SC

令和５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　デジタル庁，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(たい)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　シングルサインオンの実装方式の一つである SAML 認証の流れとして，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元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。

問５　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 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　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　ブロック暗号の暗号利用モードの一つである CTR（Counter）モードに関する記述のうち，適切なものはどれか。

ア　暗号化と復号の処理において，出力は，入力されたブロックと鍵ストリームとの排他的論理和である。

イ　暗号化の処理において，平文のデータ長がブロック長の倍数でないときにパディングが必要である。

ウ　ビット誤りがある暗号文を復号すると，ビット誤りのあるブロック全体と次のブロックの対応するビットが平文ではビット誤りになる。

エ　複数ブロックの暗号化の処理は並列に実行できないが，複数ブロックの復号の処理は並列に実行できる。

問８　政府情報システムのためのセキュリティ評価制度に用いられる“ISMAP 管理基準”が基礎としているものはどれか。

ア　FIPS 140-3（暗号モジュールのセキュリティ要求事項）

イ　ISO/IEC 27018:2019（個人識別情報（PII）プロセッサとして作動するパブリッククラウドにおける PII の保護のための実施基準）

ウ　JIS Q 15001:2017（個人情報保護マネジメントシステム－要求事項）

エ　日本セキュリティ監査協会“クラウド情報セキュリティ管理基準（平成 28 年度版）”

問9　NIST“サイバーセキュリティフレームワーク：重要インフラのサイバーセキュリティを改善するためのフレームワーク 1.1 版”における“フレームワークコア”を構成する機能はどれか。

ア　観察，状況判断，意思決定，行動
イ　識別，防御，検知，対応，復旧
ウ　準備，検知と分析，封じ込め/根絶/復旧，事件後の対応
エ　責任，戦略，取得，パフォーマンス，適合，人間行動

問10　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，“<”などの数式を含んだ正当な 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。
イ　HTTP リクエストのうち，RFC などに仕様が明確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の仕様で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11　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　故障を検出する機構を設けて，検出したら秘密情報を破壊する。

ウ　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。

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12　インラインモードで動作するシグネチャ型 IPS の特徴はどれか。

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，通常時の通信から外れた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，定義した異常な通信と合致する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，通常時の通信から外れた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，定義した異常な通信と合致する通信を不正と判断して遮断する。

問13　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14　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15　DKIM（DomainKeys Identified Mail）の説明はどれか。

ア　送信側メールサーバにおいてデジタル署名を電子メールのヘッダーに付加し，受信側メールサーバにおいてそのデジタル署名を公開鍵によって検証する仕組み

イ　送信側メールサーバにおいて利用者が認証された場合，電子メールの送信が許可される仕組み

ウ　電子メールのヘッダーや配送経路の情報から得られる送信元情報を用いて，電子メールの送信元のIPアドレスを検証する仕組み

エ　ネットワーク機器において，内部ネットワークから外部のメールサーバのTCPポート番号25への直接の通信を禁止する仕組み

問16　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17　SQL インジェクション対策について，Web アプリケーションプログラムの実装における対策と，Web アプリケーションプログラムの実装以外の対策の組みとして，適切なものはどれか。

	Web アプリケーションプログラムの実装における対策	Web アプリケーションプログラムの実装以外の対策
ア	Web アプリケーションプログラム中でシェルを起動しない。	chroot 環境で Web サーバを稼働させる。
イ	セッション ID を乱数で生成する。	TLS によって通信内容を秘匿する。
ウ	パス名やファイル名をパラメータとして受け取らないようにする。	重要なファイルを公開領域に置かない。
エ	プレースホルダを利用する。	Web アプリケーションプログラムが利用するデータベースのアカウントがもつデータベースアクセス権限を必要最小限にする。

問18　1 台のサーバと複数台のクライアントが，1G 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 6M 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，1G ビット／秒＝10^9 ビット／秒，1M バイト＝10^6 バイトとする。

ア　10　　イ　625　　ウ　1,250　　エ　5,000

問19　スパニングツリープロトコルが適用されている複数のブリッジから成るネットワークにおいて，任意の一つのリンクの両端のブリッジのうち，ルートブリッジまでの経路コストが小さいブリッジの側にあるポートを何と呼ぶか。

