SC

令和３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　リフレクタ攻撃に悪用されることの多いサービスの例はどれか。

ア　DKIM，DNSSEC，SPF

イ　DNS，Memcached，NTP

ウ　FTP，L2TP，Telnet

エ　IPsec，SSL，TLS

問２　PKI を構成する OCSP を利用する目的はどれか。

ア　誤って破棄してしまった秘密鍵の再発行処理の進捗状況を問い合わせる。

イ　ディジタル証明書から生成した鍵情報の交換が OCSP クライアントと OCSP レスポンダの間で失敗した際，認証状態を確認する。

ウ　ディジタル証明書の失効情報を問い合わせる。

エ　有効期限が切れたディジタル証明書の更新処理の進捗状況を確認する。

問３　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４　DoS 攻撃の一つである Smurf 攻撃はどれか。

ア　ICMP の応答パケットを大量に発生させ，それが攻撃対象に送られるようにする。

イ　TCP 接続要求である SYN パケットを攻撃対象に大量に送り付ける。

ウ　サイズが大きい UDP パケットを攻撃対象に大量に送り付ける。

エ　サイズが大きい電子メールや大量の電子メールを攻撃対象に送り付ける。

問５　サイドチャネル攻撃はどれか。

ア　暗号化装置における暗号化処理時の消費電力などの測定や統計処理によって，当該装置内部の秘密情報を推定する攻撃

イ　攻撃者が任意に選択した平文とその平文に対応した暗号文から数学的手法を用いて暗号鍵を推測し，同じ暗号鍵を用いて作成された暗号文を解読する攻撃

ウ　操作中の人の横から，入力操作の内容を観察することによって，利用者 ID とパスワードを盗み取る攻撃

エ　無線 LAN のアクセスポイントを不正に設置し，チャネル間の干渉を発生させることによって，通信を妨害する攻撃

問6　ステートフルパケットインスペクション方式のファイアウォールの特徴はどれか。

ア　Web クライアントと Web サーバとの間に配置され，リバースプロキシサーバとして動作する方式であり，Web クライアントからの通信を目的の Web サーバに中継する際に，受け付けたパケットに不正なデータがないかどうかを検査する。

イ　アプリケーションプロトコルごとにプロキシソフトウェアを用意する方式であり，クライアントからの通信を目的のサーバに中継する際に，通信に不正なデータがないかどうかを検査する。

ウ　特定のアプリケーションプロトコルだけを通過させるゲートウェイソフトウェアを利用する方式であり，クライアントからのコネクションの要求を受け付け，目的のサーバに改めてコネクションを要求することによって，アクセスを制御する。

エ　パケットフィルタリングを拡張した方式であり，過去に通過したパケットから通信セッションを認識し，受け付けたパケットを通信セッションの状態に照らし合わせて通過させるか遮断するかを判断する。

問7　NIST が制定した，AES における鍵長の条件はどれか。

ア　128 ビット，192 ビット，256 ビットから選択する。

イ　256 ビット未満で任意に指定する。

ウ　暗号化処理単位のブロック長よりも 32 ビット長くする。

エ　暗号化処理単位のブロック長よりも 32 ビット短くする。

問８　JVN などの脆弱性対策情報ポータルサイトで採用されている CVE（Common Vulnerabilities and Exposures）識別子の説明はどれか。

ア　コンピュータで必要なセキュリティ設定項目を識別するための識別子

イ　脆弱性が悪用されて改ざんされた Web サイトのスクリーンショットを識別するための識別子

ウ　製品に含まれる脆弱性を識別するための識別子

エ　セキュリティ製品の種別を識別するための識別子

問９　サイバー情報共有イニシアティブ（J-CSIP）の説明として，適切なものはどれか。

ア　サイバー攻撃対策に関する情報セキュリティ監査を参加組織間で相互に実施して，監査結果を共有する取組

イ　参加組織がもつデータを相互にバックアップして，サイバー攻撃から保護する取組

ウ　セキュリティ製品のサイバー攻撃に対する有効性に関する情報を参加組織が取りまとめ，その情報を活用できるように公開する取組

エ　標的型サイバー攻撃などに関する情報を参加組織間で共有し，高度なサイバー攻撃対策につなげる取組

問10　DNSにおいてDNS CAA（Certification Authority Authorization）レコードを使う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11　セキュリティ対策として，CASB（Cloud Access Security Broker）を利用した際の効果はどれか。

