SC

令和元年度　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　認証処理のうち，FIDO（Fast IDentity Online） UAF（Universal Authentication Framework） 1.1 に基づいたものはどれか。

ア　SaaS 接続時の認証において，PIN コードとトークンが表示したワンタイムパスワードとを PC から認証サーバに送信した。

イ　SaaS 接続時の認証において，スマートフォンで顔認証を行った後，スマートフォン内の秘密鍵でディジタル署名を生成して，そのディジタル署名を認証サーバに送信した。

ウ　インターネットバンキング接続時の認証において，PC に接続されたカードリーダを使って，利用者のキャッシュカードからクライアント証明書を読み取って，そのクライアント証明書を認証サーバに送信した。

エ　インターネットバンキング接続時の認証において，スマートフォンを使い指紋情報を読み取って，その指紋情報を認証サーバに送信した。

問２　暗号機能を実装した IoT 機器において脅威となるサイドチャネル攻撃に該当するものはどれか。

ア　暗号化関数を線形近似する式を導き，その線形近似式から秘密情報の取得を試みる。

イ　機器が発する電磁波を測定することによって秘密情報の取得を試みる。

ウ　二つの平文の差とそれぞれの暗号文の差の関係から，秘密情報の取得を試みる。

エ　理論的にあり得る復号鍵の全てを機器に入力して秘密情報の取得を試みる。

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　ディジタル証明書にディジタル署名を付与する。
ウ　ディ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，ディジタル証明書の発行を指示する。

問４　XML ディジタル署名の特徴として，適切なものはどれか。

ア　XML 文書中の任意のエレメントに対してデタッチ署名（Detached Signature）を付けることができる。
イ　エンベロープピング署名（Enveloping Signature）では一つの署名対象に必ず複数の署名を付ける。
ウ　署名形式として，CMS（Cryptographic Message Syntax）を用いる。
エ　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　ファイアウォールにおけるダイナミックパケットフィルタリングの特徴はどれか。

ア　IP アドレスの変換が行われるので，内部のネットワーク構成を外部から隠蔽できる。
イ　暗号化されたパケットのデータ部を復号して，許可された通信かどうかを判断できる。
ウ　過去に通過したリクエストパケットに対応付けられる戻りのパケットを通過させることができる。
エ　パケットのデータ部をチェックして，アプリケーション層での不正なアクセスを防止できる。

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

ア　PKI の利用者は，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。

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

ウ　認証局は，発行したディ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られている。

エ　認証局は，有効期限内のディジタル証明書のシリアル番号を CRL に記載することがある。

問7　JIS Q 27014:2015（情報セキュリティガバナンス）における，情報セキュリティを統治するために経営陣が実行するガバナンスプロセスのうちの“モニタ”はどれか。

ア　情報セキュリティの目的及び戦略について，指示を与えるガバナンスプロセス

イ　戦略的目的の達成を評価することを可能にするガバナンスプロセス

ウ　独立した立場からの客観的な監査，レビュー又は認証を委託するガバナンスプロセス

エ　利害関係者との間で，特定のニーズに沿って情報セキュリティに関する情報を交換するガバナンスプロセス

問８　総務省及び経済産業省が策定した“電子政府における調達のために参照すべき暗号のリスト（CRYPTREC 暗号リスト）”を構成する暗号リストの説明のうち，適切なものはどれか。

ア　推奨候補暗号リストとは，CRYPTREC によって安全性及び実装性能が確認された暗号技術のうち，市場における利用実績が十分であるか今後の普及が見込まれると判断され，当該技術の利用を推奨するもののリストである。

イ　推奨候補暗号リストとは，候補段階に格下げされ，互換性維持目的で利用する暗号技術のリストである。

ウ　電子政府推奨暗号リストとは，CRYPTREC によって安全性及び実装性能が確認された暗号技術のうち，市場における利用実績が十分であるか今後の普及が見込まれると判断され，当該技術の利用を推奨するもののリストである。

エ　電子政府推奨暗号リストとは，推奨段階に格下げされ，互換性維持目的で利用する暗号技術のリストである。

問９　基本評価基準，現状評価基準，環境評価基準の三つの基準で情報システムの脆弱性の深刻度を評価するものはどれか。

ア　CVSS　　イ　ISMS　　ウ　PCI DSS　　エ　PMS

問10　BlueBorne の説明はどれか。

ア　Bluetooth を悪用してデバイスを不正に操作したり，情報を窃取したりする，複数の脆弱性の呼称

イ　感染した PC の画面の背景を青 1 色に表示させた上，金銭の支払を要求するランサムウェアの一種

ウ　攻撃側（Red Team）と防御側（Blue Team）に分かれて疑似的にサイバー攻撃を行う演習における，防御側の戦術の一種

エ　ブルーレイディスクを経由して感染を拡大した，日本の政府機関や重要インフラ事業者を標的とした APT 攻撃の呼称

問11　Cookie に Secure 属性を設定しなかったときと比較した，設定したときの動作として，適切なものはどれか。

ア　Cookie に設定された有効期間を過ぎると，Cookie が無効化される。

イ　JavaScript による Cookie の読出しが禁止される。

ウ　URL 内のスキームが https のときだけ，Web ブラウザから Cookie が送出される。

エ　Web ブラウザがアクセスする URL 内のパスと Cookie に設定されたパスのプレフィックスが一致するときだけ，Web ブラウザから Cookie が送出される。

