SC

平成28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 27000	JIS Q 27000:2014
JIS Q 27001	JIS Q 27001:2014
JIS Q 27002	JIS Q 27002:2014
JIS X 0160	JIS X 0160:2012
ISO 21500	ISO 21500:2012
ITIL	ITIL 2011 edition
PMBOK	PMBOK ガイド 第5版
共通フレーム	共通フレーム 2013

問１　CRL（Certificate Revocation List）に掲載されるものはどれか。

ア　有効期限切れになったディジタル証明書の公開鍵
イ　有効期限切れになったディジタル証明書のシリアル番号
ウ　有効期限内に失効したディジタル証明書の公開鍵
エ　有効期限内に失効したディジタル証明書のシリアル番号

問２　次の攻撃において，攻撃者がサービス不能にしようとしている標的はどれか。

〔攻撃〕
(1) A社ドメイン配下のサブドメイン名を，ランダムに多数生成する。
(2) (1)で生成したサブドメイン名に関する大量の問合せを，多数の第三者の DNS キャッシュサーバに分散して送信する。
(3) (2)で送信する問合せの送信元 IP アドレスは，問合せごとにランダムに設定して詐称する。

ア　A社ドメインの権威 DNS サーバ
イ　A社内の利用者 PC
ウ　攻撃者が詐称した送信元 IP アドレスに該当する利用者 PC
エ　第三者の DNS キャッシュサーバ

問３　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　有効期限が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４　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５　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　衝突発見困難性とは，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　衝突発見困難性とは，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６　情報セキュリティにおけるエクスプロイトコードに該当するものはどれか。

ア　同じセキュリティ機能の製品に乗り換える場合に，CSV など他の製品が取り込める形式でファイルを出力するプログラム

イ　コンピュータに接続されたハードディスクなどの外部記憶装置や，その中に保存されている暗号化されたファイルなどを閲覧，管理するソフトウェア

ウ　セキュリティ製品を設計する際の早い段階から実際に動作する試作品を作成し，それに対する利用者の反応を見ながら徐々に完成に近づける開発手法

エ　ソフトウェアやハードウェアの脆弱(ぜい)性を利用するために作成されたプログラム

問7　DoS 攻撃の一つである Smurf 攻撃はどれか。

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8　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 で標準化されている。
イ　ディジタル証明書は，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9　暗号に関連するデータのうち，次に示す処理で出力可能なものはどれか。

〔処理〕

(1)　カウンタを初期化する。

(2)　その時点に得た時刻データを共通鍵で暗号化する。

(3)　カウンタの値と(2)の結果のXORをとり，さらに共通鍵で暗号化する。

(4)　(3)の結果を出力する。

(5)　(3)の結果と(2)の結果のXORをとり，さらに共通鍵で暗号化する。

(6)　(5)の結果をカウンタの新しい値とする。

(7)　(4)の出力について，必要とする分の数を得るまで(2)～(6)を繰り返す。

ア　擬似乱数　　イ　ディジタル証明書

ウ　ハッシュ値　　エ　メッセージ認証コード

問10　“サイバー情報共有イニシアティブ（J-CSIP）”の説明はどれか。

ア　暗号技術の調査を行い，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を公表するためのプロジェクト

イ　検知したサイバー攻撃の情報を公的機関に集約し，高度なサイバー攻撃対策につなげていく取組み

ウ　制御システムにおけるセキュリティマネジメントシステムの認証制度

エ　脆弱性関連情報の発見から公表に至るまでの対処プロセス

問11　JIS Q 27000 における情報セキュリティリスクに関する定義のうち，適切なものはどれか。

ア　脅威とは，一つ以上の要因によって悪用される可能性がある，資産又は管理策の弱点のことである。

イ　脆弱性とは，望ましくないインシデントを引き起こし，システム又は組織に損害を与える可能性がある潜在的な原因のことである。

ウ　リスク対応とは，リスクの大きさが，受容可能か又は許容可能かを決定するために，リスク分析の結果をリスク基準と比較するプロセスのことである。

エ　リスク特定とは，リスクを発見，認識及び記述するプロセスのことであり，リスク源，事象，それらの原因及び起こり得る結果の特定が含まれる。

問12　DNS キャッシュポイズニング攻撃に対して有効な対策はどれか。

ア　DNS サーバで，マルウェアの侵入をリアルタイムに検知する。

イ　DNS 問合せに使用する DNS ヘッダ内の ID を固定せずにランダムに変更する。

ウ　DNS 問合せに使用する送信元ポート番号を 53 番に固定する。

エ　外部からの DNS 問合せに対しては，宛先ポート番号 53 のものだけに応答する。

問13　スパムメールの対策として，宛先ポート番号 25 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14　ディジタルフォレンジックスに該当するものはどれか。

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　犯罪に関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　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したいとき，ファイアウォールのルールで“通過禁止”に設定するものはどれか。

