SC

平成 30 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〕　秋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　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　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　セキュリティ製品を識別するための識別子

問３　ブロックチェーンに関する記述のうち，適切なものはどれか。

ア　RADIUS が必須の技術であり，参加者の利用者認証を一元管理するために利用する。
イ　SPF が必須の技術であり，参加者間で電子メールを送受信するときに送信元の正当性を確認するために利用する。
ウ　楕円曲線暗号が必須の技術であり，参加者間の P2P（Peer to Peer）ネットワークを暗号化するために利用する。
エ　ハッシュ関数が必須の技術であり，参加者がデータの改ざんを検出するために利用する。

問4　マルチベクトル型 DDoS 攻撃に該当するものはどれか。

ア　攻撃対象の Web サーバ 1 台に対して，多数の PC から一斉にリクエストを送ってサーバのリソースを枯渇させる攻撃と，大量の DNS 通信によってネットワークの帯域を消費させる攻撃を同時に行う。

イ　攻撃対象の Web サイトのログインパスワードを解読するために，ブルートフォースによるログイン試行を，多数のスマートフォンや IoT 機器などの踏み台から成るボットネットから一斉に行う。

ウ　攻撃対象のサーバに大量のレスポンスが同時に送り付けられるようにするために，多数のオープンリゾルバに対して，送信元 IP アドレスを攻撃対象のサーバの IP アドレスに偽装した名前解決のリクエストを一斉に送信する。

エ　攻撃対象の組織内の多数の端末をマルウェアに感染させ，当該マルウェアを遠隔操作することによってデータの改ざんやファイルの消去を一斉に行う。

問5　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の要求事項

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6　経済産業省と IPA が策定した“サイバーセキュリティ経営ガイドライン（Ver2.0）”の説明はどれか。

ア　企業が IT 活用を推進していく中で，サイバー攻撃から企業を守る観点で経営者が認識すべき 3 原則と，情報セキュリティ対策を実施する上での責任者となる担当幹部に，経営者が指示すべき事項をまとめたもの

イ　経営者が情報セキュリティについて方針を示し，マネジメントシステムの要求事項を満たすルールを定め，組織が保有する情報資産を CIA の観点から維持管理し，それらを継続的に見直すためのプロセス及び管理策を体系的に規定したもの

ウ　事業体の IT に関する経営者の活動を，大きく IT ガバナンス（統制）と IT マネジメント（管理）に分割し，具体的な目標と工程として 37 のプロセスを定義したもの

エ　世界的規模で生じているサイバーセキュリティ上の脅威の深刻化に関して，企業の経営者を支援する施策を総合的かつ効果的に推進するための国の責務を定めたもの

問7　UDP の性質を悪用した DDoS 攻撃に該当するものはどれか。

ア　DNS リフレクタ攻撃　　イ　SQL インジェクション攻撃

ウ　ディレクトリトラバーサル攻撃　　エ　パスワードリスト攻撃

問８　EDSA 認証における評価対象と評価項目について，適切な組みはどれか。

	評価対象	評価項目
ア	組込み機器である制御機器	組込み機器ロバストネス試験
イ	組込み機器である制御機器が運用されている施設	入退室管理の評価
ウ	複数の制御機器から構成される制御システム	脆弱(ぜい)性試験
エ	複数の制御機器から構成される制御システムを管理する組織	セキュリティポリシの評価

問９　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 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10　JIS X 9401:2016（情報技術－クラウドコンピューティング－概要及び用語）の定義によるクラウドサービス区分の一つであり，クラウドサービスカスタマの責任者が表中の項番 1 と 2 の責務を負い，クラウドサービスプロバイダが項番 3～5 の責務を負うものはどれか。

項番	責　務
1	アプリケーションに対して，データのアクセス制御と暗号化の設定を行う。
2	アプリケーションに対して，セキュアプログラミングと脆弱性診断を行う。
3	DBMS に対して，修正プログラム適用と権限設定を行う。
4	OS に対して，修正プログラム適用と権限設定を行う。
5	ハードウェアに対して，アクセス制御と物理セキュリティ確保を行う。

ア　HaaS　　イ　IaaS　　ウ　PaaS　　エ　SaaS

問11　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 サーバの脆弱性を悪用して感染を広げ，Web サーバの 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 IP アドレスを生成して telnet ポートにログインを試行し，工場出荷時の弱いパスワードを使っている 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12　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，EV SSL 証明書であることを利用者が容易に識別できるように，Web ブラウザのアドレス表示部分を緑色に表示する。

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 サイトにアクセスすると，Web ブラウザは，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13　Web アプリケーションの脆弱(ぜい)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14　SMTP-AUTH の特徴はどれか。

ア　ISP 管理下の動的 IP アドレスから管理外ネットワークのメールサーバへの SMTP 接続を禁止する。

イ　電子メール送信元のサーバが，送信元ドメインの DNS に登録されていることを確認して，電子メールを受信する。

ウ　メールクライアントからメールサーバへの電子メール送信時に，利用者 ID とパスワードによる利用者認証を行う。

エ　メールクライアントからメールサーバへの電子メール送信は，POP 接続で利用者認証済みの場合にだけ許可する。

問15　TLS に関する記述のうち，適切なものはどれか。

ア　TLS で使用する Web サーバのディジタル証明書には IP アドレスの組込みが必須なので，Web サーバの IP アドレスを変更する場合は，ディジタル証明書を再度取得する必要がある。