問12　DKIM（DomainKeys Identified Mail）の説明はどれか。

ア　送信側メールサーバにおいてディジタル署名を電子メールのヘッダに付加し，受信側メールサーバにおいてそのディジタル署名を公開鍵によって検証する仕組み

イ　送信側メールサーバにおいて利用者が認証された場合，電子メールの送信が許可される仕組み

ウ　電子メールのヘッダや配送経路の情報から得られる送信元情報を用いて，メール送信元のIPアドレスを検証する仕組み

エ　ネットワーク機器において，内部ネットワークから外部のメールサーバのTCPポート番号25への直接の通信を禁止する仕組み

問13　マルチベクトル型DDoS攻撃に該当するものはどれか。

ア　DNSリフレクタ攻撃によってDNSサービスを停止させ，複数のPCでの名前解決を妨害する。

イ　Webサイトに対して，SYN Flood攻撃とHTTP POST Flood攻撃を同時に行う。

ウ　管理者用IDのパスワードを初期設定のままで利用している複数のIoT機器を感染させ，それらのIoT機器から，Webサイトに UDP Flood攻撃を行う。

エ　ファイアウォールでのパケットの送信順序を不正に操作するパケットを複数送信することによって，ファイアウォールのCPUやメモリを枯渇させる。

問14　Web サイトにおいて，全ての Web ページを TLS で保護するよう設定する常時 SSL/TLS のセキュリティ上の効果はどれか。

ア　Web サイトでの SQL 組立て時にエスケープ処理が施され，SQL インジェクション攻撃による個人情報などの非公開情報の漏えいやデータベースに蓄積された商品価格などの情報の改ざんを防止する。

イ　Web サイトへのアクセスが人間によるものかどうかを確かめ，Web ブラウザ以外の自動化された Web クライアントによる大量のリクエストへの応答を避ける。

ウ　Web サイトへのブルートフォース攻撃によるログイン試行を検出してアカウントロックし，Web サイトへの不正ログインを防止する。

エ　Web ブラウザと Web サイトとの間における中間者攻撃による通信データの漏えい及び改ざんを防止し，サーバ証明書によって偽りの Web サイトの見分けを容易にする。

問15　攻撃者に脆弱性に関する専門の知識がなくても，OS やアプリケーションソフトウェアの脆弱性を悪用した攻撃ができる複数のプログラムや管理機能を統合したものはどれか。

ア　Exploit Kit　　イ　iLogScanner

ウ　MyJVN　　エ　Remote Access Tool

問16　IEEE 802.1X で使われる EAP-TLS が行う認証はどれか。

ア　CHAP を用いたチャレンジレスポンスによる利用者認証

イ　あらかじめ登録した共通鍵によるサーバ認証と，時刻同期のワンタイムパスワードによる利用者認証

ウ　ディジタル証明書による認証サーバとクライアントの相互認証

エ　利用者 ID とパスワードによる利用者認証

問17　SQL インジェクション対策について，Web アプリケーションプログラムの実装における対策と，Web アプリケーションプログラムの実装以外の対策として，ともに適切なものはどれか。

	Web アプリケーションプログラムの実装における対策	Web アプリケーションプログラムの実装以外の対策
ア	Web アプリケーションプログラム中でシェルを起動しない。	chroot 環境で Web サーバを稼働させる。
イ	セッション ID を乱数で生成する。	TLS によって通信内容を秘匿する。
ウ	パス名やファイル名をパラメタとして受け取らないようにする。	重要なファイルを公開領域に置かない。
エ	プレースホルダを利用する。	Web アプリケーションプログラムが利用するデータベースのアカウントがもつデータベースアクセス権限を必要最小限にする。

問18　DNSSEC に関する記述として，適切なものはどれか。

ア　DNS サーバへの DoS 攻撃を防止できる。
イ　IPsec による暗号化通信が前提となっている。
ウ　代表的な DNS サーバの実装である BIND の代替として使用する。
エ　ディジタル署名によって DNS 応答の正当性を確認できる。

問19　IPv4 ネットワークにおいて，IP パケットの分割処理と，分割されたパケットを元に戻す再構築処理に関する記述のうち，適切なものはどれか。

ア　IP パケットの再構築処理は宛先のホストで行われる。
イ　IP パケットの再構築処理は中継するルータで行われる。
ウ　IP パケットの分割処理は送信元のホストだけで行われる。
エ　IP パケットの分割処理は中継するルータだけで行われる。

問20　TCP に関する記述のうち，適切なものはどれか。

ア　OSI 基本参照モデルのネットワーク層の機能である。
イ　ウィンドウ制御の単位は，バイトではなくビットである。
ウ　確認応答がない場合は再送処理によってデータ回復を行う。
エ　データの順序番号をもたないので，データは受信した順番のままで処理する。

