SC

平成23年度　春期　　特別試験

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. この注意事項は，問題冊子の**裏表紙**に続きます。必ず読んでください。
4. **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。**
5. 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

6. 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**のとおりマークされていない場合は，読み取れず，採点されないことがありますので，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。

(2) 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。

(3) **受験番号欄**に，**受験番号**を記入及びマークしてください。正しくマークされていない場合は，採点されません。

(4) **生年月日欄**に，受験票に印字されているとおりの**生年月日**を記入及びマークしてください。正しく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。

(5) 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。

〔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1　AESの暗号化方式を説明したものはどれか。

ア　鍵長によって，段数が決まる。

イ　段数は，6回以内の範囲で選択できる。

ウ　データの暗号化，復号，暗号化の順に3回繰り返す。

エ　同一の公開鍵を用いて暗号化を3回繰り返す。

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　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

イ　チャレンジレスポンスによる利用者認証

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　PC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4　暗号アルゴリズムの危殆化を説明したものはどれか。

ア　外国の輸出規制によって十分な強度をもつ暗号アルゴリズムを実装した製品が利用できなくなること

イ　鍵の不適切な管理によって，鍵が漏えいする危険性が増すこと

ウ　計算能力の向上などによって，鍵の推定が可能となり，暗号の安全性が低下すること

エ　最高性能のコンピュータを用い，膨大な時間やコストを掛けて暗号強度をより確実なものとすること

問5　SMTP-AUTH における認証の動作を説明したものはどれか。

ア　SMTP サーバに電子メールを送信する前に，電子メールを受信し，その際にパスワード認証が行われたクライアントの IP アドレスに対して，一定時間だけ電子メールの送信を許可する。

イ　クライアントが SMTP サーバにアクセスしたときに利用者認証を行い，許可された利用者だけから電子メールを受け付ける。

ウ　サーバは認証局のディジタル証明書をもち，クライアントから送信された認証局の署名付きクライアント証明書の妥当性を確認する。

エ　利用者が電子メールを受信する際の認証情報を秘匿できるように，パスワードからハッシュ値を計算して，その値で利用者認証を行う。

問6　X.509 における CRL（Certificate Revocation List）の運用を説明したものはどれか。

ア　PKI の利用者は，認証局の公開鍵が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，X.509 によって 1 年に 1 回の CRL 発行が義務付けられている。

ウ　認証局は，ディジタル証明書を有効期限内に CRL に登録することがある。

エ　認証局は，発行したすべてのディジタル証明書の有効期限を CRL に登録する。

問7　認証局が送信者に発行したディジタル証明書を使用して送信者又は受信者が行えることはどれか。

ア　受信した暗号文を復号して，盗聴を検知する。

イ　受信した暗号文を復号して，メッセージが改ざんされていないことと送信者が商取引相手として信頼できることを確認する。

ウ　受信したメッセージのディジタル署名を検証して，メッセージが改ざんされていないこととメッセージの送信者に偽りのないことを確認する。

エ　メッセージにディジタル署名を添付して，盗聴を防止する。

問8　サーバへのログイン時に用いるパスワードを不正に取得しようとする攻撃とその対策の組合せのうち，適切なものはどれか。

	辞書攻撃	スニッフィング	ブルートフォース攻撃
ア	パスワードを平文で送信しない。	ログインの試行回数に制限を設ける。	ランダムな値でパスワードを設定する。
イ	ランダムな値でパスワードを設定する。	パスワードを平文で送信しない。	ログインの試行回数に制限を設ける。
ウ	ランダムな値でパスワードを設定する。	ログインの試行回数に制限を設ける。	パスワードを平文で送信しない。
エ	ログインの試行回数に制限を設ける。	ランダムな値でパスワードを設定する。	パスワードを平文で送信しない。