ア　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 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。

イ　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。

ウ　クラウドサービス利用組織の管理者が，組織で利用しているクラウドサービスに対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。

エ　クラウドサービス利用組織の管理者が，組織の利用者が利用している全てのクラウドサービスの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。

問12　安全な Web アプリケーションの作り方について，攻撃と対策の適切な組合せはどれか。

	攻撃	対策
ア	SQL インジェクション	SQL 文の組立てに静的プレースホルダを使用する。
イ	クロスサイトスクリプティング	任意の外部サイトのスタイルシートを取り込めるようにする。
ウ	クロスサイトリクエストフォージェリ	リクエストに GET メソッドを使用する。
エ	セッションハイジャック	利用者ごとに固定のセッション ID を使用する。

問13　マルウェアの検出手法であるビヘイビア法を説明したものはどれか。

ア　あらかじめ特徴的なコードをパターンとして登録したマルウェア定義ファイルを用いてマルウェア検査対象と比較し，同じパターンがあればマルウェアとして検出する。

イ　マルウェアに感染していないことを保証する情報をあらかじめ検査対象に付加しておき，検査時に不整合があればマルウェアとして検出する。

ウ　マルウェアの感染が疑わしい検査対象のハッシュ値と，安全な場所に保管されている原本のハッシュ値を比較し，マルウェアを検出する。

エ　マルウェアの感染や発病によって生じるデータの読込みの動作，書込みの動作，通信などを監視して，マルウェアを検出する。

問14　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15　HSTS（HTTP Strict Transport Security）の説明はどれか。

ア　HSTS を利用する Web サイトに Web ブラウザが HTTP でアクセスした場合，Web ブラウザから当該サイトへのその後のアクセスを強制的に HTTP over TLS（HTTPS）にする。

イ　HSTS を利用する Web サイトに Web ブラウザが HTTP でアクセスした場合，Web ページの文書やスクリプトについて，あるオリジンから読み込まれたリソースから他のオリジンのリソースにアクセスできないように制限する。

ウ　HTTPS で通信が保護されている場合にだけ，cookie の属性によらず強制的に cookie を送信する。

エ　信頼性が高いサーバ証明書を有する Web サイトとの HTTPS 通信では，Web ブラウザに鍵マークを表示する。

問16　内部ネットワークにある PC からインターネット上の Web サイトを参照するときは，DMZ にある VDI（Virtual Desktop Infrastructure）サーバ上の仮想マシンに PC からログインし，仮想マシン上の Web ブラウザを必ず利用するシステムを導入する。インターネット上の Web サイトから内部ネットワークにある PC へのマルウェアの侵入，及びインターネット上の Web サイトへの PC 内のファイルの流出を防止する効果を得るために必要な条件はどれか。

ア　PC と VDI サーバ間は，VDI の画面転送プロトコル及びファイル転送を利用する。
イ　PC と VDI サーバ間は，VDI の画面転送プロトコルだけを利用する。
ウ　VDI サーバが，プロキシサーバとして HTTP 通信を中継する。
エ　VDI サーバが，プロキシサーバとして VDI の画面転送プロトコルだけを中継する。

問17　RFC 8110 に基づいたものであり，公衆無線 LAN などでパスフレーズなどでの認証なしに，端末とアクセスポイントとの間の無線通信を暗号化するものはどれか。

ア　Enhanced Open　　イ　FIDO2
ウ　WebAuthn　　エ　WPA3

問18　ETSI（欧州電気通信標準化機構）が提唱する NFV（Network Functions Virtualisation）に関する記述のうち，適切なものはどれか。

