SC

平成28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 9001:2015
JIS Q 14001	JIS Q 14001:2015
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　RADIUS や DIAMETER が提供する AAA フレームワークの構成要素は，認証（Authentication）及び認可（Authorization）の他にどれか。

ア　Accounting　　イ　Activation

ウ　Audit　　エ　Augmented Reality

問２　NTP リフレクション攻撃の特徴はどれか。

ア　攻撃対象である NTP サーバに高頻度で時刻を問い合わせる。

イ　攻撃対象である NTP サーバの時刻情報を書き換える。

ウ　送信元を偽って，NTP サーバに echo request を送信する。

エ　送信元を偽って，NTP サーバにレスポンスデータが大きくなる要求を送信する。

問３　POODLE（CVE-2014-3566）攻撃の説明はどれか。

ア　SSL 3.0 のサーバプログラムの脆弱性を突く攻撃であり，サーバのメモリに不正アクセスして秘密鍵を窃取できる。

イ　SSL 3.0 を使用した通信において，ブロック暗号の CBC モード利用時の脆弱性を突く攻撃であり，パディングを悪用して暗号化通信の内容を解読できる。

ウ　TLS 1.2 のプロトコル仕様の脆弱性を突く攻撃であり，TLS の旧バージョンにダウングレードして暗号化通信の内容を解読できる。

エ　TLS 1.2 を使用した通信において，Diffie-Hellman 鍵交換アルゴリズムの脆弱性を突く攻撃であり，交換されたセッション鍵を窃取して暗号化通信の内容を解読できる。

問4　XML ディジタル署名の特徴のうち，適切なものはどれか。

ア　XML 文書中の，任意のエレメントに対してデタッチ署名（Detached Signature）を付けることができる。

イ　エンベローピング署名（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5　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6　リスクベース認証に該当するものはどれか。

ア　インターネットからの全てのアクセスに対し，トークンで生成されたワンタイムパスワードで認証する。

イ　インターネットバンキングでの連続する取引において，取引の都度，乱数表の指定したマス目にある英数字を入力させて認証する。

ウ　利用者の IP アドレスなどの環境を分析し，いつもと異なるネットワークからのアクセスに対して追加の認証を行う。

エ　利用者の記憶，持ち物，身体の特徴のうち，必ず二つ以上の方式を組み合わせて認証する。

問7　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８　CRYPTREC の主な活動内容はどれか。

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　Cookie に secure 属性を付けなかったときと比較した，付けたときの動作の差はどれか。

ア　Cookie に指定された有効期間を過ぎると，Cookie が無効化される。

イ　JavaScript による Cookie の読出しが禁止される。

ウ　URL のスキームが https のページのときだけ，Web ブラウザから Cookie が送出される。

エ　Web ブラウザがアクセスする URL 内のパスと Cookie によって指定されたパスのプレフィックスが一致するとき，Web ブラウザから Cookie が送出される。

問10　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，ダークネットともいわれるものはどれか。

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の特徴はどれか。

ア　OSなどに不正に組み込んだツールを隠蔽する。
イ　OSの中核であるカーネル部分の脆弱性を分析する。
ウ　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。
エ　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。

問13　DNSSECで実現できることはどれか。

ア　DNSキャッシュサーバが得た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14　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15　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，暗号化通信の区間において，エンドツーエンドの通信で用いる元の IP のヘッダを含めて暗号化できる。
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　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。
ウ　メールクライアント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。
エ　メールクライアント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。

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　DNS に関する記述のうち，適切なものはどれか。

ア　DNS サーバに対して，IP アドレスに対応するドメイン名，又はドメイン名に対応する IP アドレスを問い合わせるクライアントソフトウェアを，リゾルバという。

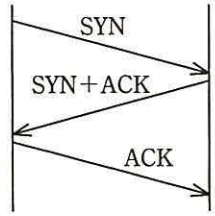
イ　問合せを受けた DNS サーバが要求されたデータをもっていない場合に，他の DNS サーバを参照先として回答することを，ゾーン転送という。

