SC

令和５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　Web アプリケーションソフトウェアの脆弱性を悪用する攻撃手法のうち，入力した文字列が PHP の exec 関数などに渡されることを利用し，不正にシェルスクリプトを実行させるものは，どれに分類されるか。

ア　HTTP ヘッダインジェクション
イ　OS コマンドインジェクション
ウ　クロスサイトリクエストフォージェリ
エ　セッションハイジャック

問２　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　AEAD（Authenticated Encryption with Associated Data）とハッシュアルゴリズムの組みで構成されている。
イ　TLS 1.2 で規定されている共通鍵暗号 AES-CBC をサポート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。
ウ　Wi-Fi アライアンスにおいて規格化されている。
エ　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。

問３　VA（Validation Authority）の役割はどれか。

ア　属性証明書の発行を代行する。
イ　デジタル証明書にデジタル署名を付与する。
ウ　デジタル証明書の失効状態についての問合せに応答する。
エ　本人確認を行い，デジタル証明書の発行を指示する。

問４　XML デジタル署名の特徴として，適切なものはどれか。

ア　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。

イ　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。

ウ　署名の書式として，CMS（Cryptographic Message Syntax）を用いる。

エ　デジタル署名では，署名対象と署名アルゴリズムを ASN.1 によって記述する。

問５　クリプトジャッキングに該当するものはどれか。

ア　PC に不正アクセスし，その PC のリソースを利用して，暗号資産のマイニングを行う攻撃

イ　暗号資産取引所の Web サイトに不正ログインを繰り返し，取引所の暗号資産を盗む攻撃

ウ　巧妙に細工した電子メールのやり取りによって，企業の担当者をだまし，攻撃者の用意した暗号資産口座に送金させる攻撃

エ　マルウェア感染した PC に制限を掛けて利用できないようにし，その制限の解除と引換えに暗号資産を要求する攻撃

問６　マルウェア Mirai の動作はどれか。

ア　IoT 機器などで動作する Web サーバプログラムの脆弱性を悪用して感染を広げ，Web ページを改ざんし，決められた日時に特定の IP アドレスに対して DDoS 攻撃を行う。

イ　Web サーバプログラムの脆弱性を悪用して企業の Web ページに不正な JavaScript を挿入し，当該 Web ページを閲覧した利用者を不正な Web サイトへと誘導する。

ウ　ファイル共有ソフトを使っている PC 内でマルウェアの実行ファイルを利用者が誤って実行すると，PC 内の情報をインターネット上の Web サイトにアップロードして不特定多数の人に公開する。

エ　ランダムな宛先 IP アドレスを使用して IoT 機器などに感染を広げるとともに，C&C サーバからの指令に従って標的に対して DDoS 攻撃を行う。

問７　インターネットバンキングでの MITB 攻撃による不正送金について，対策として用いられるトランザクション署名の説明はどれか。

ア　携帯端末からの送金取引の場合，金融機関から利用者の登録メールアドレスに送金用のワンタイムパスワードを送信する。

イ　特定認証業務の認定を受けた認証局が署名したデジタル証明書をインターネットバンキングでの利用者認証に用いることによって，ログインパスワードが漏えいした際の不正ログインを防止する。

ウ　利用者が送金取引時に，“送金操作を行う PC とは別のデバイスに振込先口座番号などの取引情報を入力して表示された値”をインターネットバンキングに送信する。

エ　ログイン時に，送金操作を行う PC とは別のデバイスによって，一定時間だけ有効なログイン用のワンタイムパスワードを算出し，インターネットバンキングに送信する。

問８　SAML（Security Assertion Markup Language）の説明はどれか。

ア　Web サーバにある利用者のリソースに，Web サーバに限らない他のサーバが利用者に代わってアクセスすることを許可するための認証プロトコル

イ　異なるインターネットドメイン間でセキュリティ情報を共有してシングルサインオンに利用するための，XML をベースにした標準規格

ウ　利用者 ID として URL 又は XRI（Extensible Resource Identifier）だけを使用することができ，一つの利用者 ID で様々な Web サイトにログインできる仕組み

エ　利用者が文書やデータの属性情報や論理構造を定義する言語である SGML を，インターネット用に最適化したもの

問９　公開鍵基盤における CPS（Certification Practice Statement）に該当するものはどれか。

ア　認証局が発行するデジタル証明書の所有者が策定したセキュリティ宣言

イ　認証局でのデジタル証明書発行手続を代行する事業者が策定したセキュリティ宣言

ウ　認証局の認証業務の運用などに関する詳細を規定した文書

エ　認証局を監査する第三者機関の運用などに関する詳細を規定した文書

問10　総務省及び国立研究開発法人情報通信研究機構（NICT）が 2019 年 2 月から実施している取組“NOTICE”に関する記述のうち，適切なものはどれか。

ア　NICT が運用するダークネット観測網において，マルウェアに感染した IoT 機器から到達するパケットを分析した結果を当該機器の製造者に提供し，国内での必要な対策を促す。

