SC

平成24年度　春期
情報セキュリティスペシャリスト試験
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　クリックジャッキング攻撃に該当するものはどれか。

ア　Web アプリケーションの脆弱性を悪用し，Web サーバに不正なリクエストを送って Web サーバからのレスポンスを二つに分割させることによって，利用者のブラウザのキャッシュを偽造する。

イ　Web ページのコンテンツ上に透明化した標的サイトのコンテンツを配置し，利用者が気づかないうちに標的サイト上で不正操作を実行させる。

ウ　ブラウザのタブ表示機能を利用し，ブラウザの非活性なタブの中身を，利用者が気づかないうちに偽ログインページに書き換えて，それを操作させる。

エ　利用者のブラウザの設定を変更することによって，利用者の Web ページの閲覧履歴やパスワードなどの機密情報を盗み出す。

問2　作成者によってディジタル署名された電子文書に，タイムスタンプ機関がタイムスタンプを付与した。この電子文書を公開する場合のタイムスタンプの効果のうち，適切なものはどれか。

ア　タイムスタンプを付与した時刻以降に，作成者が電子文書の内容を他の電子文書へコピーして流用することを防止する。

イ　タイムスタンプを付与した時刻以降に，第三者が電子文書の内容を他の電子文書へコピーして流用することを防止する。

ウ　電子文書がタイムスタンプの時刻以前に存在したことを示すことによって，作成者が電子文書の作成を否認することを防止する。

エ　電子文書がタイムスタンプの時刻以前に存在したことを示すことによって，第三者が電子文書を改ざんすることを防止する。

問3　ディジタル証明書に関する記述のうち，適切なものはどれか。

ア　S/MIME や TLS で利用するディジタル証明書の規格は，ITU-T X.400 で規定されている。

イ　ディジタル証明書は，SSL/TLS プロトコルにおいて通信データの暗号化のための鍵交換や通信相手の認証に利用されている。

ウ　認証局が発行するディジタル証明書は，申請者の秘密鍵に対して認証局がディジタル署名したものである。

エ　ルート認証局は，下位層の認証局の公開鍵にルート認証局の公開鍵でディジタル署名したディジタル証明書を発行する。

問4　米国 NIST が制定した，AES における鍵長の条件はどれか。

ア　128 ビット，192 ビット，256 ビットから選択する。

イ　256 ビット未満で任意に指定する。

ウ　暗号化処理単位のブロック長より 32 ビット長くする。

エ　暗号化処理単位のブロック長より 32 ビット短くする。

問5　コンティンジェンシープランにおける留意点はどれか。

ア　企業の全てのシステムを対象とするのではなく，システムの復旧の重要性と緊急性を勘案して対象を決定する。

イ　災害などへの対応のために，すぐに使用できるよう，バックアップデータをコンピュータ室内又はセンタ内に保存しておく。

ウ　バックアップの対象は，機密情報の中から機密度を勘案して選択する。

エ　被害のシナリオを作成し，これに基づく“予防策策定手順”を策定する。

問6　JIS Q 27001:2006 における情報システムのリスクとその評価に関する記述のうち，適切なものはどれか。

ア　脅威とは，脆弱性が顕在化する源のことであり，情報システムに組み込まれた技術的管理策によって脅威のレベルと発生の可能性が決まる。

イ　脆弱性とは，情報システムに対して悪い影響を与える要因のことであり，自然災害，システム障害，人為的過失及び不正行為に大別される。

ウ　リスクの特定では，脅威が管理策の脆弱性に付け込むことによって情報資産に与える影響を特定する。

エ　リスク評価では，リスク回避とリスク低減の二つに評価を分類し，リスクの大きさを判断して対策を決める。

問7　ファイアウォールにおいて，自ネットワークのホストへの侵入を防止する対策のうち，IP スプーフィング（spoofing）攻撃の対策について述べたものはどれか。

