SC

令和３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　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，判定結果を誤らせる攻撃はどれか。

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２　Pass the Hash 攻撃はどれか。

ア　パスワードのハッシュ値から導出された平文パスワードを使ってログインする。
イ　パスワードのハッシュ値だけでログインできる仕組みを悪用してログインする。
ウ　パスワードを固定し，利用者 ID の文字列のハッシュ化を繰り返しながら様々な利用者 ID を試してログインする。
エ　ハッシュ化されずに保存されている平文パスワードを使ってログインする。

問３　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た攻撃に対しても，安全性を保つことができる暗号方式
ウ　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
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4　シングルサインオンの実装方式の一つである SAML 認証の特徴はどれか。

ア　IdP（Identity Provider）が SP（Service Provider）の認証要求によって利用者認証を行い，認証成功後に発行されるアサーションを SP が検証し，問題がなければクライアントが SP にアクセスする。

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利用者に発行される cookie を使用して SP にアクセスする。

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 にアクセスする。

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 にアクセスする。

問5　サイバーキルチェーンに関する説明として，適切なものはどれか。

ア　委託先の情報セキュリティリスクが委託元にも影響するという考え方を基にしたリスク分析のこと

イ　攻撃者がクライアントとサーバとの間の通信を中継し，あたかもクライアントとサーバが直接通信しているかのように装うことによって情報を盗聴するサイバー攻撃手法のこと

ウ　攻撃者の視点から，攻撃の手口を偵察から目的の実行までの段階に分けたもの

エ　取引データを複数の取引ごとにまとめ，それらを時系列につなげたチェーンに保存することによって取引データの改ざんを検知可能にしたもの

問６　ファイアウォールにおけるステートフルパケットインスペクションの特徴はどれか。

ア　IP アドレスの変換が行われることによって，内部のネットワーク構成を外部から隠蔽できる。

イ　暗号化されたパケットのデータ部を復号して，許可された通信かどうかを判断できる。

ウ　過去に通過したリクエストパケットに対応付けられる戻りのパケットを通過させることができる。

エ　パケットのデータ部をチェックして，アプリケーション層での不正なアクセスを防止できる。

問７　FIPS PUB 140-3 はどれか。

ア　暗号モジュールのセキュリティ要求事項

イ　情報セキュリティマネジメントシステムの要求事項

ウ　ディジタル証明書や証明書失効リストの技術仕様

エ　無線 LAN セキュリティの技術仕様

問８　X.509 における CRL（Certificate Revocation List）に関する記述のうち，適切なものはどれか。

ア　PKI の利用者の Web ブラウザは，認証局の公開鍵が Web ブラウザに組み込まれていれば，CRL を参照しなくてもよい。

イ　RFC 5280 では，認証局は，発行したディジタル証明書のうち失効したものについては，シリアル番号を失効後１年間 CRL に記載するよう義務付けている。

ウ　認証局は，発行した全てのディジタル証明書の有効期限を CRL に記載する。

エ　認証局は，有効期限内のディジタル証明書のシリアル番号を CRL に記載することがある。

問9　JIS Q 27002:2014 には記載されていないが，JIS Q 27017:2016 には記載されている管理策はどれか。

ア　クラウドサービス固有の情報セキュリティ管理策
イ　事業継続マネジメントシステムにおける管理策
ウ　情報セキュリティガバナンスにおける管理策
エ　制御システム固有のサイバーセキュリティ管理策

問10　cookie に Secure 属性を設定しなかったときと比較した，設定したときの動作として，適切なものはどれか。

ア　cookie に設定された有効期間を過ぎると，cookie が無効化される。
イ　JavaScript による cookie の読出しが禁止される。
ウ　URL 内のスキームが https のときだけ，Web ブラウザから cookie が送出される。
エ　Web ブラウザがアクセスする URL 内のパスと cookie に設定されたパスのプレフィックスが一致するときだけ，Web ブラウザから cookie が送出される。

問11　ネットワークカメラなどの IoT 機器では TCP 23 番ポートへの攻撃が多い理由はどれか。

ア　TCP 23 番ポートは IoT 機器の操作用プロトコルで使用されており，そのプロトコルを用いると，初期パスワードを使った不正ログインが成功し，不正に IoT 機器を操作できることが多いから

