SC

令和７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　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 暗号リストには運用監視暗号リストがあり，それ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 暗号リストには証明書失効リストがあり，それ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 暗号リストには推奨候補暗号リストがあり，それ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 暗号リストには電子政府推奨暗号リストがあり，それ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　PQC（Post-Quantum Cryptography）はどれか。

ア　量子コンピュータを使うことによって，従来のコンピュータを使うときと比べて暗号化の処理速度を飛躍的に向上させることができる暗号技術

イ　量子コンピュータを使うことによっても従来のコンピュータを使うことによっても，暗号化の処理に掛かる処理時間を一定にできる暗号技術

ウ　量子コンピュータを使った攻撃では，従来のコンピュータを使った攻撃と比べて解読時間が大幅に短くなる可能性のある暗号技術

エ　量子コンピュータを使った攻撃に対しても従来のコンピュータを使って安全性を確保できる暗号技術

問４　PKI（公開鍵基盤）を構成するRA（Registration Authority）の役割はどれか。

ア　デジタル証明書にデジタル署名を付与する。

イ　デジタル証明書に紐付けられた属性証明書を発行する。

ウ　デジタル証明書の失効リストを管理し，デジタル証明書の有効性を確認する。

エ　本人確認を行い，デジタル証明書の発行申請の承認又は却下を行う。

問５　AIに対するモデルインバージョン攻撃に該当するものはどれか。

ア　AI モデルに対して入力データを調整しながら出力結果の取得を繰り返し行って解析し，学習に用いた元のデータを推測する。

イ　AI モデルに対して複数のデータを入力して得られた出力結果を観察することによって，当該AIモデルを模倣し，同等の性能をもつAIモデルを得る。

ウ　学習時のデータセットに悪意あるデータを混入し，誤った学習をさせる。

エ　何らかの方法で AI の実行ファイルを入手し，逆アセンブルや逆コンパイルによってAIのソースコードを得る。

問６　XML デジタル署名の特徴はどれか。

ア　XML デジタル署名の構文には，CMS（Cryptographic Message Syntax）が用いられる。

イ　XML 文書中のエレメントに対するデタッチ署名（Detached Signature）を作成し，同じ XML 文書に含めることができる。

ウ　エンベロープピング署名（Enveloping Signature）では，一つの署名対象に複数の署名を付与する。

エ　署名対象と署名アルゴリズムは ASN.1 によって記述する。

問７　送信元 IP アドレスが A，送信元ポート番号が 80/tcp，宛先 IP アドレスがホストに割り振られていない未使用の IP アドレスである SYN/ACK パケットを大量に観測した場合，推定できる攻撃はどれか。

ア　IP アドレス A を攻撃先とするサービス妨害攻撃

イ　IP アドレス A を攻撃先とするパスワードリスト攻撃

ウ　IP アドレス A を攻撃元とするサービス妨害攻撃

エ　IP アドレス A を攻撃元とするパスワードリスト攻撃

問８　ドメインフロンティングを悪用した攻撃の例として，適切なものはどれか。

ア　マルウェアが，CDN の機能を悪用し，実際の通信先を隠蔽して攻撃者のサーバに接続する。

イ　マルウェアが，DNS キャッシュサーバに偽の DNS 情報を蓄積させる。

ウ　マルウェアが，送信元 IP アドレスを攻撃対象に偽装した DNS リクエストを多数の DNS キャッシュサーバに送信し，攻撃対象のサーバをダウンさせる。

エ　マルウェアが，ドメイン情報を管理しているサイトに不正にアクセスし，ドメイン情報を書き換える。

問９　情報理論的安全性に基づく暗号技術はどれか。

ア　DH 鍵共有　　イ　RSA 暗号

ウ　楕円曲線暗号　　エ　ワンタイムパッド

問10　認証デバイスに関する記述のうち，適切なものはどれか。

ア　USB メモリにデジタル証明書を組み込み，認証デバイスとする場合は，その USB メモリを接続する PC の MAC アドレスをデジタル証明書に組み込む必要がある。

イ　成人の虹彩を用いる虹彩認証では，認証デバイスで用いる虹彩パターンの更新がほとんど不要である。

ウ　静電容量方式の指紋認証デバイスは，LED 照明を設置した室内では正常に認証できない可能性が高い。

エ　認証に利用する接触型 IC カードは，カード内のコイルの誘導起電力を利用している。

問11　NIST SP 800-63-3 で定義されている Identity Proofing に該当するものはどれか。

ア　システムに利用者を登録する際に，利用者本人と写真付き身分証とを照合し，確認する。

イ　システムに利用者を登録する際に，利用者本人の希望する利用者 ID が既に別の利用者に利用されていないかどうかを確認する。

ウ　利用者がシステムにログインした際に，システムから利用者に電子メールを送信し，ログインしたことを利用者本人に確認させる。

エ　利用者がシステムにログインする際に，利用者の入力した利用者 ID 及びパスワードとシステムに登録されている情報とを照合し，利用者本人かどうかを確認する。

問12　MITRE の役割に該当するものはどれか。

ア　CVE の事務局であり，サイバー攻撃のプロセスを記述したナレッジベースの公開をする。

イ　サイバーセキュリティフレームワーク，コンピュータセキュリティ関連のガイドライン及び技術仕様などを発行する。

ウ　高いレベルのサイバーセキュリティを EU 加盟諸国が達成するための支援をする。

エ　日本国内で発生した情報セキュリティインシデントの受付，対応支援を技術的な立場から行う。

問13　ある企業で，社内機能として CSIRT，PSIRT，SOC，WHOIS データベースの技術連絡担当組織があるとき，自社製品の脆弱性に起因するリスクに対応するべき社内機能はどれか。

