SC

平成26年度　秋期
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〕　秋の情報処理技術者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。

問題文中で共通に使用される表記ルール

各問題文中に注記がない限り，次の表記ルールが適用されているものとする。

試験問題での表記	規格・標準の名称
JIS Q 9001	JIS Q 9001:2008
JIS Q 14001	JIS Q 14001:2004
JIS Q 15001	JIS Q 15001:2006
JIS Q 20000-1	JIS Q 20000-1:2012
JIS Q 20000-2	JIS Q 20000-2:2013
JIS Q 27001	JIS Q 27001:2006
JIS Q 27002	JIS Q 27002:2006
JIS X 0160	JIS X 0160:2012
ISO 21500	ISO 21500:2012
ITIL	ITIL 2011 edition
PMBOK	PMBOK ガイド 第4版
共通フレーム	共通フレーム 2013

問1　PKI を構成する OCSP を利用する目的はどれか。

ア　誤って破棄してしまった秘密鍵の再発行処理の進捗状況を問い合わせる。

イ　ディジタル証明書から生成した鍵情報の交換が OCSP クライアントとレスポンダの間で失敗した際，認証状態を確認する。

ウ　ディジタル証明書の失効情報を問い合わせる。

エ　有効期限の切れたディジタル証明書の更新処理の進捗状況を確認する。

問2　ハッシュ関数の性質の一つである衝突発見困難性に関する記述のうち，適切なものはどれか。

ア　SHA-256 の衝突発見困難性を示す，ハッシュ値が一致する二つのメッセージの探索に要する最大の計算量は，256 の 2 乗である。

イ　SHA-256 の衝突発見困難性を示す，ハッシュ値の元のメッセージの探索に要する最大の計算量は，2 の 256 乗である。

ウ　ハッシュ値が与えられたときに，元のメッセージの探索に要する計算量の大きさによる，探索の困難性のことである。

エ　ハッシュ値が一致する二つのメッセージの探索に要する計算量の大きさによる，探索の困難性のことである。

問3　経済産業省が公表した“クラウドサービス利用のための情報セキュリティマネジメントガイドライン”が策定された目的について述べたものはどれか。

ア　JIS Q 27002 の管理策を補完し，クラウドサービス利用者が情報セキュリティ対策を円滑に行えるようにする。

イ　クラウドサービス提供事業者に対して情報セキュリティ監査を実施する方法を利用者に提示する。

ウ　クラウドサービスの利用がもたらすセキュリティリスクをサービス提供事業者の視点で提示する。

エ　セキュリティリスクの懸念が少ないクラウドサービス提供事業者を利用者が選択できるような格付け基準を提供する。

問4　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5　FIPS 140-2 を説明したものはどれか。

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標準仕様
エ　無線 LAN セキュリティ技術

問6　CSIRT の説明として，適切なものはどれか。

ア　IP アドレスの割当て方針の決定，DNS ルートサーバの運用監視，DNS 管理に関する調整などを世界規模で行う組織である。
イ　インターネットに関する技術文書を作成し，標準化のための検討を行う組織である。
ウ　企業・組織内や政府機関に設置され，コンピュータセキュリティインシデントに関する報告を受け取り，調査し，対応活動を行う組織の総称である。
エ　情報技術を利用し，宗教的又は政治的な目標を達成するという目的をもった人や組織の総称である。

問7　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 IT 製品のセキュリティ脆弱性の深刻さを評価するものはどれか。

ア　CVSS　　イ　ISMS　　ウ　PCI DSS　　エ　PMS

問8　CRYPTREC の活動内容はどれか。

ア　暗号技術の安全性，実装性及び利用実績の評価・検討を行う。

イ　情報セキュリティ政策に係る基本戦略の立案，官民における統一的，横断的な情報セキュリティ対策の推進に係る企画などを行う。

ウ　組織の情報セキュリティマネジメントシステムについて評価し認証する制度を運用する。

エ　認証機関から貸与された暗号モジュール試験報告書作成支援ツールを用いて暗号モジュールの安全性についての評価試験を行う。

問9　DNS キャッシュサーバに対して外部から行われるキャッシュポイズニング攻撃への対策のうち，適切なものはどれか。

ア　外部ネットワークからの再帰的な問合せに応答できるように，コンテンツサーバにキャッシュサーバを兼ねさせる。

イ　再帰的な問合せに対しては，内部ネットワークからのものだけに応答するように設定する。

ウ　再帰的な問合せを行う際の送信元のポート番号を固定する。

エ　再帰的な問合せを行う際のトランザクション ID を固定する。

問10　標準化団体 OASIS が，Web サイト間で認証，属性及び認可の情報を安全に交換するために策定したフレームワークはどれか。

ア　SAML　　イ　SOAP　　ウ　XKMS　　エ　XML Signature

問11 暗号化や認証機能をもち，遠隔にあるコンピュータを操作する機能をもったものはどれか。

ア IPsec　　イ L2TP　　ウ RADIUS　　エ SSH

問12 DoS 攻撃の一つである Smurf 攻撃の特徴はどれか。

ア ICMP の応答パケットを大量に送り付ける。
イ TCP 接続要求である SYN パケットを大量に送り付ける。
ウ サイズが大きい UDP パケットを大量に送り付ける。
エ サイズが大きい電子メールや大量の電子メールを送り付ける。

