SC

平成30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　CVSS v3 の評価基準には，基本評価基準，現状評価基準，環境評価基準の三つがある。基本評価基準の説明はどれか。

ア　機密性への影響，どこから攻撃が可能かといった攻撃元区分，攻撃する際に必要な特権レベルなど，脆弱性そのものの特性を評価する。

イ　攻撃される可能性，利用可能な対策のレベル，脆弱性情報の信頼性など，評価時点における脆弱性の特性を評価する。

ウ　脆弱性を悪用した攻撃シナリオについて，機会，正当化，動機の三つの観点から，脆弱性が悪用される基本的なリスクを評価する。

エ　利用者のシステムやネットワークにおける情報セキュリティ対策など，攻撃の難易度や攻撃による影響度を再評価し，脆弱性の最終的な深刻度を評価する。

問2　Web サーバのログを分析したところ，Web サーバへの攻撃と思われる HTTP リクエストヘッダが記録されていた。次の HTTP リクエストヘッダから推測できる，攻撃者が悪用しようとしている脆弱性はどれか。ここで，HTTP リクエストヘッダはデコード済みである。

〔HTTP リクエストヘッダの部分〕

```
GET /cgi-bin/submit.cgi?user=;cat /etc/passwd HTTP/1.1
Accept: */*
Accept-Language: ja
UA-CPU: x86
Accept-Encoding: gzip, deflate
User-Agent:  (省略)
Host: test.example.com
Connection: Keep-Alive
```

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　SQL インジェクション　　エ　クロスサイトスクリプティング

問3　XML ディジタル署名の特徴のうち，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4　エクスプロイトコードの説明はどれか。

ア　攻撃コードとも呼ばれ，脆弱性を悪用するソフトウェアのコードのことであるが，使い方によっては脆弱性の検証に役立つこともある。

イ　マルウェアのプログラムを解析して得られる，マルウェアを特定するための特徴的なコードのことであり，マルウェア対策ソフトの定義ファイルとしてマルウェアの検知に用いられる。

ウ　メッセージとシークレットデータから計算されるハッシュコードのことであり，メッセージの改ざんの検知に用いられる。

エ　ログインの度に変化する認証コードのことであり，窃取されても再利用できないので不正アクセスを防ぐ。

問5　シングルサインオンの実装方式に関する記述のうち，適切なものはどれか。

ア　cookie を使ったシングルサインオンの場合，サーバごとの認証情報を含んだ cookie をクライアントで生成し，各サーバ上で保存，管理する。

イ　cookie を使ったシングルサインオンの場合，認証対象のサーバを，異なるインターネットドメインに配置する必要がある。

ウ　リバースプロキシを使ったシングルサインオンの場合，認証対象の Web サーバを，異なるインターネットドメインに配置する必要がある。

エ　リバースプロキシを使ったシングルサインオンの場合，利用者認証においてパスワードの代わりにディジタル証明書を用いることができる。

問6　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，ファイアウォール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7　発信者がメッセージのハッシュ値からディジタル署名を生成するのに使う鍵はどれか。

ア　受信者の公開鍵　　イ　受信者の秘密鍵

ウ　発信者の公開鍵　　エ　発信者の秘密鍵

問８　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 に登録する。

ウ　認証局は，発行したディジタル証明書のうち，失効したものは，シリアル番号を失効後１年間 CRL に登録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 に登録することがある。

問９　認証デバイスに関する記述のうち，適切なものはどれか。

ア　USB メモリにディジタル証明書を組み込み，認証デバイスとする場合は，その USB メモリを接続する PC の MAC アドレスを組み込む必要がある。

イ　成人の虹彩は，経年変化がなく，虹彩認証では，認証デバイスでのパターン更新がほとんど不要である。

ウ　静電容量方式の指紋認証デバイスは，LED 照明を設置した室内では正常に認証できなくなる可能性が高くなる。

エ　認証に利用する接触型 IC カードは，カード内のコイルの誘導起電力を利用している。

問10　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み

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み

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み

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み

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の差として，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 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，Web ブラウザから cookie が送出される。

問12　スパムメールへの対策である 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　テンペスト攻撃を説明したものはどれか。