イ　TCP 23 番ポートは IoT 機器の操作用プロトコルで使用されており，そのプロトコルを用いると，マルウェアを添付した電子メールを IoT 機器に送信するという攻撃ができることが多いから

ウ　TCP 23 番ポートは IoT 機器へのメール送信用プロトコルで使用されており，そのプロトコルを用いると，初期パスワードを使った不正ログインが成功し，不正に IoT 機器を操作できることが多いから

エ　TCP 23 番ポートは IoT 機器へのメール送信用プロトコルで使用されており，そのプロトコルを用いると，マルウェアを添付した電子メールを IoT 機器に送信するという攻撃ができることが多いから

問12　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。このとき，稼働状態にある調査対象のサーバ，記憶媒体などから表に示すａ～ｄを証拠として保全する。保全の順序のうち，揮発性の観点から最も適切なものはどれか。

	証拠として保全するもの
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13　テンペスト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，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て解析する。

ウ　処理中に機器から放射される電磁波を観測して解析する。

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て解析する。

問14　ルートキットの特徴はどれか。

ア　OS などに不正に組み込んだツールの存在を隠す。
イ　OS の中核であるカーネル部分の脆弱性を分析する。
ウ　コンピュータがマルウェアに感染していないことをチェックする。
エ　コンピュータやルータのアクセス可能な通信ポートを外部から調査する。

問15　無線 LAN の暗号化通信を実装するための規格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 で利用する秘密鍵であり，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　WPA3-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規格である。

問16　IEEE 802.1X で使われる EAP-TLS が行う認証はどれか。

ア　CHAP を用いたチャレンジレスポンスによる利用者認証
イ　あらかじめ登録した共通鍵によるサーバ認証と，時刻同期のワンタイムパスワードによる利用者認証
ウ　ディジタル証明書による認証サーバとクライアントの相互認証
エ　利用者 ID とパスワードによる利用者認証

問17　TLS 1.3 の暗号スイートに関する説明のうち，適切なものはどれか。

ア　TLS 1.2 で規定されている共通鍵暗号 AES-CBC を必須の暗号アルゴリズムとして継続利用できるようにしている。

イ　Wi-Fi アライアンスにおいて規格化されている。

ウ　サーバとクライアントのそれぞれがお互いに別の暗号アルゴリズムを選択できる。

エ　認証暗号アルゴリズムとハッシュアルゴリズムの組みで構成されている。

問18　レイヤ 3 ネットワーク内に論理的なレイヤ 2 ネットワークをカプセル化によって構築するプロトコルはどれか。

ア　IEEE 802.1ad（QinQ）　　イ　IPsec

ウ　PPPoE　　エ　VXLAN

問19　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20　クラスBのIPアドレスで，サブネットマスクが16進数のFFFFFF80である場合，利用可能なホスト数は最大幾つか。

ア　126　　イ　127　　ウ　254　　エ　255

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　テスト担当者が，ソフトウェアを動作させてその動きを学習しながら，自身の経験に基づいて以降のテストを動的に計画して進めるテストの方法はどれか。

ア　実験計画法　　イ　状態遷移テスト
ウ　探索的テスト　　エ　モデルベースドテスト

問23　ブルーレイディスクで使われているコンテンツ保護技術はどれか。

ア　AACS　　イ　CPRM　　ウ　CSS　　エ　WMRM

問24　情報システムの設計の例のうち，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　クラウドサービスの導入検討プロセスに対するシステム監査において，クラウドサービス上に保存されている情報の保全及び消失の予防に関するチェックポイントとして，最も適切なものはどれか。

ア　クラウドサービスの障害時における最大許容停止時間が検討されているか。

イ　クラウドサービスの利用者 ID と既存の社内情報システムの利用者 ID の一元管理の可否が検討されているか。

ウ　クラウドサービスを提供する事業者が信頼できるか，事業者の事業継続性に懸念がないか，及びサービスが継続して提供されるかどうかが検討されているか。

エ　クラウドサービスを提供する事業者の施設内のネットワークに，暗号化通信が採用されているかどうかが検討されているか。

〔 メ モ 用 紙 〕

〔 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，マスク

   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。