SC

平成29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，読み取れません。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ご注意ください。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**のとおり記入及び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〕　春の情報処理技術者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　AESの特徴はどれか。

ア　鍵長によって，段数が決まる。

イ　段数は，6段以内の範囲で選択できる。

ウ　データの暗号化，復号，暗号化の順に3回繰り返す。

エ　同一の公開鍵を用いて暗号化を3回繰り返す。

問2　SSL/TLSのダウングレード攻撃に該当するものはどれか。

ア　暗号化通信中にクライアントPCからサーバに送信するデータを操作して，強制的にサーバのディジタル証明書を失効させる。

イ　暗号化通信中にサーバからクライアントPCに送信するデータを操作して，クライアントPCのWebブラウザを古いバージョンのものにする。

ウ　暗号化通信を確立するとき，弱い暗号スイートの使用を強制することによって，解読しやすい暗号化通信を行わせる。

エ　暗号化通信を盗聴する攻撃者が，暗号鍵候補を総当たりで試すことによって解読する。

問3　サイドチャネル攻撃の説明はどれか。

ア　暗号アルゴリズムを実装した攻撃対象の物理デバイスから得られる物理量（処理時間や消費電流など）やエラーメッセージから，攻撃対象の機密情報を得る。

イ　企業などの機密情報を詐取するソーシャルエンジニアリングの手法の一つであり，不用意に捨てられた機密情報の印刷物をオフィスの紙ごみの中から探し出す。

ウ　通信を行う2者間に割り込んで，両者が交換する情報を自分のものとすり替えることによって，気付かれることなく盗聴する。

エ　データベースを利用するWebサイトに入力パラメタとしてSQL文の断片を与えることによって，データベースを改ざんする。

問4　PC などに内蔵されるセキュリティチップ（TPM：Trusted Platform Module）がもつ機能はどれか。

ア　TPM 間での共通鍵の交換　　　イ　鍵ペアの生成

ウ　ディジタル証明書の発行　　　エ　ネットワーク経由の乱数送信

問5　セッション ID の固定化（Session Fixation）攻撃の手口はどれか。

ア　HTTPS 通信で Secure 属性がない Cookie にセッション ID を格納する Web サイトにおいて，HTTP 通信で送信されるセッション ID を悪意のある者が盗聴する。

イ　URL パラメタにセッション ID を格納する Web サイトにおいて，Referer によってリンク先の Web サイトに送信されるセッション ID が含まれた URL を，悪意のある者が盗用する。

ウ　悪意のある者が正規の Web サイトから取得したセッション ID を，利用者の Web ブラウザに送り込み，利用者がそのセッション ID でログインして，セッションがログイン状態に変わった後，利用者になりすます。

エ　推測が容易なセッション ID を生成する Web サイトにおいて，悪意のある者がセッション ID を推測し，ログインを試みる。

問6　DNS 水責め攻撃（ランダムサブドメイン攻撃）の手口と目的に関する記述のうち，適切なものはどれか。

ア　ISP が管理する DNS キャッシュサーバに対して，送信元を攻撃対象のサーバの IP アドレスに詐称してランダムかつ大量に生成したサブドメイン名の問合せを送り，その応答が攻撃対象のサーバに送信されるようにする。

イ　オープンリゾルバとなっている DNS キャッシュサーバに対して，攻撃対象のドメインのサブドメイン名をランダムかつ大量に生成して問い合わせ，攻撃対象の権威 DNS サーバを過負荷にさせる。

ウ　攻撃対象の DNS サーバに対して，攻撃者が管理するドメインのサブドメイン名をランダムかつ大量に生成してキャッシュさせ，正規の DNS リソースレコードを強制的に上書きする。

エ　攻撃対象の Web サイトに対して，当該ドメインのサブドメイン名をランダムかつ大量に生成してアクセスし，非公開の Web ページの参照を試みる。

問7　FIPS PUB 140-2 の記述内容はどれか。

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に関する認証基準

ウ　ディ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8　NIST の定義によるクラウドコンピューティングのサービスモデルにおいて，パブリッククラウドサービスの利用企業のシステム管理者が，仮想サーバのゲスト OS に対するセキュリティパッチの管理と適用を実施可か実施不可かの組合せのうち，適切なものはどれか。