イ　国内のグローバル IP アドレスを有する IoT 機器に対して，容易に推測されるパスワードを入力することなどによって，サイバー攻撃に悪用されるおそれのある機器を調査し，インターネットサービスプロバイダを通じて当該機器の利用者に注意喚起を行う。

ウ　国内の利用者からの申告に基づき，利用者の所有する IoT 機器に対して無料でリモートから，侵入テストや OS の既知の脆弱性の有無の調査を実施し，結果を通知するとともに，利用者が自ら必要な対処ができるよう支援する。

エ　製品のリリース前に，不要にもかかわらず開放されているポートの存在，パスワードの設定漏れなど約 200 項目の脆弱性の有無を調査できるテストベッドを国内の IoT 機器製造者向けに公開し，市場に流通する IoT 機器のセキュリティ向上を目指す。

問11　JIS Q 27000:2019（情報セキュリティマネジメントシステム－用語）の用語に関する記述のうち，適切なものはどれか。

ア　脅威とは，一つ以上の要因によって付け込まれる可能性がある，資産又は管理策の弱点のことである。

イ　脆弱性とは，システム又は組織に損害を与える可能性がある，望ましくないインシデントの潜在的な原因のことである。

ウ　リスク対応とは，リスクの大きさが，受容可能か又は許容可能かを決定するために，リスク分析の結果をリスク基準と比較するプロセスのことである。

エ　リスク特定とは，リスクを発見，認識及び記述するプロセスのことであり，リスク源，事象，それらの原因及び起こり得る結果の特定が含まれる。

問12　脆弱性管理，測定，評価を自動化するためにNISTが策定した基準はどれか。

ア　FIPS (Federal Information Processing Standards)

イ　SCAP (Security Content Automation Protocol)

ウ　SIEM (Security Information and Event Management)

エ　SOAR (Security Orchestration, Automation and Response)

問13　DNSSECに関する記述のうち，適切なものはどれか。

ア　権威DNSサーバが，DNS問合せに対する応答時に，リソースレコードを公開鍵暗号方式で暗号化することによって，通信経路上の盗聴を防ぐ。

イ　権威DNSサーバが，リソースレコードの受信時にデジタル署名を検証することによって，データの作成元の正当性とデータの完全性を確認する。

ウ　リゾルバが，DNS問合せに対する応答時に，リソースレコードを公開鍵暗号方式で暗号化することによって，通信経路上の盗聴を防ぐ。

エ　リゾルバが，リソースレコードの受信時にデジタル署名を検証することによって，データの作成元の正当性とデータの完全性を確認する。

問14　OAuth 2.0 に関する記述のうち，適切なものはどれか。

ア　認可を行うためのプロトコルであり，認可サーバが，アクセスしてきた者が利用者（リソースオーナー）本人であるかどうかを確認するためのものである。

イ　認可を行うためのプロトコルであり，認可サーバが，利用者（リソースオーナー）の許可を得て，サービス（クライアント）に対し，適切な権限を付与するためのものである。

ウ　認証を行うためのプロトコルであり，認証サーバが，アクセスしてきた者が利用者（リソースオーナー）本人であるかどうかを確認するためのものである。

エ　認証を行うためのプロトコルであり，認証サーバが，利用者（リソースオーナー）の許可を得て，サービス（クライアント）に対し，適切な権限を付与するためのものである。

問15　通信の暗号化や利用者の認証の機能をもち，遠隔にあるコンピュータに安全にログインするためのプロトコルはどれか。

ア　L2TP　　イ　LDAP　　ウ　RADIUS　　エ　SSH

問16　電子メールをスマートフォンのメール・アプリケーションプログラムで受信する際のメールサーバとスマートフォンとの間の通信を，メール本文を含めて暗号化するプロトコルはどれか。

ア　APOP　　イ　IMAPS

ウ　POP3　　エ　SMTP Submission

問17　セキュリティ対策として，次の条件の下でデータベース（DB）サーバをDMZから内部ネットワークに移動するような次のネットワーク構成の変更を計画している。このとき，ステートフルパケットフィルタリング型のファイアウォール（FW）において，必要となるフィルタリングルールの変更のうちの一つはどれか。

〔条件〕

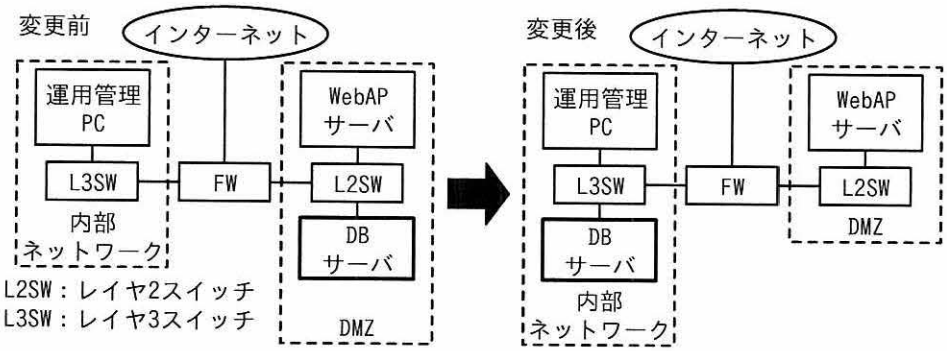
(1) Webアプリケーション（WebAP）サーバを，インターネットに公開し，HTTPSでアクセスできるようにする。