問13 サイドチャネル攻撃を説明したものはどれか。

ア 暗号化装置における暗号化処理時の消費電力などの測定や統計処理によって，当該装置内部の機密情報を推定する攻撃
イ 攻撃者が任意に選択した平文とその平文に対応した暗号文から数学的手法を用いて暗号鍵を推測し，同じ暗号鍵を用いて作成された暗号文を解読する攻撃
ウ 操作中の人の横から，入力操作の内容を観察することによって，ID とパスワードを盗み取る攻撃
エ 無線 LAN のアクセスポイントを不正に設置し，チャネル間の干渉を発生させることによって，通信を妨害する攻撃

問14 ディジタルフォレンジックスを説明したものはどれか。

ア　画像や音楽などのディジタルコンテンツに著作権者などの情報を埋め込む。

イ　コンピュータやネットワークのセキュリティ上の弱点を発見するテスト手法の一つであり，システムを実際に攻撃して侵入を試みる。

ウ　ネットワークの管理者や利用者などから，巧みな話術や盗み聞き，盗み見などの手段によって，パスワードなどのセキュリティ上重要な情報を入手する。

エ　犯罪に対する証拠となり得るデータを保全し，その後の訴訟などに備える。

問15 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でディジタル署名を電子メールのヘッダに付加して，受信側メールサーバで検証する。

イ　送信側メールサーバで利用者が認証されたとき，電子メールの送信が許可される。

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。

エ　ネットワーク機器で，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。

問16 認証にクライアント証明書を用いるプロトコルはどれか。

ア　EAP-MD5　　イ　EAP-PEAP　　ウ　EAP-TLS　　エ　EAP-TTLS

問17 サンドボックスの仕組みについて述べたものはどれか。

ア Web アプリケーションの脆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 侵入者をおびき寄せるために本物そっくりのシステムを設置し，侵入者の挙動などを監視する。

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 リモートアクセス環境において，認証情報やアカウンティング情報をやり取りするプロトコルはどれか。

ア CHAP　　イ PAP　　ウ PPTP　　エ RADIUS

問20 インターネット標準 RFC 5322（旧 RFC 822）に準拠した電子メールにおいて，ヘッダと本体を区別する方法はどれか。

ア <header>と</header>で囲まれた部分をヘッダ，<body>と</body>で囲まれた部分を本体とする。

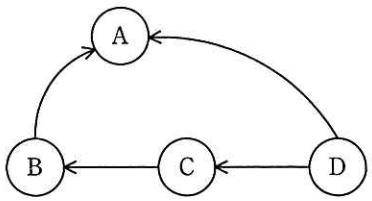
イ 1個のピリオドだけから成る行の前後でヘッダと本体を分ける。

ウ Subject フィールドがヘッダの最後であり，それ以降を本体とする。

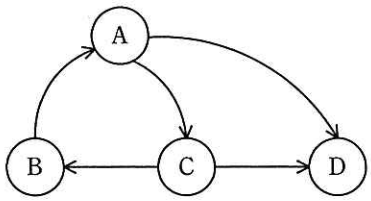
エ 最初に現れる空行の前後でヘッダと本体を分ける。

問21 トランザクション A ～ D に関する待ちグラフのうち，デッドロックが発生しているものはどれか。ここで，待ちグラフの矢印は，$X \rightarrow Y$ のとき，トランザクション X はトランザクション Y がロックしている資源のアンロックを待っていることを表す。

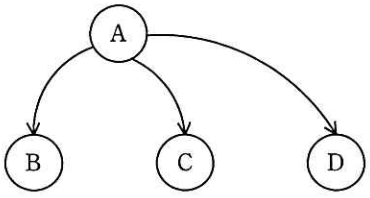
ア



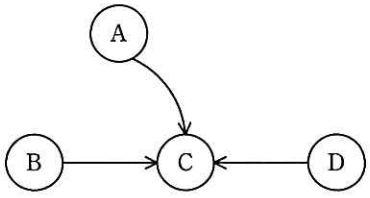
イ



ウ



エ



問22 テストで使用されるスタブ又はドライバの説明のうち，適切なものはどれか。

ア　スタブは，テスト対象モジュールからの戻り値を表示・印刷する。
イ　スタブは，テスト対象モジュールを呼び出すモジュールである。
ウ　ドライバは，テスト対象モジュールから呼び出されるモジュールである。
エ　ドライバは，引数を渡してテスト対象モジュールを呼び出す。

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 JIS Q 20000-1 で定義されるインシデントに該当するものはどれか。

ア　IT サービスの新人向け教育の依頼
イ　IT サービスやシステムの機能，使い方に対する問合せ
ウ　アプリケーションの応答の大幅な遅延
エ　新設営業所への IT サービス提供要求

問25　情報セキュリティに関する従業員の責任について，“情報セキュリティ管理基準”に基づいて監査を行った。指摘事項に該当するものはどれか。

ア　雇用の終了をもって守秘責任が解消されることが，雇用契約に定められている。

イ　定められた勤務時間以外においても守秘責任を負うことが，雇用契約に定められている。

ウ　定められた守秘責任を果たさなかった場合，相応の措置がとられることが，雇用契約に定められている。

エ　定められた内容の守秘義務契約書に署名することが，雇用契約に定められている。

〔 メ モ 用 紙 〕

〔 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，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。