ウ　ドメイン名に対応する IP アドレスを求めることを，逆引きという。

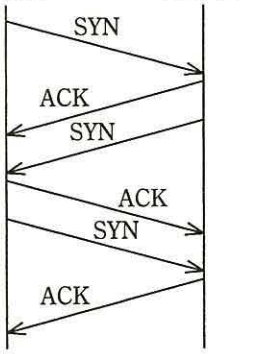
エ　ドメイン名を管理する DNS サーバを指定する資源レコードのことを，CNAME という。

問19　TCP のコネクション確立方式である 3 ウェイハンドシェイクを表す図はどれか。

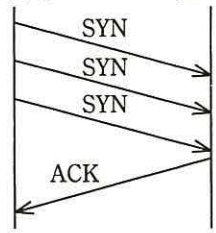
ア



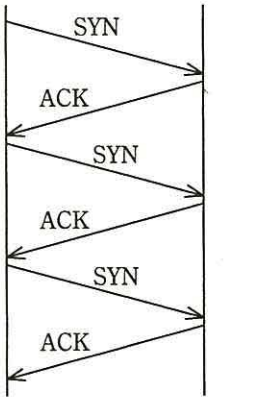
イ



ウ



エ



問20　TCP に関する記述のうち，適切なものはどれか。

ア　OSI 基本参照モデルのネットワーク層の機能である。

イ　ウィンドウ制御の単位は，バイトではなくビットである。

ウ　確認応答がない場合は再送処理によってデータ回復を行う。

エ　データの順序番号をもたないので，データは受信した順番のままで処理する。

問21　システム障害発生時には，データベースの整合性を保ち，かつ，最新のデータベース状態に復旧する必要がある。このために，DBMS がトランザクションのコミット処理を完了とするタイミングとして，適切なものはどれか。

ア　アプリケーションの更新命令完了時点

イ　チェックポイント処理完了時点

ウ　ログバッファへのコミット情報書込み完了時点

エ　ログファイルへのコミット情報書込み完了時点

問22　システム開発で行うテストについて，テスト要求事項を定義するアクティビティと対応するテストの組合せのうち，適切なものはどれか。

	システム方式設計	ソフトウェア方式設計	ソフトウェア詳細設計
ア	運用テスト	システム結合テスト	ソフトウェア結合テスト
イ	運用テスト	ソフトウェア結合テスト	ソフトウェアユニットテスト
ウ	システム結合テスト	ソフトウェア結合テスト	ソフトウェアユニットテスト
エ	システム結合テスト	ソフトウェアユニットテスト	ソフトウェア結合テスト

問23　表はシステムの特性や制約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。

開発方針	開発モデル
最初にコア部分を開発し，順次機能を追加していく。	a
要求が明確なので，全機能を一斉に開発する。	b
要求に不明確な部分があるので，開発を繰り返しながら徐々に要求内容を洗練していく。	c

	a	b	c
ア	進化的モデル	ウォータフォールモデル	段階的モデル
イ	段階的モデル	ウォータフォールモデル	進化的モデル
ウ	ウォータフォールモデル	進化的モデル	段階的モデル
エ	進化的モデル	段階的モデル	ウォータフォールモデル

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 サービス応答時間の大幅な超過

イ　IT サービスの新人向け教育の依頼

ウ　IT サービスやシステムの機能，使い方に対する問合せ

エ　新設営業所に対する IT サービス提供の要求

問25　データベースに対する不正アクセスの防止・発見を目的としたアクセスコントロールについて，“システム管理基準”への準拠性を確認する監査手続として，適切なものはどれか。

ア　利用者がデータベースにアクセスすることによって業務が効率的に実施できるかどうかを確認するために，システム仕様書を閲覧する。

イ　利用者がデータベースにアクセスするための画面の操作手順が操作ミスを起こしにくい設計になっているかどうかを確認するために，利用者にヒアリングする。

ウ　利用者が要求した応答時間が実現できているかどうかを確認するために，データベースにアクセスしてから出力結果が表示されるまでの時間を測定する。

エ　利用者のデータベースに対するアクセス状況を確認するために，アクセス記録を出力し内容を調査する。

〔 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。ただし，問題冊子を切り離して利用することはできません。
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。