SC

平成26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　特定の認証局が発行したCRL（Certificate Revocation List）に関する記述のうち，適切なものはどれか。

ア　CRLには，失効したディジタル証明書に対応する秘密鍵が登録される。

イ　CRLには，有効期限内のディジタル証明書のうち破棄されているディジタル証明書と破棄された日時の対応が提示される。

ウ　CRLは，鍵の漏えい，破棄申請の状況をリアルタイムに反映するプロトコルである。

エ　有効期限切れで失効したディジタル証明書は，所有者が新たなディジタル証明書を取得するまでの間，CRLに登録される。

問2　XML署名において署名対象であるオブジェクトの参照を指定する表記形式はどれか。

ア　OIDの形式

イ　SSIDの形式

ウ　URIの形式

エ　ディジタル証明書のシリアル番号の形式

問3　クラウドサービスにおける，従量課金を利用したEDoS（Economic Denial of Service, Economic Denial of Sustainability）攻撃の説明はどれか。

ア　カード情報の取得を目的に，金融機関が利用しているクラウドサービスに侵入する攻撃

イ　課金回避を目的に，同じハードウェア上に構築された別の仮想マシンに侵入し，課金機能を利用不可にする攻撃

ウ　クラウド利用企業の経済的な損失を目的に，リソースを大量消費させる攻撃

エ　パスワード解析を目的に，クラウド環境のリソースを悪用する攻撃

問4　スパムメールの対策として，宛先ポート番号 25 番の通信に対して ISP が実施する OP25B の説明はどれか。

ア　ISP 管理外のネットワークからの通信のうち，スパムメールのシグネチャに該当するものを遮断する。

イ　動的 IP アドレスを割り当てたネットワークから ISP 管理外のネットワークへの直接の通信を遮断する。

ウ　メール送信元のメールサーバについて DNS の逆引きができない場合，そのメールサーバからの通信を遮断する。

エ　メール不正中継の脆弱性をもつメールサーバからの通信を遮断する。

問5　PC などに内蔵されるセキュリティチップ（TPM：Trusted Platform Module）がもつ機能はどれか。

ア　TPM 間での共通鍵の交換

イ　鍵ペアの生成

ウ　ディジタル証明書の発行

エ　ネットワーク経由の乱数送信

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　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。

エ　戻りのパケットに関しては，過去に通過したリクエストパケットに対応付けられるものだけを通過させることができる。

問7　ポリモーフィック型ウイルスの説明として，適切なものはどれか。

ア　インターネットを介して，攻撃者が PC を遠隔操作する。

イ　感染するごとにウイルスのコードを異なる鍵で暗号化し，ウイルス自身を変化させて同一のパターンで検知されないようにする。

ウ　複数の OS で利用できるプログラム言語でウイルスを作成することによって，複数の OS 上でウイルスが動作する。

エ　ルートキットを利用してウイルスに感染していないように見せかけることによって，ウイルスを隠蔽する。

問8　ICMP Flood 攻撃に該当するものはどれか。

ア　HTTP GET コマンドを繰返し送ることによって，攻撃対象のサーバにコンテンツ送信の負荷を掛ける。

イ　ping コマンドを用いて大量の要求パケットを発信することによって，攻撃対象のサーバに至るまでの回線を過負荷にしてアクセスを妨害する。

ウ　コネクション開始要求に当たる SYN パケットを大量に送ることによって，攻撃対象のサーバに，接続要求ごとに応答を返すための過大な負荷を掛ける。

エ　大量の TCP コネクションを確立することによって，攻撃対象のサーバに接続を維持させ続けてリソースを枯渇させる。

問9　自ネットワークのホストへの侵入を，ファイアウォールにおいて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10 Web サーバが HTTPS 通信の応答で cookie に Secure 属性を設定したときのブラウザの処理はどれか。

ア　ブラウザは，cookie の“Secure=”に続いて指定された時間を参照し，指定された時間を過ぎている場合にその cookie を削除する。

イ　ブラウザは，cookie の“Secure=”に続いて指定されたホスト名を参照し，指定されたホストにその cookie を送信する。

ウ　ブラウザは，cookie の“Secure”を参照し，HTTPS 通信時だけその cookie を送信する。

エ　ブラウザは，cookie の“Secure”を参照し，ブラウザの終了時にその cookie を削除する。

問11 テンペスト（TEMPEST）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解析する。

問12　脆弱性検査で，対象ホストに対してポートスキャンを行った。対象ポートの状態を判定する方法のうち，適切なものはどれか。

ア　対象ポートに SYN パケットを送信し，対象ホストから“RST/ACK”パケットを受信するとき，対象ポートが開いていると判定する。

イ　対象ポートに SYN パケットを送信し，対象ホストから“SYN/ACK”パケットを受信するとき，対象ポートが閉じていると判定する。

ウ　対象ポートに UDP パケットを送信し，対象ホストからメッセージ“port unreachable”を受信するとき，対象ポートが閉じていると判定する。

エ　対象ポートに UDP パケットを送信し，対象ホストからメッセージ“port unreachable”を受信するとき，対象ポートが開いていると判定する。

問13　無線 LAN のセキュリティ対策に関する記述のうち，適切なものはどれか。

ア　EAP は，クライアント PC とアクセスポイントとの間で，あらかじめ登録した共通鍵による暗号化通信を実現できる。

イ　RADIUS では，クライアント PC とアクセスポイントとの間で公開鍵暗号方式による暗号化通信を実現できる。

ウ　SSID は，クライアント PC ごとの秘密鍵を定めたものであり，公開鍵暗号方式による暗号化通信を実現できる。

エ　WPA2 では，IEEE 802.1X の規格に沿った利用者認証及び動的に更新される暗号化鍵を用いた暗号化通信を実現できる。

問14 JVN（Japan Vulnerability Notes）などの脆弱性対策ポータルサイトで採用されている CWE（Common Weakness Enumeration）はどれか。