イ　TLS で使用する共通鍵の長さは，128 ビット未満で任意に指定する。

ウ　TLS で使用する個人認証用のディジタル証明書は，IC カードにも格納することができ，利用する PC を特定の PC に限定する必要はない。

エ　TLS は Web サーバと特定の利用者が通信するためのプロトコルであり，Web サーバへの事前の利用者登録が不可欠である。

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　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。

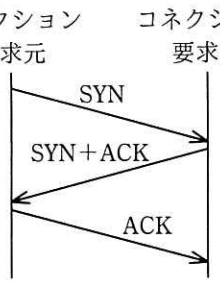
イ　アクセスポイントには IEEE 802.1X のオーセンティケータを実装し，かつ，RADIUS クライアントの機能をもたせる。

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。

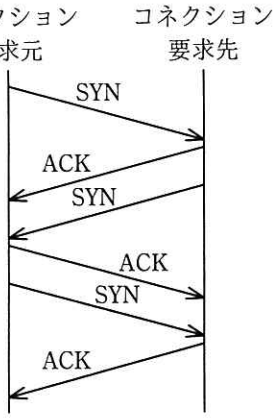
エ　サーバには IEEE 802.1X のオーセンティケータを実装し，かつ，RADIUS サーバの機能をもたせる。

問18　TCP のコネクション確立方式である 3 ウェイハンドシェイクを表す図はどれか。

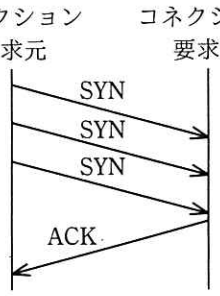
ア



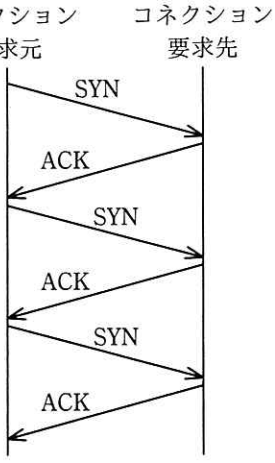
イ



ウ



エ



問19　クラス D の IP アドレス（224.0.0.0～239.255.255.255）に関する記述として，適切なものはどれか。

ア　DHCP サーバが見つからないときの自動設定アドレスに使用される。

イ　IETF での実験用アドレスとして予約されており，一般には使用されない。

ウ　UDP などを用いるマルチキャスト通信で使用される。

エ　小規模なネットワークでプライベートアドレスとして使用される。

問20　日本国内において，無線 LAN の規格 IEEE 802.11n 及び IEEE 802.11ac で使用される周波数帯域の組合せとして，適切なものはどれか。

	IEEE 802.11n	IEEE 802.11ac
ア	2.4 GHz 帯	2.4 GHz 帯，5 GHz 帯
イ	2.4 GHz 帯，5 GHz 帯	2.4 GHz 帯
ウ	2.4 GHz 帯，5 GHz 帯	5 GHz 帯
エ	5 GHz 帯	2.4 GHz 帯，5 GHz 帯

問21　次の SQL 文の実行結果の説明に関する記述のうち，適切なものはどれか。

```
CREATE VIEW 東京取引先 AS
        SELECT * FROM 取引先
        WHERE 取引先.所在地 = '東京'
GRANT SELECT
        ON 東京取引先 TO "8823"
```

ア　このビューには，8823 行までを記録できる。

イ　このビューの作成者は，このビューに対する SELECT 権限をもたない。

ウ　実表“取引先”が削除されても，このビューに対する利用者の権限は残る。

エ　利用者“8823”は，実表“取引先”の所在地が‘東京’の行を参照できるようになる。

問22　図のような階層構造で設計及び実装し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。この段階で行う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　SOA でシステムを設計する際の注意点のうち，適切なものはどれか。

ア　可用性を高めるために，ステートフルなインタフェースとする。
イ　業務からの独立性を確保するために，サービスの名称は抽象的なものとする。
ウ　業務の変化に対応しやすくするために，サービス間の関係は疎結合にする。
エ　セキュリティを高めるために，一度提供したサービスの設計は再利用しない。

問24　ITサービスマネジメントの情報セキュリティ管理プロセスに対して，JIS Q 20000-1:2012（サービスマネジメントシステム要求事項）が要求している事項はどれか。

ア　CMDBに記録されているCIの原本を，セキュリティが保たれた物理的又は電子的な格納庫で管理しなければならない。

イ　潜在的な問題を低減させるために，予防処置をとらなければならない。

ウ　変更要求が情報セキュリティ基本方針及び管理策に与える潜在的影響を評価しなければならない。

エ　変更要求の受入れについての意思決定では，リスク，事業利益及び技術的実現可能性を考慮しなければならない。

問25　ある企業が，自社が提供するWebシステムのセキュリティについて，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システムのセキュリティに責任を負う者	保証報告書の想定利用者
A	Webシステム利用者	外部監査人	当該企業の経営者
B	外部監査人	Webシステム利用者	当該企業の経営者
C	外部監査人	当該企業の経営者	Webシステム利用者
D	当該企業の経営者	外部監査人	Webシステム利用者

ア　A　　イ　B　　ウ　C　　エ　D

〔 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。