ア　外部から入る TCP コネクション確立要求パケットのうち，外部へのインターネットサービスの提供に必要なもの以外を破棄する。

イ　外部から入る UDP パケットのうち，外部へのインターネットサービスの提供や利用したいインターネットサービスに必要なもの以外を破棄する。

ウ　外部から入るパケットの宛先 IP アドレスが，インターネットとの直接の通信をすべきでない自ネットワークのホストのものであれば，そのパケットを破棄する。

エ　外部から入るパケットの送信元 IP アドレスが自ネットワークのものであれば，そのパケットを破棄する。

問8 サイドチャネル攻撃の手法であるタイミング攻撃の対策として，最も適切なものはどれか。

ア　演算アルゴリズムに対策を施して，演算内容による処理時間の差異が出ないようにする。

イ　故障を検出する機構を設けて，検出したら機密情報を破壊する。

ウ　コンデンサを挿入して，電力消費量が時間的に均一となるようにする。

エ　保護層を備えて，内部のデータが不正に書き換えられないようにする。

問9 PCIデータセキュリティ基準（PCI DSS Version 2.0）の要件のうち，詳細要件の選択肢として，WAFの導入を含むものはどれか。

ア　要件1：カード会員データを保護するために，ファイアウォールをインストールして構成を維持すること

イ　要件3：保存されるカード会員データを保護すること

ウ　要件6：安全性の高いシステムとアプリケーションを開発し，保守すること

エ　要件7：カード会員データへのアクセスを，業務上必要な範囲内に制限すること

問10 DMZ上のコンピュータがインターネットからの ping に応答しないようにファイアウォールのセキュリティルールを定めるとき，“通過禁止”に設定するものはどれか。

ア　ICMP

イ　TCP及びUDPのポート番号53

ウ　TCPのポート番号21

エ　UDPのポート番号123

問11　有料の公衆無線 LAN サービスにおいて実施される，ネットワークサービスの不正利用に対するセキュリティ対策の方法と目的はどれか。

ア　利用者ごとに異なる SSID を割り当てることによって，利用者 PC への不正アクセスを防止する。

イ　利用者ごとに異なるサプリカントを割り当てることによって，利用者 PC への不正アクセスを防止する。

ウ　利用者ごとに異なるプライベート IP アドレスを割り当てることによって，第三者によるアクセスポイントへのなりすましを防止する。

エ　利用者ごとに異なる利用者 ID を割り当て，パスワードを設定することによって，契約者以外の利用者によるアクセスを防止する。

問12　送信元を詐称した電子メールを拒否するために，SPF（Sender Policy Framework）の仕組みにおいて受信側が行うことはどれか。

ア　Resent-Sender:，Resent-From:，Sender:，From:などのメールヘッダ情報の送信者メールアドレスを基に送信メールアカウントを検証する。

イ　SMTP が利用するポート番号 25 の通信を拒否する。

ウ　SMTP 通信中にやり取りされる MAIL FROM コマンドで与えられた送信ドメインと送信サーバの IP アドレスの適合性を検証する。

エ　電子メールに付加されたディジタル署名を受信側が検証する。

問13　迷惑メールの検知手法であるベイジアンフィルタリングの説明はどれか。

ア　信頼できるメール送信元を許可リストに登録しておき，許可リストにない送信元からの電子メールは迷惑メールと判定する。

イ　電子メールが正規のメールサーバから送信されていることを検証し，迷惑メールであるかどうかを判定する。

ウ　電子メールの第三者中継を許可しているメールサーバを登録したデータベースに掲載されている情報を基に，迷惑メールであるかどうかを判定する。

エ　迷惑メールを利用者が振り分けるときに，迷惑メールの特徴を自己学習し，迷惑メールであるかどうかを統計的に解析して判定する。

問14　DNS の再帰的な問合せを使ったサービス不能攻撃（DNS amp）の踏み台にされることを防止する対策はどれか。

ア　キャッシュサーバとコンテンツサーバに分離し，インターネット側からキャッシュサーバに問合せできないようにする。

イ　問合せされたドメインに関する情報を Whois データベースで確認する。

ウ　一つの DNS レコードに複数のサーバの IP アドレスを割り当て，サーバへのアクセスを振り分けて分散させるように設定する。

エ　他の DNS サーバから送られてくる IP アドレスとホスト名の対応情報の信頼性をディジタル署名で確認するように設定する。

問15 SMTP-AUTH を使ったメールセキュリティ対策はどれか。

ア　ISP 管理下の動的 IP アドレスからの電子メール送信について，管理外ネットワークのメールサーバへの SMTP 通信を禁止する。

イ　PC からの電子メール送信は，POP 接続で利用者認証済の場合にだけ許可する。

ウ　通常の SMTP のポートとは別のサブミッションポートを使用して，PC からメールサーバへの電子メール送信時の認証を行う。

エ　電子メール送信元のサーバについて DNS の逆引きが成功した場合にだけ，電子メール受信を許可する。

問16 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 サーバを実行する。
イ	セッション ID を複雑なものにする。	SSL によって通信内容を秘匿する。
ウ	バインド機構を利用する。	データベースのアカウントのもつデータベースアクセス権限を必要最小限にする。
エ	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。