ア　アクセスポート（Access Port）　　イ　代表ポート（Designated Port）
ウ　トランクポート（Trunk Port）　　エ　ルートポート（Root Port）

問20　サブネット 192.168.10.0/24 において使用できる 2 種類のブロードキャストアドレス 192.168.10.255 と 255.255.255.255 とに関する記述のうち，適切なものはどれか。

ア　192.168.10.255 と 255.255.255.255 とは，ともにサブネット内のブロードキャストに使用される。
イ　192.168.10.255 はサブネットの外からのブロードキャストだけに使用され，サブネット内のブロードキャストには使用できない。
ウ　255.255.255.255 は互換性のために残されており，ブロードキャストには 192.168.10.255 を使用することが推奨されている。
エ　255.255.255.255 はサブネットの外へのブロードキャストだけに使用され，サブネット内のブロードキャストには使用できない。

問21　次の SQL 文を A 表の所有者が発行したときの，利用者 B への A 表に関する権限の付与を説明したものはどれか。

```
GRANT ALL PRIVILEGES ON A TO B WITH GRANT OPTION
```

ア　SELECT 権限，UPDATE 権限，INSERT 権限，DELETE 権限などの全ての権限，及びそれらの付与権を付与する。

イ　SELECT 権限，UPDATE 権限，INSERT 権限，DELETE 権限などの全ての権限を付与するが，それらの付与権は付与しない。

ウ　SELECT 権限，UPDATE 権限，INSERT 権限，DELETE 権限は付与しないが，それらの付与権だけを付与する。

エ　SELECT 権限，及び SELECT 権限の付与権を付与するが，UPDATE 権限，INSERT 権限，DELETE 権限，及びそれらの付与権は付与しない。

問22　IoT 機器のペネトレーションテスト（Penetration Test）の説明として，適切なものはどれか。

ア　開発の最終段階に，IoT 機器と通信対象となるサーバ及びネットワーク全体の動作が仕様書どおりであることをテストする。

イ　回路図，ソースコードなどのシステムの内部構造を参照して，仕様確認のためのテストを行う。

ウ　恒温恒湿器を用いて，要求仕様で定められた温湿度条件で動作するかどうか，耐久性はどうかをテストする。

エ　ネットワーク，バス，デバッグインタフェースなどの脆弱性を利用して，IoT 機器への攻撃と侵入を試みるテストを行う。

問23　プログラムの著作権管理上，不適切な行為はどれか。

ア　公開されているプロトコルに基づいて，他社が販売しているソフトウェアと同等の機能をもつソフトウェアを独自に開発して販売した。

イ　使用，複製及び改変する権利を付与するというソースコード使用許諾契約を締結した上で，許諾対象のソフトウェアを改変して製品に組み込み，当該許諾契約の範囲内で製品を販売した。

ウ　ソフトウェアハウスと使用許諾契約を締結し，契約上は複製権の許諾は受けていないが，使用許諾を受けたソフトウェアにはプロテクトが掛けられていたので，そのプロテクトを外し，バックアップのために複製した。

エ　他人のソフトウェアを正当な手段で入手し，試験又は研究のために逆コンパイルを行った。

問24　サービスマネジメントにおける問題管理において実施する活動はどれか。

ア　インシデントの発生後に暫定的にサービスを復旧させ，業務を継続できるようにする。

イ　インシデントの発生後に未知の根本原因を特定し，恒久的な解決策を策定する。

ウ　インシデントの発生に備えて，復旧のための設計をする。

エ　インシデントの発生を記録し，関係する部署に状況を連絡する。

問25　システム監査基準（平成 30 年）に基づくシステム監査において，リスクに基づく監査計画の策定（リスクアプローチ）で考慮すべき事項として，適切なものはどれか。

ア　監査対象の不備を見逃して監査の結論を誤る監査リスクを完全に回避する監査計画を策定する。

イ　情報システムリスクの大小にかかわらず，全ての監査対象に対して一律に監査資源を配分する。

ウ　情報システムリスクは，情報システムに係るリスクと，情報の管理に係るリスクの二つに大別されることに留意する。

エ　情報システムリスクは常に一定ではないことから，情報システムリスクの特性の変化及び変化がもたらす影響に留意する。

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。

午