問9　ウイルスの検出手法であるビヘイビア法を説明したものはどれか。

ア　あらかじめ特徴的なコードをパターンとして登録したウイルス定義ファイルを用いてウイルス検査対象と比較し，同じパターンがあれば感染を検出する。

イ　ウイルスに感染していないことを保証する情報をあらかじめ検査対象に付加しておき，検査時に不整合があれば感染を検出する。

ウ　ウイルスの感染が疑わしい検査対象を，安全な場所に保管する原本と比較し，異なっていれば感染を検出する。

エ　ウイルスの感染や発病によって生じるデータ書込み動作の異常や通信量の異常増加などの変化を監視して，感染を検出する。

問10 ウイルスの調査手法に関する記述のうち，適切なものはどれか。

ア　逆アセンブルは，バイナリコードの新種ウイルスの動作を解明するのに有効な手法である。

イ　パターンマッチングでウイルスを検知する方式は，暗号化された文書中のマクロウイルスの動作を解明するのに有効な手法である。

ウ　ファイルのハッシュ値を基にウイルスを検知する方式は，ウイルスのハッシュ値からどのウイルスの亜種かを特定するのに確実な手法である。

エ　不正な動作からウイルスを検知する方式は，ウイルス名を特定するのに確実な手法である。

問11 通信の暗号化に関する記述のうち，適切なものはどれか。

ア　IPsec のトランスポートモードでは，ゲートウェイ間の通信経路上だけではなく，送信ホストと受信ホストとの間の全経路上でメッセージが暗号化される。

イ　LDAP クライアントが LDAP サーバに接続するとき，その通信内容は暗号化することができない。

ウ　S/MIME で暗号化した電子メールは，受信側のメールサーバ内に格納されている間は，メール管理者が平文として見ることができる。

エ　SSL を使用すると，暗号化された HTML 文書はブラウザでキャッシュの有無が設定できず，ディスク内に必ず保存される。

問12　自社の中継用メールサーバのログのうち，外部ネットワークからの第三者中継と判断できるものはどれか。ここで，AAA.168.1.5 と AAA.168.1.10 は自社のグローバル IP アドレスとし，BBB.45.67.89 と BBB.45.67.90 は社外のグローバル IP アドレスとする。a.b.c は自社のドメイン名とし，a.b.d と a.b.e は他社のドメイン名とする。また，IP アドレスとドメイン名は詐称されていないものとする。

	接続元 IP アドレス	送信者のドメイン名	受信者のドメイン名
ア	AAA.168.1.5	a.b.c	a.b.d
イ	AAA.168.1.10	a.b.c	a.b.c
ウ	BBB.45.67.89	a.b.d	a.b.e
エ	BBB.45.67.90	a.b.d	a.b.c

問13　経済産業省“ソフトウェア管理ガイドライン”に定められた，ソフトウェアを使用する法人，団体などが実施すべき基本的事項の記述のうち，適切なものはどれか。

ア　ウイルスからソフトウェアを保護するため，関係法令や使用許諾契約などについて利用者の教育啓発を行う。

イ　セキュリティ対策に責任を負うセキュリティ管理責任者を任命し，適切な管理体制を整備する。

ウ　ソフトウェアの違法複製などの有無を確認するため，すべてのソフトウェアを対象として，その使用状況についての監査を実施する。

エ　ソフトウェアの脆弱(ぜいじゃく)性を突いた不正アクセスから保護するため，ソフトウェアの使用手順や管理方法などを定めたソフトウェア管理規則を制定する。

問14　共通フレーム2007に従いシステム開発の要件定義の段階で実施することとして，適切なものはどれか。

ア　システムに必要なセキュリティ機能及びその機能が対策として達成すべき内容を決定する。

イ　システムに必要なセキュリティ機能に関連するチェックリストを用いてソースコードをレビューする。

ウ　組織に必要なセキュリティ機能を含むシステム化計画を立案する。

エ　第三者によるシステムのセキュリティ監査を脆弱性評価ツールを用いて定期的に実施する。

問15　ICカードの耐タンパ性を高める対策はどれか。

ア　IC カードと IC カードリーダとが非接触の状態で利用者を認証して，利用者の利便性を高めるようにする。

イ　故障に備えてあらかじめ作成した予備のICカードを保管し，故障時に直ちに予備カードに交換して利用者がICカードを使い続けられるようにする。

ウ　信号の読出し用プローブの取付けを検出するとICチップ内の保存情報を消去する回路を設けて，ICチップ内の情報を容易に解析できないようにする。

エ　退職者のICカードは業務システム側で利用を停止して，ほかの利用者が使用できないようにする。

問16 ルータで接続された二つのセグメント間でのコリジョンの伝搬とブロードキャストフレームの中継について，適切な組合せはどれか。

	コリジョンの伝搬	ブロードキャストフレームの中継
ア	伝搬する	中継する
イ	伝搬する	中継しない
ウ	伝搬しない	中継する
エ	伝搬しない	中継しない

問17 ある企業の本店で内線通話を調査したところ，通話数が 1 時間当たり 120 回，平均通話時間が 90 秒であった。本店内線の呼量は何アーランか。

ア 0.03　　イ 3　　ウ 180　　エ 10,800

問18 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19 TCP のフロー制御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　ウィンドウ制御はビット単位で行う。