(2) WebAPサーバ上のプログラムだけがDBサーバ上のDBに接続でき，ODBC（Open Database Connectivity）を使用して特定のポート間で通信する。

(3) SSHを使用して各サーバに接続できるのは，運用管理PCだけである。

(4) フィルタリングルールは，必要な通信だけを許可する設定にする。

〔ネットワーク構成の変更〕



	ルールの変更種別	ルール			
		送信元	宛先	サービス	制御
ア	削除	インターネット	WebAPサーバ	HTTPS	許可
イ	削除	運用管理PC	変更前のDBサーバ	SSH	許可
ウ	追加	WebAPサーバ	変更後のDBサーバ	SSH	許可
エ	追加	インターネット	WebAPサーバ	ODBC	許可

問18　クラス C のネットワークを，50 ノードずつ収納できる四つのサブネットに分割した場合のサブネットマスクはどれか。

ア　255.255.255.0　　イ　255.255.255.64

ウ　255.255.255.128　　エ　255.255.255.192

問19　複数ノードから成るグループにマルチキャストでデータを送るときに，宛先として使用できる IP アドレスはどれか。

ア　10.0.1.1　　イ　127.0.1.1

ウ　192.168.1.1　　エ　239.0.1.1

問20　DHCP のクライアントが，サーバから配布された IPv4 アドレスを，クライアント自身のホストアドレスとして設定する際に，そのアドレスが他のホストに使用されていないことを，クライアント自身でも確認することが推奨されている。この確認に使用するプロトコルとして，適切なものはどれか。

ア　ARP　　イ　DNS　　ウ　ICMP　　エ　RARP

問21　DBMS のデータディクショナリはどれか。

ア　DBMS 内部でのソートデータ，サブクエリを展開したデータなど，一時的なデータを格納したもの

イ　障害が発生した場合にバックアップを取った時点まで回復させるため，データベース自体の複製を格納したもの

ウ　データベースに関するユーザー情報，データ構造など，データベース管理情報を格納したもの

エ　ユーザーからの指示によるデータベースの読込み情報，書込み情報などを格納したもの

問22　目的別のサービスが多数連携して動作する大規模な分散型のシステムでは，障害時の挙動を予知することが困難である。このようなシステムにおいて，ステージング環境や本番環境で意図的に障害を引き起こしてシステムの挙動を観察し，発見した問題を修正することを継続的に実施し，システムの耐障害性及びシステム運用の信頼性を高めていく手法はどれか。

ア　DevOps　　イ　Infrastructure as Code

ウ　カオスエンジニアリング　　エ　テスト駆動開発

問23　アジャイル開発手法の説明のうち，スクラムのものはどれか。

ア　コミュニケーション，シンプル，フィードバック，勇気，尊重の五つの価値を基礎とし，テスト駆動型開発，ペアプログラミング，リファクタリングなどのプラクティスを推奨する。

イ　推測（プロジェクト立上げ，適応的サイクル計画），協調（並行コンポーネント開発），学習（品質レビュー，最終QA／リリース）のライフサイクルをもつ。

ウ　プロダクトオーナーなどの役割，スプリントレビューなどのイベント，プロダクトバックログなどの作成物，及びルールから成る。

エ　モデルの全体像を作成した上で，優先度を付けた詳細なフィーチャリストを作成し，フィーチャを単位として計画し，フィーチャごとの設計と構築とを繰り返す。

問24　JIS Q 20000-1:2020（サービスマネジメントシステム要求事項）を適用している組織において，サービスマネジメントシステム（SMS）が次の要求事項に適合している状況にあるか否かに関する情報を提供するために，あらかじめ定めた間隔で組織が実施するものはどれか。

〔要求事項〕

・SMSに関して，組織自体が規定した要求事項

・JIS Q 20000-1:2020の要求事項

ア　監視，測定，分析及び評価　　イ　サービスの報告

ウ　内部監査　　エ　マネジメントレビュー

問25　データベースの直接修正に関して，監査人が，システム監査報告書で報告すべき指摘事項はどれか。ここで，直接修正とは，アプリケーションソフトウェアの機能を経由せずに，特権 ID を使用してデータを追加，変更又は削除することをいう。

ア　更新ログ上は，アプリケーションソフトウェアの機能を経由したデータ更新として記録していた。

イ　事前のデータ変更申請の承認，及び事後のデータ変更結果の承認を行っていた。

ウ　直接修正の作業終了時には，直接修正用の特権 ID を無効にしていた。

エ　利用部門からのデータ変更依頼票に基づいて，システム部門が直接修正を実施していた。

〔 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。