SC

令和６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　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，毎回異なる値を HTTP レスポンスボディに含め，Web ブラウザからのリクエストごとに送付されるその値を，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2　送信者から受信者にメッセージ認証符号（MAC：Message Authentication Code）を付与したメッセージを送り，次に受信者が第三者に転送した。そのときの MAC に関する記述のうち，適切なものはどれか。ここで，共通鍵は送信者と受信者だけが知っており，送信者と受信者のそれぞれの公開鍵は第三者を含めた3名が知っているものとする。

ア　MAC は，送信者がメッセージと共通鍵を用いて生成する。MAC を用いると，受信者がメッセージの完全性を確認できる。

イ　MAC は，送信者がメッセージと共通鍵を用いて生成する。MAC を用いると，第三者が送信者の真正性を確認できる。

ウ　MAC は，送信者がメッセージと受信者の公開鍵を用いて生成する。MAC を用いると，第三者がメッセージの完全性を確認できる。

エ　MAC は，送信者がメッセージと送信者の公開鍵を用いて生成する。MAC を用いると，受信者が送信者の真正性を確認できる。

問３　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(ひも)づ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４　標準化団体OASISが，Webサイトなどを運営するオンラインビジネスパートナー間で認証，属性及び認可の情報を安全に交換するために策定したものはどれか。

ア　SAML　　イ　SOAP　　ウ　XKMS　　エ　XML Signature

問５　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６　X.509 における CRL に関する記述のうち，適切なものはどれか。

ア　RFC 5280 では，認証局は，発行したデ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。

イ　Web サイトの利用者の Web ブラウザは，その Web サイトにサーバ証明書を発行した認証局の公開鍵が 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。

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

エ　認証局は，有効期限内のデジタル証明書が失効されたとき，そのシリアル番号を CRL に記載する。

問７　ISMAP-LIU クラウドサービス登録規則（令和 6 年 3 月 1 日最終改定）での ISMAP-LIU に関する記述として，適切なものはどれか。

ア　JIS Q 27001 に加え，JIS Q 27017 に規定されたクラウドサービス固有の管理策が適切に導入，実施されていることも認証する。

イ　アウトソーシング事業者が記述したセキュリティの内部統制に対しても，監査法人が評価手続を実施した結果とその意見を表明する。

ウ　リスクの小さな業務・情報の処理に用いる SaaS サービスを対象とする。

エ　我が国の政府機関などにおける情報セキュリティのベースライン，及びより高い水準の情報セキュリティを確保するための対策事項を規定している。

問８　組織のセキュリティインシデント管理の成熟度を評価するために Open CSIRT Foundation が開発したモデルはどれか。

ア　CMMC　　イ　CMMI　　ウ　SAMM　　エ　SIM3

問９　JVN などの脆弱性対策ポータルサイトで採用されている CWE はどれか。

ア　IT 製品の脆弱性を評価する手法
イ　製品を識別するためのプラットフォーム名の一覧
ウ　セキュリティに関連する設定項目を識別するための識別子
エ　ソフトウェア及びハードウェアの脆弱性の種類の一覧

問10　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11　セキュリティ対策として，CASB を利用した際の効果はどれか。

ア　クラウドサービスカスタマの管理者が，従業員が利用しているクラウドサービスに対して，CASB を利用して脆弱性診断を行うことによって，脆弱性を特定できる。
イ　クラウドサービスカスタマの管理者が，従業員が利用しているクラウドサービスに対して，CASB を利用して利用状況の可視化を行うことによって，許可を得ずにクラウドサービスを利用している者を特定できる。
ウ　クラウドサービスプロバイダが，運用しているクラウドサービスに対して，CASB を利用して DDoS 攻撃対策を行うことによって，クラウドサービスの可用性低下を緩和できる。
エ　クラウドサービスプロバイダが，クラウドサービスを運用している施設に対して，CASB を利用して入退室管理を行うことによって，クラウドサービス運用環境への物理的な不正アクセスを防止できる。

問12　不特定多数の利用者に無料で開放されている公衆無線LANサービスのアクセスポイントと端末で利用される仕様として，Wi-Fi Alliance の Enhanced Open によって新規に規定されたものはどれか。

