と一致する候補キーが存在しなくてもよい。
エ　一つの関係に外部キーが複数存在してもよい。

問22　ソフトウェアパターンのうち，GoF のデザインパターンの説明はどれか。

ア　Java のパターンとして，引数オブジェクト，オブジェクトの可変性などで構成される。
イ　オブジェクト指向開発のためのパターンであって，生成，構造，振る舞いの三つのカテゴリに分類される。
ウ　構造，分散システム，対話型システム及び適合型システムの四つのカテゴリに分類される。
エ　抽象度が異なる要素を分割して階層化するための Layers，コンポーネント分割のための Broker などで構成される。

問23　エクストリームプログラミング（XP：Extreme Programming）における“テスト駆動開発”の特徴はどれか。

ア　最初のテストで，なるべく多くのバグを摘出する。
イ　テストケースの改善を繰り返す。
ウ　テストでのカバレージを高めることを目的とする。
エ　プログラムコードを書く前にテストコードを書く。

問24　JIS Q 20000-1:2020（サービスマネジメントシステム要求事項）によれば，サービスマネジメントシステム（SMS）における継続的改善の定義はどれか。

ア　意図した結果を得るためにインプットを使用する，相互に関連する又は相互に作用する一連の活動
イ　価値を提供するため，サービスの計画立案，設計，移行，提供及び改善のための組織の活動及び資源を，指揮し，管理する，一連の能力及びプロセス
ウ　サービスを中断なしに，又は合意した可用性を一貫して提供する能力
エ　パフォーマンスを向上するために繰り返し行われる活動

問25　アクセス管理に関する内部統制のうち，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）”におけるITに係る業務処理統制に該当するものはどれか。

ア　組織としてアクセス管理規程を定め，統一的なアクセス管理を行う。
イ　組織としてアクセス権限の設定方針を定め，周知徹底を図る。
ウ　組織内のアプリケーションシステムに，利用者 ID とパスワードによって利用者を認証する機能を設ける。
エ　組織内の全ての利用者に対して，アクセス管理の重要性についての教育を行う。

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。