問21　JSON 形式で表現される図 1，図 2 のような商品データを複数の Web サービスから取得し，商品データベースとして蓄積する際のデータの格納方法に関する記述のうち，適切なものはどれか。ここで，商品データの取得元となる Web サービスは随時変更され，項目数や内容は予測できない。したがって，商品データベースの検索時に使用するキーにはあらかじめ制限を設けない。

```
{
  "_id":"AA09",
  "品名":"47 型テレビ",
  "価格":"オープンプライス",
  "関連商品 id": [
    "AA101",
    "BC06"
  ]
}
```

図 1　A 社 Web サービスの商品データ

```
{
  "_id":"AA10",
  "商品名":"りんご",
  "生産地":"青森",
  "価格":100,
  "画像 URL":"http://www.example.com/apple.jpg"
}
```

図 2　B 社 Web サービスの商品データ

ア　階層型データベースを使用し，項目名を上位階層とし，値を下位階層とした 2 階層でデータを格納する。

イ　グラフ型データベースを使用し，商品データの項目名の集合から成るノードと値の集合から成るノードを作り，二つのノードを関係づけたグラフとしてデータを格納する。

ウ　ドキュメント型データベースを使用し，項目構成の違いを区別せず，商品データ単位にデータを格納する。

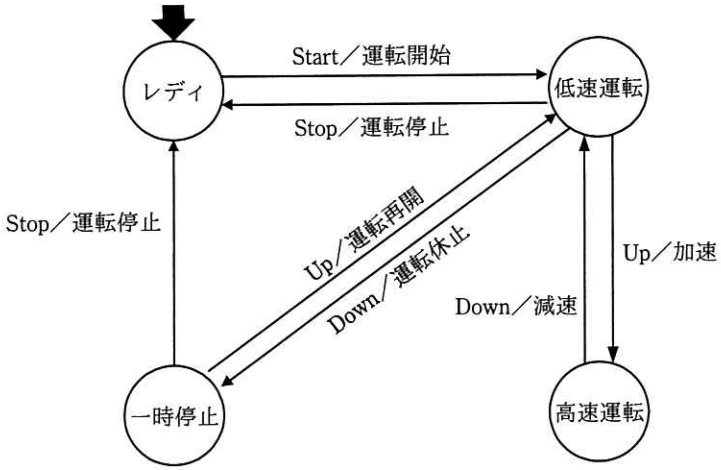
エ　リレーショナルデータベースを使用し，商品データの各項目名を個別の列名とした表を定義してデータを格納する。

問22　次の仕様で動作する装置がある。未完成の状態遷移図を完成させるために，追加すべき遷移はどれか。

〔仕様〕

・レディで Start ボタンが押された場合，運転開始して低速運転に遷移する。
・低速運転で Up ボタンが押された場合，加速して高速運転に遷移する。
・低速運転で Down ボタンが押された場合，運転休止して一時停止に遷移する。
・高速運転で Down ボタンが押された場合，減速して低速運転に遷移する。
・一時停止で Up ボタンが押された場合，運転再開して低速運転に遷移する。
・レディ以外の状態で Stop ボタンが押された場合，運転停止してレディに遷移する。

〔未完成の状態遷移図〕



	遷移元の状態名	条件部／動作部	遷移先の状態名
ア	一時停止	Start／運転再開	高速運転
イ	一時停止	Start／運転再開	低速運転
ウ	高速運転	Stop／運転休止	一時停止
エ	高速運転	Stop／運転停止	レディ

問23　マッシュアップを利用して Web コンテンツを表示する例として，最も適切なものはどれか。

ア　Web ブラウザにプラグインを組み込み，動画やアニメーションを表示する。
イ　地図上のカーソル移動に伴い，Web ページを切り替えずにスクロール表示する。
ウ　鉄道経路の探索結果上に，各鉄道会社の Web ページへのリンクを表示する。
エ　店舗案内の Web ページ上に，他のサイトが提供する地図検索機能を利用して出力された情報を表示する。

問24　情報システムの設計の例のうち，フェールソフトの考え方を適用した例はどれか。

ア　UPS を設置することによって，停電時に手順どおりにシステムを停止できるようにする。
イ　制御プログラムの障害時に，システムの暴走を避け，安全に運転を停止できるようにする。
ウ　ハードウェアの障害時に，パフォーマンスは低下するが，構成を縮小して運転を続けられるようにする。
エ　利用者の誤操作や誤入力を未然に防ぐことによって，システムの誤動作を防止できるようにする。

問25　システムの本番移行が失敗するリスクに対するコントロールを監査するときのチェックポイントはどれか。

ア　システム運用段階で新システムの稼働状況がレビューされ，その結果についてシステム開発部門及び利用部門の責任者の承認が得られていること

イ　システム開発段階で抽出された問題への対策が，次期システム改善計画に反映されていること

ウ　システム企画段階で，システムの投資対効果が評価されていること

エ　利用部門を含めた各部門の役割と責任を明確にした本番移行計画が作成されていること

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。