ア　ICMP　　イ　TCP のポート番号 21

ウ　TCP のポート番号 110　　エ　UDP のポート番号 123

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-FAST　　イ　EAP-MD5　　ウ　EAP-TLS　　エ　EAP-TTLS

問17　電子メールを暗号化する三つのプロトコルについて，公開鍵を用意する単位の適切な組合せはどれか。

	PGP	S/MIME	SMTP over TLS
ア	メールアドレスごと	メールアドレスごと	メールサーバごと
イ	メールアドレスごと	メールサーバごと	メールアドレスごと
ウ	メールサーバごと	メールアドレスごと	メールアドレスごと
エ	メールサーバごと	メールサーバごと	メールサーバごと

問18　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19　IPv4 ネットワークで IP アドレスを割り当てる際に，DHCP クライアントと DHCP サーバ間でやり取りされるメッセージの順序として，適切なものはどれか。

ア　DHCPDISCOVER，DHCPACK，DHCPREQUEST，DHCPOFFER
イ　DHCPDISCOVER，DHCPOFFER，DHCPREQUEST，DHCPACK
ウ　DHCPREQUEST，DHCPACK，DHCPDISCOVER，DHCPOFFER
エ　DHCPREQUEST，DHCPDISCOVER，DHCPOFFER，DHCPACK

問20　TCP のサブミッションポート（ポート番号 587）の説明として，適切なものはどれか。

ア　FTP サービスで，制御用コネクションのポート番号 21 とは別にデータ転送用に使用する。
イ　Web アプリケーションで，ポート番号 80 の HTTP 要求とは別に，サブミットボタンをクリックした際の入力フォームのデータ送信に使用する。
ウ　コマンド操作の遠隔ログインで，通信内容を暗号化するために TELNET のポート番号 23 の代わりに使用する。
エ　電子メールサービスで，迷惑メール対策として SMTP のポート番号 25 の代わりに使用する。

問21　“アカウント”表に対して，SQL 文を実行したとき，“アカウント”表の全ての行が取得される入力パラメタはどれか。ここで，入力パラメタのエスケープ処理は行わない。また，“;”は SQL 文の終端として解釈されるものとする。

アカウント

ID	ユーザ名	メールアドレス
A001	TARO JOHO	t-joho@email.org.jp
A002	JIRO JOHO	j-joho@email.org.jp
A003	HANAKO JOHO	h-joho@email.org.jp

〔SQL 文〕

```
SELECT ID,ユーザ名,メールアドレス FROM アカウント
  WHERE ユーザ名 = '［入力パラメタ］';
```

ア　' OR '--' = '--

イ　' OR ユーザ名 = 'ユーザ名

ウ　'-- OR 1 = 1

エ　¥' OR 1 = 1 ';--

問22　フェールセーフの考えに基づいて設計したものはどれか。

ア　乾電池のプラスとマイナスを逆にすると，乾電池が装填できないようにする。

イ　交通管制システムが故障したときには，信号機に赤色が点灯するようにする。

ウ　ネットワークカードのコントローラを二重化しておき，故障したコントローラの方を切り離しても運用できるようにする。

エ　ハードディスクに RAID1 を採用して，MTBF で示される信頼性が向上するようにする。

問23　アジャイルソフトウェア開発などで導入されている“ペアプログラミング”の説明はどれか。

ア　開発工程の初期段階に要求仕様を確認するために，プログラマと利用者がペアとなり，試作した画面や帳票を見て，相談しながらプログラムの開発を行う。

イ　効率よく開発するために，2 人のプログラマがペアとなり，メインプログラムとサブプログラムを分担して開発を行う。

ウ　短期間で開発するために，2 人のプログラマがペアとなり，作業と休憩を交代しながら長時間にわたって連続でプログラムの開発を行う。

エ　品質の向上や知識の共有を図るために，2 人のプログラマがペアとなり，その場で相談したりレビューしたりしながら，一つのプログラムの開発を行う。

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　CMDB に記録されている CI 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。

イ　潜在的な問題を低減させるために，予防処置をとらなければならない。

ウ　変更要求が情報セキュリティ基本方針及び管理策に与える潜在的影響を評価しなければならない。

エ　変更要求の受入れについての意思決定では，リスク，事業利益及び技術的実現可能性を考慮しなければならない。

問25　組織体が情報システムにまつわるリスクに対するコントロールを適切に整備・運用する目的として，“システム管理基準”に示されているものはどれか。

ア　システム監査業務の品質を確保し，有効かつ効率的に監査を実施するため

イ　情報システムが，組織体の目的を実現するように安全，有効かつ効率的に機能するため

ウ　情報セキュリティに係るリスクのマネジメントが効果的に実施されるよう，リスクマネジメントに基づくコントロールの整備・運用の状況を評価するため

エ　リスクに対するコントロールをシステム監査人が評価し，保証又は助言を行い，IT ガバナンスの実現に寄与するため

〔 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（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。