ア　故意に暗号化演算を誤動作させて正しい処理結果との差異を解析する。

イ　処理時間の差異を計測して解析する。

ウ　処理中に機器から放射される電磁波を観測して解析する。

エ　チップ内の信号線などに探針を直接当て，処理中のデータを観測して解析する。

問14　内部ネットワークの PC がダウンローダ型マルウェアに感染したとき，そのマルウェアがインターネット経由で他のマルウェアをダウンロードすることを防ぐ方策として，最も有効なものはどれか。

ア　インターネットから内部ネットワークに向けた要求パケットによる不正侵入行為を IPS で破棄する。
イ　インターネット上の危険な Web サイトの情報を保持する URL フィルタを用いて，危険な Web サイトとの接続を遮断する。
ウ　スパムメール対策サーバでインターネットからのスパムメールを拒否する。
エ　メールフィルタでインターネット上の他サイトへの不正な電子メールの発信を遮断する。

問15　ルートキットの特徴はどれか。

ア　OS などに不正に組み込んだツールを隠蔽する。
イ　OS の中核であるカーネル部分の脆弱性を分析する。
ウ　コンピュータがウイルスやワームに感染していないことをチェックする。
エ　コンピュータやルータのアクセス可能な通信ポートを外部から調査する。

問16　DNSSEC で実現できることはどれか。

ア　DNS キャッシュサーバが得た応答中のリソースレコードが，権威 DNS サーバで管理されているものであり，改ざんされていないことの検証
イ　権威 DNS サーバと DNS キャッシュサーバとの通信を暗号化することによる，ゾーン情報の漏えいの防止
ウ　長音“ー”と漢数字“一”などの似た文字をドメイン名に用いて，正規サイトのように見せかける攻撃の防止
エ　利用者の URL の入力誤りを悪用して，偽サイトに誘導する攻撃の検知

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

	Web アプリケーションの実装における対策	Web アプリケーションの実装以外の対策
ア	Web アプリケーション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。	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　IPv4 において，IP パケットで送られているデータが，ICMP メッセージであることを識別できるヘッダ情報はどれか。

ア　IP ヘッダのプロトコル番号
イ　MAC ヘッダのイーサタイプ値
ウ　TCP ヘッダのコントロールフラグ
エ　UDP ヘッダの宛先ポート番号

問19　IEEE 802.1Q の VLAN 機能を有したスイッチにおいて，複数の VLAN に所属しているポートを何と呼ぶか。

ア　アクセスポート　　イ　代表ポート
ウ　トランクポート　　エ　ルートポート

問20　WebDAV の特徴はどれか。

ア　HTTP 上の SOAP によってソフトウェア同士が通信して，ネットワーク上に分散したアプリケーションを連携させることができる。

イ　HTTP を拡張したプロトコルを使って，サーバ上のファイルの参照，作成，削除及びバージョン管理が行える。

ウ　Web アプリケーションから IMAP サーバにアクセスして，Web ブラウザから添付ファイルを含む電子メールの操作ができる。

エ　Web ブラウザで “ftp://” から始まる URL を指定して，ソフトウェアなどの大きなファイルのダウンロードができる。

問21　DBMS がトランザクションのコミット処理を完了とするタイミングはどれか。

ア　アプリケーションの更新命令完了時点

イ　チェックポイント処理完了時点

ウ　ログバッファへのコミット情報書込み完了時点

エ　ログファイルへのコミット情報書込み完了時点

問22　UML 2.0 において，オブジェクト間の相互作用を時間の経過に注目して記述するものはどれか。

ア　アクティビティ図　　イ　コミュニケーション図

ウ　シーケンス図　　エ　ユースケース図

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重視する。
エ　プログラムを書く前にテストケースを作成する。

問24　サービス提供時間帯が毎日0～24時のITサービスにおいて，ある年の4月1日0時から6月30日24時までのシステム停止状況は表のとおりであった。システムバージョンアップ作業に伴う停止時間は，計画停止時間として顧客との間で合意されている。このとき，4月1日から6月30日までのITサービスの可用性は何%か。ここで，可用性（%）は小数第3位を四捨五入することとする。

〔システム停止状況〕

停止理由	停止時間
システムバージョンアップ作業に伴う停止	5月2日22時から5月6日10時までの84時間
ハードウェア故障	6月26日10時から20時までの10時間

ア　95.52　　イ　95.70　　ウ　99.52　　エ　99.63

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　更新ログを加工して，アプリケーションの機能を経由した正常な処理によるログとして残していた。

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　直接修正の作業時以外は，使用する直接修正用の特権 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 〕

〔 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。