	IaaS	PaaS	SaaS
ア	実施可	実施可	実施不可
イ	実施可	実施不可	実施不可
ウ	実施不可	実施可	実施不可
エ	実施不可	実施不可	実施可

問9　個人情報の漏えいに関するリスク対応のうち，リスク回避に該当するものはどれか。

ア　個人情報の重要性と対策費用を勘案し，あえて対策をとらない。

イ　個人情報の保管場所に外部の者が侵入できないように，入退室をより厳重に管理する。

ウ　個人情報を含む情報資産を外部のデータセンタに預託する。

エ　収集済みの個人情報を消去し，新たな収集を禁止する。

問10　JVN などの脆弱性対策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である。

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である。

ウ　製品に含まれる脆弱性を識別するための識別子である。

エ　セキュリティ製品を識別するための識別子である。

問11　インターネットバンキングの利用時に被害をもたらす MITB（Man-in-the-Browser）攻撃に有効な対策はどれか。

ア　インターネットバンキングでの送金時に Web ブラウザで利用者が入力した情報と，金融機関が受信した情報とに差異がないことを検証できるよう，トランザクション署名を利用する。
イ　インターネットバンキングでの送金時に接続する Web サイトの正当性を確認できるよう，EV SSL サーバ証明書を採用する。
ウ　インターネットバンキングでのログイン認証において，一定時間ごとに自動的に新しいパスワードに変更されるワンタイムパスワードを用意する。
エ　インターネットバンキング利用時の通信を SSL ではなく TLS を利用して暗号化する。

問12　Web アプリケーションの脆(ぜい)弱性を悪用する攻撃手法のうち，Web ページ上で入力した文字列が Perl の system 関数や 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13　ウイルス対策ソフトでの，フォールスネガティブに該当するものはどれか。

ア　ウイルスに感染していないファイルを，ウイルスに感染していないと判断する。
イ　ウイルスに感染していないファイルを，ウイルスに感染していると判断する。
ウ　ウイルスに感染しているファイルを，ウイルスに感染していないと判断する。
エ　ウイルスに感染しているファイルを，ウイルスに感染していると判断する。

問14　特定の利用者が所有するリソースが，Web サービス A 上にある。OAuth 2.0 において，その利用者の認可の下，Web サービス B からそのリソースへの限定されたアクセスを可能にするときのプロトコルの動作はどれか。

ア　Web サービス A が，アクセストークンを発行する。
イ　Web サービス A が，利用者のディジタル証明書を Web サービス B に送信する。
ウ　Web サービス B が，アクセストークンを発行する。
エ　Web サービス B が，利用者のディジタル証明書を Web サービス A に送信する。

問15　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16　サンドボックスの仕組みに関する記述のうち，適切なものはどれか。

ア　Web アプリケーションの脆(ぜい)弱性を悪用する攻撃に含まれる可能性が高い文字列を定義し，攻撃であると判定した場合には，その通信を遮断する。

イ　クラウド上で動作する複数の仮想マシン（ゲスト OS）間で，お互いの操作ができるように制御する。

ウ　プログラムの影響がシステム全体に及ばないように，プログラムが実行できる機能やアクセスできるリソースを制限して動作させる。

エ　プログラムのソースコードで SQL 文の雛(ひな)形の中に変数の場所を示す記号を置いた後，実際の値を割り当てる。

問17　利用者認証情報を管理するサーバ 1 台と複数のアクセスポイントで構成された無線 LAN 環境を実現したい。PC が無線 LAN 環境に接続するときの利用者認証とアクセス制御に，IEEE 802.1X と RADIUS を利用する場合の標準的な方法はどれか。