ア　ONF（Open Networking Foundation）が提唱する SDN（Software-Defined Networking）を用いて，仮想化を実現する。

イ　OpenFlow コントローラや OpenFlow スイッチなどの OpenFlow プロトコルの専用機器だけを使ってネットワークを構築する。

ウ　ルータ，ファイアウォールなどのネットワーク機能を，汎用サーバを使った仮想マシン上のソフトウェアで実現する。

エ　ロードバランサ，スイッチ，ルータなどの専用機器を使って，VLAN，VPN などの仮想ネットワークを実現する。

問19　スイッチングハブ同士を接続する際に，複数のポートを束ねて一つの論理ポートとして扱う技術はどれか。

ア　MIME　　イ　MIMO

ウ　マルチパート　　エ　リンクアグリゲーション

問20　IPv4 ネットワークにおける IP アドレス 127.0.0.1 に関する記述として，適切なものはどれか。

ア　DHCP が使用できないときに自動生成される IP アドレスとして使用される。

イ　全ホストに対するブロードキャストアドレスとして使用される。

ウ　単一のコンピュータ上で動作するプログラム同士が通信する際に使用される。

エ　デフォルトゲートウェイのアドレスとして使用される。

問21　複数のバッチ処理を並行して動かすとき，デッドロックの発生をできるだけ回避したい。バッチ処理の設計ガイドラインのうち，適切なものはどれか。

ア　参照するレコードにも，専有ロックを掛けるように設計する。

イ　大量データに同じ処理を行うバッチ処理は，まとめて一つのトランザクションとして処理するように設計する。

ウ　トランザクション開始直後に，必要なレコード全てに専有ロックを掛ける。ロックに失敗したレコードには，しばらく待って再度ロックを掛けるように設計する。

エ　複数レコードを更新するときにロックを掛ける順番を決めておき，全てのバッチ処理がこれに従って処理するように設計する。

問22　JIS X 25010:2013（システム及びソフトウェア製品の品質要求及び評価（SQuaRE）－システム及びソフトウェア品質モデル）で定義されたシステム及び／又はソフトウェア製品の品質特性に関する説明のうち，適切なものはどれか。

ア　機能適合性とは，明示された状況下で使用するとき，明示的ニーズ及び暗黙のニーズを満足させる機能を，製品又はシステムが提供する度合いのことである。

イ　信頼性とは，明記された状態（条件）で使用する資源の量に関係する性能の度合いのことである。

ウ　性能効率性とは，明示された利用状況において，有効性，効率性及び満足性をもって明示された目標を達成するために，明示された利用者が製品又はシステムを利用することができる度合いのことである。

エ　保守性とは，明示された時間帯で，明示された条件下に，システム，製品又は構成要素が明示された機能を実行する度合いのことである。

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　プログラムを書く前にテストコードを記述する。

問24　ディスク障害時に，フルバックアップを取得してあるテープからディスクにデータを復元した後，フルバックアップ取得時以降の更新後コピーをログから反映させてデータベースを回復する方法はどれか。

ア　チェックポイントリスタート　　イ　リブート
ウ　ロールバック　　エ　ロールフォワード

問25　ソフトウェア開発プロセスにおけるセキュリティを確保するための取組について，JIS Q 27001:2014（情報セキュリティマネジメントシステム－要求事項）の附属書Aの管理策に照らして監査を行った。判明した状況のうち，監査人が，監査報告書に指摘事項として記載すべきものはどれか。

ア　ソフトウェア開発におけるセキュリティ機能の試験は，開発期間が終了した後に実施している。
イ　ソフトウェア開発は，セキュリティ確保に配慮した開発環境において行っている。
ウ　ソフトウェア開発を外部委託している場合，外部委託先による開発活動の監督・監視において，セキュリティ確保の観点を考慮している。
エ　パッケージソフトウェアを活用した開発において，セキュリティ確保の観点から，パッケージソフトウェアの変更は必要な変更に限定している。

〔 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。