SC

平成27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　Webのショッピングサイトを安全に利用するため，Webサイトの SSL 証明書を表示して内容を確認する。Web サイトが，EV SSL 証明書を採用している場合，存在するサブジェクトフィールドの Organization Name に記載されているものはどれか。

ア　Webサイトの運営団体の組織名
イ　証明書の登録業務を行う機関（RA）の組織名
ウ　証明書の発行業務を行う機関（CA）の組織名
エ　ドメイン名の登録申請を受け付ける機関（レジストラ）の組織名

問2　IEEE 802.1X で使われる EAP-TLS によって実現される認証はどれか。

ア　CHAP を用いたチャレンジレスポンスによる利用者認証
イ　あらかじめ登録した共通鍵によるサーバ認証と，時刻同期のワンタイムパスワードによる利用者認証
ウ　ディジタル証明書による認証サーバとクライアントの相互認証
エ　利用者 ID とパスワードによる利用者認証

問3　RLO（Right-to-Left Override）を利用した手口の説明はどれか。

ア　“コンピュータウイルスに感染している”といった偽の警告を出して利用者を脅し，ウイルス対策ソフトの購入などを迫る。
イ　脆弱(ぜいじゃく)性があるホストやシステムをあえて公開し，攻撃の内容を観察する。
ウ　ネットワーク機器の MIB 情報のうち監視項目の値の変化を感知し，セキュリティに関するイベントを SNMP マネージャに通知するように動作させる。
エ　文字の表示順を変える制御文字を利用し，ファイル名の拡張子を偽装する。

問4　VA（Validation Authority）の役割はどれか。

ア　ディジタル証明書の失効状態についての問合せに応答する。
イ　ディジタル証明書を作成するためにディジタル署名する。
ウ　認証局に代わって属性証明書を発行する。
エ　本人確認を行い，ディジタル証明書の発行を指示する。

問5　サイドチャネル攻撃の説明はどれか。

ア　暗号アルゴリズムを実装した攻撃対象の物理デバイスから得られる物理量（処理時間や消費電流など）やエラーメッセージから，攻撃対象の機密情報を得る。
イ　企業などの機密情報を詐取するソーシャルエンジニアリングの手法の一つであり，不用意に捨てられた機密情報の印刷物をオフィスの紙ゴミの中から探し出す。
ウ　通信を行う 2 者間に割り込んで，両者が交換する情報を自分のものとすり替えることによって，気付かれることなく盗聴する。
エ　データベースを利用する Web サイトに入力パラメタとして SQL 文の断片を与えることによって，データベースを改ざんする。

問6　X.509 における CRL（Certificate Revocation List）についての説明のうち，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，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を CRL に登録することがある。

問7 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 CVE（Common Vulnerabilities and Exposures）識別子の説明はどれか。

ア　コンピュータで必要なセキュリティ設定項目を識別するための識別子である。

イ　脆弱性が利用されて改ざんされた Web サイトのスクリーンショットを識別するための識別子である。

ウ　製品に含まれる脆弱性を識別するための識別子である。

エ　セキュリティ製品を識別するための識別子である。

問8 総務省及び経済産業省が策定した“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（CRYPTREC 暗号リスト）”を構成する暗号リストの説明のうち，適切なものはどれか。

ア　推奨候補暗号リストとは，CRYPTREC によって安全性及び実装性能が確認された暗号技術のうち，市場における利用実績が十分であるか今後の普及が見込まれると判断され，当該技術の利用を推奨するもののリストである。

イ　推奨候補暗号リストとは，候補段階に格下げされ，互換性維持目的で利用する暗号技術のリストである。

ウ　電子政府推奨暗号リストとは，CRYPTREC によって安全性及び実装性能が確認された暗号技術のうち，市場における利用実績が十分であるか今後の普及が見込まれると判断され，当該技術の利用を推奨するもののリストである。

エ　電子政府推奨暗号リストとは，推奨段階に格下げされ，互換性維持目的で利用する暗号技術のリストである。

問9 IPsecに関する記述のうち，適切なものはどれか。

ア　IKEはIPsecの鍵交換のためのプロトコルであり，ポート番号80が使用される。

イ　暗号化アルゴリズムとして，HMAC-SHA1が使用される。

ウ　トンネルモードを使用すると，エンドツーエンドの通信で用いるIPのヘッダまで含めて暗号化される。

エ　ホストAとホストBとの間でIPsecによる通信を行う場合，認証や暗号化アルゴリズムを両者で決めるためにESPヘッダではなくAHヘッダを使用する。

問10 NTPを使った増幅型のDDoS攻撃に対して，NTPサーバが踏み台にされることを防止する対策として，適切なものはどれか。

ア　NTPサーバの設定変更によって，NTPサーバの状態確認機能（monlist）を無効にする。

イ　NTPサーバの設定変更によって，自ネットワーク外のNTPサーバへの時刻問合せができないようにする。

ウ　ファイアウォールの設定変更によって，NTPサーバが存在する自ネットワークのブロードキャストアドレス宛てのパケットを拒否する。

エ　ファイアウォールの設定変更によって，自ネットワーク外からの，NTP以外のUDPサービスへのアクセスを拒否する。

問11　マルウェアの活動傾向などを把握するための観測用センサが配備されるダークネットはどれか。

ア　インターネット上で到達可能，かつ，未使用のIPアドレス空間
イ　組織に割り当てられている IP アドレスのうち，コンピュータで使用されているIPアドレス空間
ウ　通信事業者が他の通信事業者などに貸し出す光ファイバ設備
エ　マルウェアに狙われた制御システムのネットワーク