ア　端末でのパスワードの入力で，端末からアクセスポイントへの接続が可能となる仕様

イ　端末でのパスワードの入力で，端末とアクセスポイントとの通信の暗号化が可能となる仕様

ウ　端末でのパスワードの入力なしに，端末からアクセスポイントへの接続が可能となる仕様

エ　端末でのパスワードの入力なしに，端末とアクセスポイントとの通信の暗号化が可能となる仕様

問13　HTTP Strict Transport Security (HSTS) の動作はどれか。

ア　HTTP over TLS (HTTPS) によって接続しているとき，接続先のサーバ証明書がEV SSL証明書である場合とない場合で，Webブラウザのアドレス表示部分の表示を変える。

イ　Web サーバからコンテンツをダウンロードするとき，どの文字列が秘密情報かを判定できないように圧縮する。

ウ　Webサーバと Webブラウザとの間の TLS のハンドシェイクにおいて，一度確立したセッションとは別の新たなセッションを確立するとき，既に確立したセッションを使って改めてハンドシェイクを行う。

エ　Web ブラウザは，Web サイトにアクセスすると，以降の指定された期間，当該サイトには全てHTTPSによって接続する。

問14　IEEE 802.1X におけるサプリカントはどれか。

ア　一度の認証で複数のサーバやアプリケーションを利用できる認証システム

イ　クライアント側から送信された認証情報を受け取り，認証を行うシステム

ウ　クライアント側と認証サーバの仲介役となり，クライアント側から送信された認証情報を受け取り，認証サーバに送信するネットワーク機器

エ　認証を要求するクライアント側の装置やソフトウェア

問15　DNS において DNS CAA (Certification Authority Authorization) レコードを設定することによるセキュリティ上の効果はどれか。

ア　Web サイトにアクセスしたときの Web ブラウザに鍵マークが表示されていれば当該サイトが安全であることを，利用者が確認できる。

イ　Web サイトにアクセスする際の URL を短縮することによって，利用者の URL の誤入力を防ぐ。

ウ　電子メールを受信するサーバでスパムメールと誤検知されないようにする。

エ　不正なサーバ証明書の発行を防ぐ。

問16　電子メール又はその通信を暗号化する三つのプロトコルについて，公開鍵を用意する単位の組合せのうち，適切なものはどれか。

	PGP	S/MIME	SMTP over TLS
ア	メールアドレスごと	メールアドレスごと	メールサーバごと
イ	メールアドレスごと	メールサーバごと	メールアドレスごと
ウ	メールサーバごと	メールアドレスごと	メールアドレスごと
エ	メールサーバごと	メールサーバごと	メールサーバごと

問17　ソフトウェアの脆弱性管理のためのツールとしても利用される SBOM（Software Bill of Materials）はどれか。

ア　ソフトウェアの脆弱性に対する，ベンダーに依存しないオープンで汎用的な深刻度の評価方法

イ　ソフトウェアのセキュリティアップデートを行うときに推奨される管理プロセス，組織体制などをまとめたガイドライン

ウ　ソフトウェアを構成するコンポーネント，互いの依存関係などのリスト

エ　米国の非営利団体 MITRE によって策定された，ソフトウェアにおけるセキュリティ上の弱点の種類を識別するための基準

問18　TCP ヘッダーに含まれる情報はどれか。

ア　宛先ポート番号　　イ　送信元 IP アドレス

ウ　パケット生存時間（TTL）　　エ　プロトコル番号

問19　TCP のサブミッションポート（ポート番号 587）の説明として，適切なものはどれか。

ア　FTP サービスで，制御用コネクションのポート番号 21 とは別にデータ転送用に使用する。

イ　Web サービスで，ポート番号 80 の HTTP 要求とは別に，サブミットボタンをクリックした際の入力フォームのデータ送信に使用する。

ウ　コマンド操作の遠隔ログインで，通信内容を暗号化するために TELNET のポート番号 23 の代わりに使用する。

エ　電子メールサービスで，迷惑メール対策などのために SMTP のポート番号 25 の代わりに使用する。

問20　Web サーバから送信される HTTP ヘッダーのうち，Web サーバからの応答の内容を，Web ブラウザやプロキシサーバなどのキャッシュに保持させないようにするものはどれか。