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20 通信プロトコルで使用するデータ形式を記述するための記法であって，SNMP のパケットの符号化に利用されているものはどれか。

ア　ASN.1　　イ　JSON　　ウ　SGML　　エ　SOAP

問21 次の SQL 文を A 表の所有者が発行した場合を説明したものはどれか。

```
GRANT ALL PRIVILEGES ON A TO B WITH GRANT OPTION
```

ア　A 表に関する，SELECT 権限，UPDATE 権限，INSERT 権限，DELETE 権限などのすべての権限，及びそれらの付与権限を利用者 B に対して付与する。

イ　A 表に関する，SELECT 権限，UPDATE 権限，INSERT 権限，DELETE 権限などのすべての権限を利用者 B に対して付与するが，それらの権限の付与権限は付与しない。

ウ　A 表に関する，SELECT 権限，UPDATE 権限，INSERT 権限，DELETE 権限は与えないが，それらのすべての権限の付与権限だけを利用者 B に対して付与する。

エ　A 表に関する，SELECT 権限，及び SELECT 権限の付与権限を利用者 B に対して付与し，UPDATE 権限，INSERT 権限，DELETE 権限，及びそれらの付与権限は付与しない。

問22　操作に不慣れな人も利用するシステムでは，間違ったデータが入力されることが想定される。誤入力が発生しても，プログラムやシステムを異常終了させずに，エラーメッセージを表示して次の操作を促すような設計を何というか。

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ス

問23　共通フレーム2007で取り決められているものはどれか。

ア　作成する文書の種類及び書式
イ　信頼性，保守性などのソフトウェアの品質尺度
ウ　適用すべき開発モデル，技法及びツール
エ　プロセスごとの作業の主体者（役割）と責任の所在

問24 (1)～(4)はある障害の発生から本格的な対応までの一連の活動である。(1)～(4)の各活動とそれに対応するITILの管理プロセスの組合せのうち，適切なものはどれか。

(1) 利用者からサービスデスクに“特定の入力操作が拒否される”という連絡があったので，別の入力操作による回避方法を利用者に伝えた。

(2) 原因を開発チームで追究した結果，アプリケーションプログラムに不具合があることが分かった。

(3) 障害の原因となったアプリケーションプログラムの不具合を改修する必要があるのかどうか，改修した場合に不具合箇所以外に影響が出る心配はないかどうかについて，関係者を集めて確認し，改修することを決定した。

(4) 改修したアプリケーションプログラムの稼働環境への適用については，利用者への周知，適用手順及び失敗時の切戻し手順の確認など，十分に事前準備を行った。

	(1)	(2)	(3)	(4)
ア	インシデント管理	問題管理	変更管理	リリース管理及び展開管理
イ	インシデント管理	問題管理	リリース管理及び展開管理	変更管理
ウ	問題管理	インシデント管理	変更管理	リリース管理及び展開管理
エ	問題管理	インシデント管理	リリース管理及び展開管理	変更管理

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 〕

7. **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。
8. 問題冊子の余白などは，適宜利用して構いません。
9. 試験時間中，机上に置けるもの及び使用できるものは，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，ティッシュ
   これら以外は机上に置けません。使用もできません。
10. 試験終了後，この問題冊子は持ち帰ることができます。
11. 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。
12. 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。
13. 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。

お知らせ

1. システムの構築や試験会場の確保などの諸準備が整えば，平成 23 年 11 月から IT パスポート試験において CBT※方式による試験を実施する予定です。
2. CBT 方式による試験の実施に伴い，現行の筆記による試験は，廃止する予定です。
3. 詳細が決定しましたら，ホームページなどでお知らせします。

※CBT（Computer Based Testing）：コンピュータを使用して実施する試験。