問12　rootkitに含まれる機能はどれか。

ア　OSの中核であるカーネル部分の脆弱性を分析する。
イ　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。
ウ　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。
エ　不正侵入してOSなどに組み込んだものを隠蔽する。

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，許可リストにないメール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　利用者が振り分けた迷惑メールから特徴を学習し，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 DNSSEC で実現できることはどれか。

ア　DNS キャッシュサーバからの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 の打ち間違いを悪用して，偽サイトに誘導する攻撃の検知

問15 DNS の再帰的な問合せを使ったサービス不能攻撃（DNS amp 攻撃）の踏み台にされることを防止する対策はどれか。

ア　DNS 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 DNS キャッシュサーバに問合せできないようにする。

イ　問合せがあっ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16 SMTP-AUTH の特徴はどれか。

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 接続を禁止する。

イ　PC からメールサーバへの電子メール送信時に，ユーザアカウントとパスワードによる利用者認証を行う。

ウ　PC からメールサーバへの電子メール送信は，POP 接続で利用者認証済みの場合にだけ許可する。

エ　電子メール送信元のサーバが，送信元ドメインの DNS に登録されていることを確認して，電子メールを受信する。

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 TCP ヘッダに含まれる情報はどれか。

ア　宛先ポート番号　　イ　送信元 IP アドレス

ウ　パケット生存時間（TTL）　　エ　プロトコル番号

問19 192.168.1.0/24 のネットワークアドレスを，16 個のサブネットに分割したときのサブネットマスクはどれか。

ア 255.255.255.192　　イ 255.255.255.224
ウ 255.255.255.240　　エ 255.255.255.248

問20 HTTP のヘッダ部で指定するものはどれか。

ア HTML バージョン情報（DOCTYPE 宣言）
イ POST リクエストのエンティティボディ（POST データ）
ウ Web サーバと Web ブラウザ間の状態を管理するクッキー（Cookie）
エ Web ページのタイトル（<TITLE>タグ）

問21 分散トランザクション処理で利用される 2 相コミットプロトコルでは，コミット処理を開始する調停者（coordinator）と，調停者からの指示を受信してから必要なアクションを開始する参加者（participant）がいる。この 2 相コミットプロトコルに関する記述のうち，適切なものはどれか。

ア 参加者は，フェーズ 1 で調停者にコミット了承の応答を返してしまえば，フェーズ 2 のコミット要求を受信していなくても，ローカルにコミット処理が進められる。
イ 調停者に障害が発生するタイミングによっては，その回復処理が終わらない限り，参加者全員がコミットもロールバックも行えない事態が起こる。
ウ 一つの分散トランザクションに複数の調停者及び参加者が存在し得る。例えば，5 個のシステム（プログラム）が関与している場合，調停者の数が 2，参加者の数が 3 となり得る。
エ フェーズ 1 で応答のない参加者が存在しても，調停者は強制的にそのトランザクションをコミットすることができる。

問22　共通フレームによれば，システム要件の評価タスクにおいて見極めることはどれか。

ア　システム要件とシステム方式との間に一貫性があるかどうか。
イ　システム要件とシステム方式との関連が追跡できるかどうか。
ウ　システム要件を満たすシステム方式設計が実現可能かどうか。
エ　ソフトウェア品目が割り当てられたシステム要件を満たすかどうか。

問23　マッシュアップを利用して Web コンテンツを表示している例として，最も適切なものはどれか。

ア　Web ブラウザにプラグインを組み込み，動画やアニメーションを表示する。
イ　地図上のカーソル移動に伴い，Web ページを切り替えずにスクロール表示する。
ウ　鉄道経路の探索結果上に，各鉄道会社の Web ページへのリンクを表示する。
エ　店舗案内の Web ページ上に，他のサイトが提供する地図検索機能を利用して出力された情報を表示する。

問24　データセンタにおけるコールドアイルの説明として，適切なものはどれか。

ア　IT 機器の冷却を妨げる熱気をラックの前面（吸気面）に回り込ませないための板であり，IT 機器がマウントされていないラックの空き部分に取り付ける。
イ　寒冷な外気をデータセンタ内に直接導入して IT 機器を冷却するときの，データセンタへの外気の吸い込み口である。
ウ　空調機からの冷気と IT 機器からの熱排気を分離するために，ラックの前面（吸気面）同士を対向配置したときの，ラックの前面同士に挟まれた冷気の通る部分である。
エ　発熱量が多い特定の領域に対して，全体空調とは別に個別空調装置を設置するときの，個別空調用の冷媒を通すパイプである。

問25　入出金管理システムから出力された入金データファイルを，売掛金管理システムが読み込んでマスタファイルを更新する。入出金管理システムから売掛金管理システムへのデータ受渡しの正確性及び網羅性を確保するコントロールはどれか。

ア　売掛金管理システムにおける入力データと出力結果とのランツーランコントロール

イ　売掛金管理システムのマスタファイル更新におけるタイムスタンプ機能

ウ　入金額及び入金データ件数のコントロールトータルのチェック

エ　入出金管理システムへの入力のエディットバリデーションチェック

〔 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。