ア　Cache-Control: no-cache

イ　Cache-Control: no-store

ウ　Cache-Control: private

エ　Cache-Control: public

問21　“人事”表に対して次の SQL 文を実行したとき，結果として得られる社員番号はどれか。

人事

社員番号	所属	勤続年数	年齢
1	総務部	13	31
2	総務部	5	28
3	人事部	11	28
4	営業部	8	30
5	総務部	7	29

〔SQL 文〕

```
SELECT 社員番号 FROM 人事
       WHERE (勤続年数 > 10 OR 年齢 > 28)
       AND 所属 = '総務部'
```

ア　1, 2, 5　　イ　1, 3, 4, 5

ウ　1, 3, 5　　エ　1, 5

問22　仕様書やソースコードについて，作成者を含めた複数人で，記述されたシステムやソフトウェアの振る舞いを机上でシミュレートして，問題点を発見する手法はどれか。

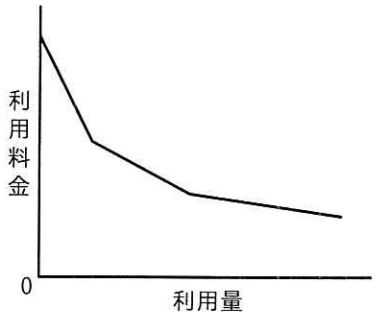
ア　ウォークスルー　　イ　サンドイッチテスト
ウ　トップダウンテスト　　エ　並行シミュレーション

問23　ソフトウェアの品質を確保するための検証に形式手法を用いる。このとき行う検証方法の説明として，適切なものはどれか。

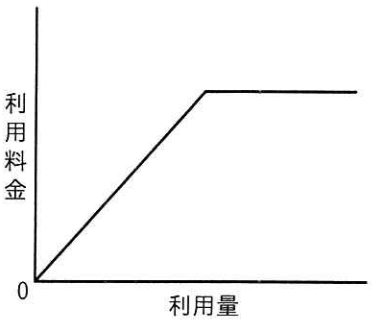
ア　進行役（モデレーター），記録役などの役割を決めた複数人で，成果物に欠陥がないかどうかを検証する。
イ　プログラムの内部構造とは無関係に，プログラムが仕様どおりに機能するかどうかを検証する。
ウ　プログラムの内部構造に着目し，プログラムが仕様どおりに動作するかどうかを検証する。
エ　明確で厳密な意味を定義することができる言語を用いてソフトウェアの仕様を記述して，満たすべき性質と仕様とが整合しているかどうかを論理的に検証する。

問24　IT サービスにおけるコンピュータシステムの利用に対する課金を逓減課金方式で行うときのグラフはどれか。

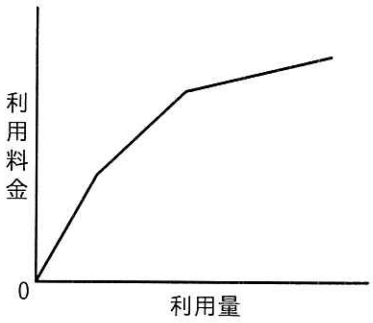
ア



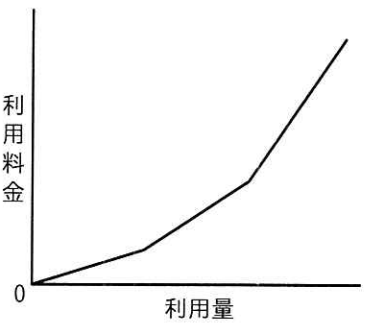
イ



ウ



エ



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)”における，IT に係る全般統制に該当するものとして，最も適切なものはどれか。

ア　アプリケーションプログラムの例外処理（エラー）の修正と再処理

イ　業務別マスタ・データの維持管理

ウ　システムの開発，保守に係る管理

エ　入力情報の完全性，正確性，正当性等を確保する統制

〔 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。