SC

平成25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 20000-2:2007
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　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2　XML ディジタル署名の特徴はどれか。

ア　XML 文書中の，指定したエレメントに対して署名することができる。

イ　エンベロービング署名（Enveloping Signature）では一つの署名対象に必ず複数の署名を付ける。

ウ　署名形式として，CMS（Cryptographic Message Syntax）を用いる。

エ　署名対象と署名アルゴリズムを ASN.1 によって記述する。

問3　共通鍵暗号方式で，100 人の送受信者のそれぞれが，相互に暗号化通信を行うときに必要な共通鍵の総数は幾つか。

ア　200　　イ　4,950　　ウ　9,900　　エ　10,000

問4　無線 LAN における WPA2 の特徴はどれか。

ア　AH と ESP の機能によって認証と暗号化を実現する。

イ　暗号化アルゴリズムに AES を採用した CCMP（Counter-mode with CBC-MAC Protocol）を使用する。

ウ　端末とアクセスポイントの間で通信を行う際に，SSL Handshake Protocol を使用して，お互いが正当な相手かどうかを認証する。

エ　利用者が設定する秘密鍵と，製品で生成する IV（Initialization Vector）とを連結した数字を基に，データをフレームごとに RC4 で暗号化する。

問5　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　脆弱性を利用して改ざんされた Web サイトの画面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6　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，機密情報の違いによって演算の処理時間に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になるようにする。

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7　テンペスト技術の説明とその対策として，適切なものはどれか。

ア　ディスプレイなどから放射される電磁波を傍受し，表示内容などを盗み見る技術であり，電磁波を遮断することによって対抗する。

イ　データ通信の途中でパケットを横取りし，内容を改ざんする技術であり，ディジタル署名を利用した改ざん検知によって対抗する。

ウ　マクロウイルスにおいて使われる技術であり，ウイルス対策ソフトを導入し，最新の定義ファイルを適用することによって対抗する。

エ　無線 LAN の信号を傍受し，通信内容を解析する技術であり，通信パケットを暗号化することによって対抗する。

問8　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9　共通鍵暗号の鍵を見つけ出す，ブルートフォース攻撃に該当するものはどれか。

ア　1 組の平文と暗号文が与えられたとき，全ての鍵候補を一つずつ試して鍵を見つけ出す。

イ　平文と暗号文と鍵の関係を代数式に表して数学的に鍵を見つけ出す。

ウ　平文の一部分の情報と暗号文の一部分の情報との間の統計的相関を手掛かりに鍵を見つけ出す。

エ　平文を一定量変化させたときの暗号文の変化から鍵を見つけ出す。

問10　利用者 PC がボットに感染しているかどうかを hosts ファイルで確認するとき，設定内容が改ざんされていないと判断できるものはどれか。ここで，hosts ファイルには設定内容が 1 行だけ書かれているものとする。

	設定内容	説　明
ア	127.0.0.1　a.b.com	a.b.com は OS 提供元の FQDN を示す。
イ	127.0.0.1　c.d.com	c.d.com は PC 製造元の FQDN を示す。
ウ	127.0.0.1　e.f.com	e.f.com はウイルス定義ファイルの提供元の FQDN を示す。
エ	127.0.0.1　localhost	localhost は利用者 PC 自身を示す。

問11　ルートキット（rootkit）を説明したものはどれか。

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

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　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15　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 を乱数で生成する。	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16　ディレクトリトラバーサル攻撃はどれか。