問17　無線 LAN で用いられる SSID の説明として，適切なものはどれか。

ア　48 ビットのネットワーク識別子であり，アクセスポイントの MAC アドレスと一致する。

イ　48 ビットのホスト識別子であり，有線 LAN の MAC アドレスと同様の働きをする。

ウ　最長 32 オクテットのネットワーク識別子であり，接続するアクセスポイントの選択に用いられる。

エ　最長 32 オクテットのホスト識別子であり，ネットワーク上で一意である。

問18　シリアル回線で使用するものと同じデータリンクのコネクション確立やデータ転送を，LAN 上で実現するプロトコルはどれか。

ア　MPLS　　イ　PPP　　ウ　PPPoE　　エ　PPTP

問19　ネットワーク管理プロトコルである SNMP バージョン 1 のメッセージタイプのうち，事象の発生をエージェント自身が自発的にマネージャに知らせるために使用するものはどれか。

ア　get-request　　イ　get-response　　ウ　set-request　　エ　trap

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や作成，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，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　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容量ファイルのダウンロードができる。

問21　SQL の GRANT 文による権限定義に関する記述のうち，適切なものはどれか。

ア　PUBLIC 指定によって，全ての権限を与えることができる。

イ　WITH GRANT OPTION 指定によって，権限を付与可能にすることができる。

ウ　ビューに対して固有の参照権限を定義できない。

エ　表定義の SQL 文内に GRANT 文を指定することによって，権限定義ができる。

問22　システム開発で行われる各テストについて，そのテスト要求事項が定義されるアクティビティとテストの組合せのうち，適切なものはどれか。

	システム方式設計	ソフトウェア方式設計	ソフトウェア詳細設計
ア	運用テスト	システム結合テスト	ソフトウェア結合テスト
イ	運用テスト	ソフトウェア結合テスト	ソフトウェアユニットテスト
ウ	システム結合テスト	ソフトウェア結合テスト	ソフトウェアユニットテスト
エ	システム結合テスト	ソフトウェアユニットテスト	ソフトウェア結合テスト

問23　開発した製品で利用している新規技術に関して特許の出願を行った。日本において特許権の取得が可能なものはどれか。

ア　学会で技術内容を発表した日から11か月目に出願した。

イ　顧客と守秘義務の確認を取った上で技術内容を説明した後，製品発表前に出願した。

ウ　製品に使用した暗号の生成式を出願した。

エ　製品を販売した後に出願した。

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が要求している事項はどれか。

ア　潜在的な問題を低減させるために，予防処置を取らなければならない。

イ　ディジタルの構成品目の原本を，物理的又は電子的にセキュリティが保たれた書庫で管理しなければならない。

ウ　変更要求に対しては，そのリスク，影響及び事業利益について，アセスメントを行わなければならない。

エ　変更を実装する前に，変更がセキュリティ管理策に与える影響のアセスメントを行わなければならない。

問25　内部監査として実施したシステム監査で，問題点を検出後，改善勧告を行うまでの間に監査人が考慮すべき事項として，適切なものはどれか。

ア　改善事項を被監査部門へ事前に通知した場合，不備の是正が行われ，元から不備が存在しなかったように見える可能性があるので，被監査部門に秘匿する。

イ　監査人からの一方的な改善提案は実行不可能なものとなるおそれがあるので，改善勧告の前に，改善策について被監査部門との間で協議する場をもつ。

ウ　経営判断に関与することを避けるため，不備を改善する際の経済合理性などの判断を行わず，そのまま経営者に対する改善勧告とする。

エ　将来のフォローアップに際して，客観的で中立的な判断を阻害する要因となるので，改善勧告の優先度付けや取捨選択を行うことを避ける。

〔 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。
8. 試験時間中，机上に置けるもの及び使用できるものは，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（アラームなど時計以外の機能は使用不可），ハンカチ，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。