ア　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 製品の脆弱性を評価する手法

イ　製品を識別するためのプラットフォーム名の一覧

ウ　セキュリティに関連する設定項目を識別するための識別子

エ　ソフトウェアの脆弱性の種類の一覧

問15 Web アプリケーションの脆弱性を悪用する攻撃手法のうち，Perl の system 関数や PHP の exec 関数など外部プログラムの呼出しを可能にするための関数を利用し，不正にシェルスクリプトや実行形式のファイル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16　WAF（Web Application Firewall）のブラックリスト又はホワイトリストの説明のうち，適切なものはどれか。

ア　ブラックリストは，脆弱性があるサイトのIPアドレスを登録したものであり，該当する通信を遮断する。

イ　ブラックリストは，問題がある通信データパターンを定義したものであり，該当する通信を遮断するか又は無害化する。

ウ　ホワイトリストは，暗号化された受信データをどのように復号するかを定義したものであり，復号鍵が登録されていないデータを遮断する。

エ　ホワイトリストは，脆弱性がないサイトのFQDNを登録したものであり，登録がないサイトへの通信を遮断する。

問17　SSLに対するバージョンロールバック攻撃の説明はどれか。

ア　SSLの実装の脆弱性を用いて，通信経路に介在する攻撃者が，弱い暗号化通信方式を強制することによって，暗号化通信の内容を解読して情報を得る。

イ　SSLのハンドシェイクプロトコルの終了前で，使用暗号化アルゴリズムの変更メッセージを，通信経路に介在する攻撃者が削除することによって，通信者が暗号化なしでセッションを開始し，攻撃者がセッションの全通信を盗聴したり改ざんしたりする。

ウ　SSLを実装した環境において，攻撃者が物理デバイスから得られた消費電流の情報などを利用して秘密情報を得る。

エ　保守作業のミスや誤操作のときに回復できるようにバックアップしたSSLの旧バージョンのライブラリを，攻撃者が外部から破壊する。

問18 10M ビット／秒の LAN で接続された 4 台のノード（A，B，C，D）のうち，2 組（A と B，C と D）のノード間でそれぞれ次のファイル転送を行った場合，LAN の利用率はおよそ何％か。ここで，転送時にはファイルの大きさの 30％に当たる各種制御情報が付加されるものとする。また，LAN ではリピータハブが使用されており，更に衝突は考えないものとする。

ファイルの大きさ： 平均 1,000 バイト
ファイルの転送頻度： 平均 60 回／秒（1 組当たり）

ア 2　　イ 6　　ウ 10　　エ 12

問19 VoIP において，ユーザエージェント間のセッションの確立，変更，切断を行うプロトコルはどれか。

ア RTCP　　イ RTP　　ウ SDP　　エ SIP

問20 インターネット VPN を実現するために用いられる技術であり，ESP（Encapsulating Security Payload）や AH（Authentication Header）などのプロトコルを含むものはどれか。

ア IPsec　　イ MPLS　　ウ PPP　　エ SSL

問21 関係モデルにおける外部キーに関する記述のうち，適切なものはどれか。

ア　外部キーの値は，その関係の中で一意でなければならない。

イ　外部キーは，それが参照する候補キーと比較可能でなくてもよい。

ウ　参照先の関係に，参照元の外部キーの値と一致する候補キーが存在しなくてもよい。

エ　一つの関係に外部キーが複数存在してもよい。

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 SOA（Service Oriented Architecture）の説明はどれか。

ア　Web サービスを利用するためのインタフェースやプロトコルを規定したものである。

イ　XML を利用して，インターネット上に存在する Web サービスを検索できる仕組みである。

ウ　業務機能を提供するサービスを組み合わせることによって，システムを構築する考え方である。

エ　サービス提供者と委託者との間でサービスの内容，範囲及び品質に対する要求水準を明確にして，あらかじめ合意を得ておくことである。

問24 システムの改善に向けて提出された 4 案について，評価項目を設定して採点した結果を，採点結果表に示す。効果及びリスクについては 5 段階評価とし，それぞれの評価項目の重要度に応じて，重み付け表に示すとおりの重み付けを行った上で次の式で総合評価点を算出したとき，総合評価点が最も高い改善案はどれか。

〔総合評価点の算出式〕

総合評価点 ＝ 効果の総評価点 － リスクの総評価点

採点結果表

評価項目＼案		案1	案2	案3	案4
効果	セキュリティ強化	3	4	5	2
	システム運用品質向上	2	4	2	5
	作業コスト削減	5	4	2	4
リスク	スケジュールリスク	2	4	1	5
	技術リスク	4	1	5	1

重み付け表

評価項目		重み
効果	セキュリティ強化	4
	システム運用品質向上	2
	作業コスト削減	3
リスク	スケジュールリスク	8
	技術リスク	3

ア 案1　　イ 案2　　ウ 案3　　エ 案4

問25　システム監査報告書に記載された改善勧告に対して，被監査部門から提出された改善計画を経営者がITガバナンスの観点から評価する際の方針のうち，適切なものはどれか。

ア　1年以内に実現できる改善を実施する。

イ　経営資源の状況を踏まえて改善を実施する。

ウ　情報システムの機能面の改善に絞って実施する。

エ　被監査部門の予算の範囲内で改善を実施する。

〔 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。