ア　PC には IEEE 802.1X のサプリカントを実装し，かつ，RADIUS クライアントの機能をもたせる。

イ　アクセスポイントには IEEE 802.1X のオーセンティケータを実装し，かつ，RADIUS クライアントの機能をもたせる。

ウ　アクセスポイントには IEEE 802.1X のサプリカントを実装し，かつ，RADIUS サーバの機能をもたせる。

エ　サーバには IEEE 802.1X のオーセンティケータを実装し，かつ，RADIUS サーバの機能をもたせる。

問18　ICMP Flood 攻撃に該当するものはどれか。

ア　HTTP GET コマンドを繰り返し送ることによって，攻撃対象のサーバにコンテンツ送信の負荷を掛ける。

イ　ping コマンドを用いて大量の要求パケットを発信することによって，攻撃対象のサーバに至るまでの回線を過負荷にしてアクセスを妨害する。

ウ　コネクション開始要求に当たる SYN パケットを大量に送ることによって，攻撃対象のサーバに，接続要求ごとに応答を返すための過大な負荷を掛ける。

エ　大量の TCP コネクションを確立することによって，攻撃対象のサーバに接続を維持させ続けてリソースを枯渇させる。

問19　PC やスイッチングハブがもつイーサネットインタフェース（物理ポート）の，Automatic MDI/MDI-X の機能はどれか。

ア　コネクタの送信端子と受信端子が正しい組合せとなるように，自動で判別して切り替える機能

イ　接続した機器のアドレスを学習し，イーサネットフレームを該当するインタフェースにだけ転送する機能

ウ　通信経路のループを自動的に検出する機能

エ　通信速度や，全二重と半二重のデータ通信モードを自動的に設定する機能

問20　IEEE 802.11a/b/g/n で採用されているアクセス制御方式はどれか。

ア　CSMA/CA
イ　CSMA/CD
ウ　LAPB
エ　トークンパッシング方式

問21　次の SQL 文を A 表の所有者が発行した場合を説明したものはどれか。

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

ア　利用者 B に対して，A 表に関する 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　利用者 B に対して，A 表に関する 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　利用者 B に対して，A 表に関する SELECT 権限，UPDATE 権限，INSERT 権限，DELETE 権限は付与しないが，それらの全ての付与権だけを付与する。

エ　利用者 B に対して，A 表に関する 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　システム及びソフトウェア品質モデルの規格である JIS X 25010:2013 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　コンテンツの不正な複製を防止する方式の一つである DTCP-IP の説明として，適切なものはどれか。

ア　BS デジタル放送や地上デジタル放送に採用され，コピーワンスの番組を録画するときに使われる方式

イ　DLNA とともに用いられ，接続する機器間で相互認証し，コンテンツ保護が行えると認識して初めて録画再生を可能にする方式

ウ　DVD に採用され，映像コンテンツを暗号化して，複製できないエリアにその暗号化鍵を記録する方式

エ　HDMI 端子が搭載されたディジタル AV 機器に採用され，HDMI 端子から表示機器にディジタル信号を送るときに受信する経路を暗号化する方式

問24　データの追加・変更・削除が，少ないながらも一定の頻度で行われるデータベースがある。このデータベースのフルバックアップを磁気テープに取得する時間間隔を今までの 2 倍にした。このとき，データベースのバックアップ又は復旧に関する記述のうち，適切なものはどれか。

ア　フルバックアップ 1 回当たりの磁気テープ使用量が約 2 倍になる。

イ　フルバックアップ 1 回当たりの磁気テープ使用量が約半分になる。

ウ　フルバックアップ取得の平均処理時間が約 2 倍になる。

エ　ログ情報を用いて復旧するときの平均処理時間が約 2 倍になる。

問25　ある企業が，自社が提供する Web サービスの信頼性について，外部監査人による保証を受ける場合において，次の表の A ～ D のうち，“IT に係る保証業務の三当事者”のそれぞれに該当する者の適切な組合せはどれか。

	IT に係る保証業務の三当事者		
	保証業務の実施者	Web サービスの信頼性に責任を負う者	保証報告書の想定利用者
A	Web サービス利用者	外部監査人	当該企業の経営者
B	外部監査人	Web サービス利用者	当該企業の経営者
C	外部監査人	当該企業の経営者	Web サービス利用者
D	当該企業の経営者	外部監査人	Web サービス利用者

ア　A　　　イ　B　　　ウ　C　　　エ　D

〔 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 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。

試験問題に記載されている会社名又は製品名は，それぞれ各社又は各組織の商標又は登録商標です。
なお，試験問題では，™ 及び ® を明記していません。