ア　攻撃者が，OS の操作コマンドを利用するアプリケーションに対して，OS のディレクトリ作成コマンドを渡して実行する。

イ　攻撃者が，SQL 文のリテラル部分の生成処理に問題があるアプリケーションに対して，任意の SQL 文を渡して実行する。

ウ　攻撃者が，シングルサインオンを提供するディレクトリサービスに対して，不正に入手した認証情報を用いてログインし，複数のアプリケーションを不正使用する。

エ　攻撃者が，ファイル名の入力を伴うアプリケーションに対して，上位のディレクトリを意味する文字列を使って，非公開のファイルにアクセスする。

問17　LANの制御方式に関する記述のうち，適切なものはどれか。

ア　CSMA/CD 方式では，単位時間当たりの送出フレーム数が増していくと，衝突の頻度が増すので，スループットはある値をピークとして，その後下がる。

イ　CSMA/CD 方式では，一つの装置から送出されたフレームが順番に各装置に伝送されるので，リング状のLANに適している。

ウ　TDMA 方式では，伝送路上におけるフレームの伝搬遅延時間による衝突が発生する。

エ　トークンパッシング方式では，トークンの巡回によって送信権を管理しているので，トラフィックが増大すると，CSMA/CD 方式に比べて伝送効率が急激に低下する。

問18　コンピュータとスイッチングハブ（レイヤ 2 スイッチ）の間，又は 2 台のスイッチングハブの間を接続する複数の物理回線を論理的に 1 本の回線に束ねる技術はどれか。

ア　スパニングツリー　　イ　ブリッジ

ウ　マルチホーミング　　エ　リンクアグリゲーション

問19　電子メールシステムにおいて，利用者端末がサーバから電子メールを受信するために使用するプロトコルであり，選択した電子メールだけを利用者端末へ転送する機能，サーバ上の電子メールを検索する機能，電子メールのヘッダだけを取り出す機能などをもつものはどれか。

ア　IMAP4　　イ　MIME　　ウ　POP3　　エ　SMTP

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 80 番の 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 分散データベースシステムにおける“分割に対する透過性”を説明したものはどれか。

ア　データの格納サイトが変更されても，利用者のアプリケーションや操作法に影響がないこと

イ　同一のデータが複数のサイトに格納されていても，利用者はそれを意識せずに利用できること

ウ　一つの表が複数のサイトに分割されて格納されていても，利用者はそれを意識せずに利用できること

エ　利用者がデータベースの位置を意識せずに利用できること

問22 安全性と信頼性について，次の方針でプログラム設計を行う場合，その方針を表す用語はどれか。

“不特定多数の人が使用するプログラムには，自分だけが使用するプログラムに比べて，より多くのデータチェックの機能を組み込む。プログラムが処理できるデータの前提条件を文書に書いておくだけでなく，その前提条件を満たしていないデータが実際に入力されたときは，エラーメッセージを表示して再入力を促すようにプログラムを作る。”

ア　フールプルーフ　　イ　フェールセーフ
ウ　フェールソフト　　エ　フォールトトレラント

問23 表は，システムへの要求の明確さに応じた開発方針と，開発方針に適した開発モデルの組である。a～cに該当する開発モデルの組合せはどれか。

要求の明確さ	開発方針	開発モデル
要求が明確になっている。	全機能を一斉に開発する。	a
要求に不明確な部分がある。	簡易なシステムを実装し，動作を評価しながら要求を早期に明確にする。その後は全機能を一斉に開発する。	b
要求に変更される可能性が高い部分がある。	最初に要求が確定した部分だけを開発する。その後に要求が確定した部分を逐次追加していく。	c

	a	b	c
ア	ウォータフォールモデル	進化的モデル	プロトタイピングモデル
イ	ウォータフォールモデル	プロトタイピングモデル	進化的モデル
ウ	進化的モデル	ウォータフォールモデル	プロトタイピングモデル
エ	プロトタイピングモデル	ウォータフォールモデル	進化的モデル

問24 IT サービスマネジメントの問題管理プロセスにおけるプロアクティブな活動はどれか。

ア　インシデントの根本原因を究明する。
イ　過去に同様のインシデントが発生していないか調査する。
ウ　過去のインシデントの記録を分析し，今後起こりそうなインシデントを予測する。
エ　根本原因を突き止めた問題を既知のエラーとして登録する。

問25 被監査企業が SaaS をサービス利用契約して業務を実施している場合，被監査企業のシステム監査人が SaaS の利用者環境から SaaS へのアクセスコントロールを評価できる対象の ID はどれか。

ア　DBMS の管理者 ID
イ　アプリケーションの利用者 ID
ウ　サーバの OS の利用者 ID
エ　ストレージデバイスの管理者 ID

〔 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。