ア　CSIRT

イ　PSIRT

ウ　SOC

エ　WHOIS データベースの技術連絡担当組織

問14　UEBA の機能はどれか。

ア　指紋，静脈などの身体的特徴によって本人確認を行う。

イ　情報への論理的アクセスを制御する。

ウ　データを USB メモリに格納する際に暗号化する。

エ　利用者や機器の異常な振る舞いを検知する。

問15　CSPM（Cloud Security Posture Management）の機能はどれか。

ア　クラウドサービス上に構築したシステムのファイルを継続的に監視し，マルウェア感染を検知する。

イ　クラウドサービスの設定を継続的に監視し，不適切な設定を検知する。

ウ　クラウドサービスへのアクセスを継続的に監視し，不正アクセスを遮断する。

エ　組織のファイルサーバのデータを継続的に監視し，重要データを暗号化してクラウドサービスのストレージにバックアップを格納する。

問16　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，HTTP レスポンスボディに含めた秘密の値と，Web ブラウザから送付される値とを，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“<”，“>”などの特殊文字を，“<”，“>”などの文字列に置き換える。

問17　無線 LAN で使用される規格 IEEE 802.1X が規定しているものはどれか。

ア　アクセスポイントが EAP を使用して，クライアントを認証する枠組み

イ　アクセスポイントが認証局と連携し，パスワードをセッションごとに生成する仕組み

ウ　無線 LAN に接続する機器のセキュリティ対策に関する WPS の仕様

エ　無線 LAN の信号レベルで衝突を検知する CSMA/CD 方式の仕様

問18　JavaScript などのスクリプト言語を使って，Web ブラウザに組み込まれているサーバとの非同期通信機能を利用する技術であり，地図の高速なスクロールや，キーボード入力に合わせた検索候補の逐次表示を実現するものはどれか。

ア　Ajax　　イ　CSS　　ウ　DOM　　エ　SAX

問19　二つのルーティングプロトコル RIP-2 と OSPF とを比較したとき，OSPF だけに当てはまる特徴はどれか。

ア　可変長サブネットマスクに対応している。
イ　リンク状態のデータベースを使用している。
ウ　ルーティング情報の更新にマルチキャストを使用している。
エ　ルーティング情報の更新を 30 秒ごとに行う。

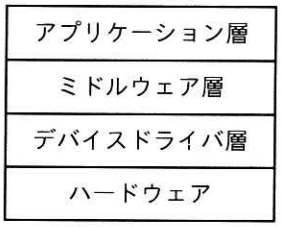
問20　HTTP のステータスコードに関する説明のうち，適切なものはどれか。

ア　100 番台は，リクエストを受けたサーバ側でエラーが発生したことを意味する。
イ　200 番台は，リクエスト内容に不備があるので，エラーが発生したことを意味する。
ウ　300 番台は，完了するためにリダイレクトなど更なる動作が必要なことを意味する。
エ　400 番台は，リクエストがサーバに正常に受信され，処理が完了したことを意味する。

問21　DBMS がトランザクションのコミット処理を完了するタイミングはどれか。

ア　アプリケーションプログラムによるデータ更新命令完了時点
イ　チェックポイント処理完了時点
ウ　ログバッファへのコミット情報書込み完了時点
エ　ログファイルへのコミット情報書込み完了時点

問22　図のような階層構造で設計された組込みシステムがある。このシステムの開発プロジェクトにおいて，デバイスドライバ層の単体テスト工程が未終了で，アプリケーション層及びミドルウェア層の単体テストが先に終了した。この段階で行えるソフトウェア結合テストの方式として，適切なものはどれか。



ア　サンドイッチテスト　　イ　トップダウンテスト
ウ　ビッグバンテスト　　エ　ボトムアップテスト

問23　商用目的で開発するソフトウェアの開発請負契約書には，企業間で様々な事項を取り決めておく必要がある。この開発請負契約書に取決めがない場合に，ソフトウェアの著作権の帰属先に関する説明として，適切なものはどれか。ここで，ソフトウェアは注文者から委託された請負人が開発するものとする。

ア　請負人，注文者のどちらにも帰属しない。
イ　請負人と注文者の両方に帰属する。
ウ　請負人に帰属する。
エ　注文者に帰属する。

問24　サービス提供時間帯が毎日0時から24時までのITサービスにおいて，ある年の4月1日0時から6月30日24時までのサービス停止状況は表のとおりであった。システムバージョンアップ作業に伴う停止時間は，サービス提供時間に含めないことが顧客との間で合意されている。4月1日から6月30日までのITサービスのサービス可用性は何%か。ここで，サービス可用性（%）は小数第3位を四捨五入するものとする。

〔サービス停止状況〕

停止理由	停止時間
システムバージョンアップ作業に伴う停止	5月2日22時から5月6日10時までの84時間
ハードウェア故障に伴う停止	6月26日10時から20時までの10時間

ア　95.52　　イ　95.70　　ウ　99.52　　エ　99.63

問25　システム監査基準（令和５年）に基づくシステム監査において，リスク評価に基づいた監査計画の策定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　システム監査におけるリスク・アプローチでは，各監査対象に対して均等に監査資源を配分する。

ウ　システム監査に係るリスクのうち，監査対象に対するリスクは，統制リスクと残存リスクの二つに大別される。

エ　組織体内外の環境変化によってリスクが相当程度変化した場合には，監査計画の見直しを検討し，必要に応じて変更する。

〔 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

   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。