SC

平成21年度　春期
情報セキュリティスペシャリスト
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) B 又は HB の黒鉛筆又はシャープペンシルを使用してください。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) 答案用紙は光学式読取り装置で処理しますので，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。
   (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，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。
   (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〕　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1　DNSキャッシュポイズニングに分類される攻撃内容はどれか。

ア　DNSサーバのソフトウェアのバージョン情報を入手して，DNSサーバのセキュリティホールを特定する。

イ　PCが参照するDNSサーバに誤ったドメイン管理情報を注入して，偽装されたWebサーバにPCの利用者を誘導する。

ウ　攻撃対象のサービスを妨害するために，攻撃者がDNSサーバを踏み台に利用して再帰的な問合せを大量に行う。

エ　内部情報を入手するために，DNSサーバが保存するゾーン情報をまとめて転送させる。

問2　SSLを使用して通信を暗号化する場合，SSL-VPN装置に必要な条件はどれか。

ア　SSL-VPN装置は，1台1台を識別できるようにディジタル証明書を組み込む必要がある。

イ　SSL-VPN装置は，装置メーカが用意した機種固有のディジタル証明書を組み込む必要がある。

ウ　SSL-VPN装置は，装置メーカから提供される認証局を利用する必要がある。

エ　同一ドメイン内で複数拠点にSSL-VPN装置を設置する場合は，同一のディジタル証明書を利用する必要がある。

問3　シングルサインオンの説明のうち，適切なものはどれか。

ア　クッキーを使ったシングルサインオンの場合，サーバごとの認証情報を含んだクッキーをクライアントで生成し，各サーバ上で保存，管理する。

イ　クッキーを使ったシングルサインオンの場合，認証対象の各サーバを異なるインターネットドメインに配置する必要がある。

ウ　リバースプロキシを使ったシングルサインオンの場合，認証対象の各 Web サーバをそれぞれ異なるインターネットドメインにする必要がある。

エ　リバースプロキシを使ったシングルサインオンの場合，利用者認証においてパスワードの代わりにディジタル証明書を用いることができる。

問4　スパムメールの対策として，あて先ポート番号 25 番のメールに対し 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受信メールのうち，スパムメールのシグネチャに該当するメールを遮断する。

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に直接送信されたメールを遮断する。

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メールを遮断する。

エ　メール不正中継の脆弱性をもつメールサーバからの受信メールを遮断する。

問5　ディジタル署名を利用する目的はどれか。

ア　受信者が署名鍵を使って暗号文を元の平文に戻すことができるようにする。

イ　送信者が固定文字列を付加した平文を署名鍵を使って暗号化し，受信者がメッセージの改ざん部位を特定できるようにする。

ウ　送信者が署名鍵を使って署名を作成し，それを平文に付加することによって，受信者が送信者を確認できるようにする。

エ　送信者が署名鍵を使って平文を暗号化し，平文の内容を関係者以外に分からないようにする。

問6　SHA-1 を説明したものはどれか。

ア　160 ビットの出力データを生成し，改ざんの検出に利用するアルゴリズム

イ　IPsec で使用される暗号化アルゴリズム

ウ　公開鍵暗号方式において暗号化鍵を生成するアルゴリズム

エ　データの暗号化が正常に完了したことの確認に利用するアルゴリズム

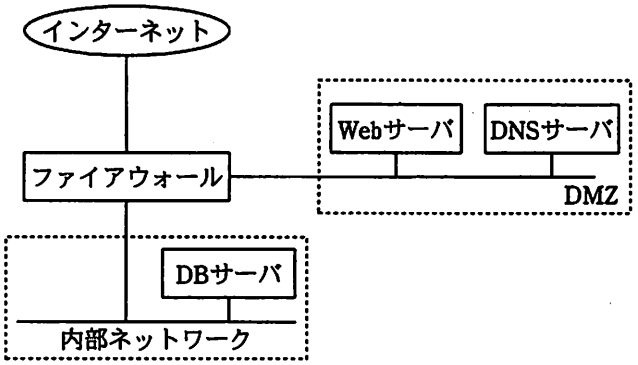
問7　リスク対策をリスクコントロールとリスクファイナンスに分けた場合，リスクファイナンスに該当するものはどれか。

ア　システムが被害を受けた場合を想定して保険をかけた。
イ　システム被害につながるリスクの発生を抑える対策に資金を投入した。
ウ　システムを復旧するのに掛かった費用を金融機関から借り入れた。
エ　リスクが顕在化した場合のシステム被害を小さくする対策に資金を投入した。

問8　情報システムのリスク分析に関する記述のうち，適切なものはどれか。

ア　リスクには，投機的リスクと純粋リスクとがある。情報セキュリティのためのリスク分析で対象とするのは，投機的リスクである。
イ　リスクの予想損失額は，損害予防のために投入されるコスト，復旧に要するコスト，及びほかの手段で業務を継続するための代替コストの合計で表される。
ウ　リスク分析では，現実に発生すれば損失をもたらすリスクが，情報システムのどこに，どのように潜在しているかを識別し，その影響の大きさを測定する。
エ　リスクを金額で測定するリスク評価額は，損害が現実のものになった場合の 1 回当たりの平均予想損失額で表される。

問9　DMZ 上の公開 Web サーバで入力データを受け付け，内部ネットワークの DB サーバにそのデータを蓄積するシステムがある。DB サーバへの不正侵入対策の一つとして，ファイアウォールの最も有効な設定はどれか。



ア　DB サーバの受信ポートを固定にし，Web サーバから DB サーバの受信ポートへ発信された通信だけをファイアウォールで通す。

イ　DMZ から DB サーバあての通信だけをファイアウォールで通す。

ウ　Web サーバの発信ポートは任意のポート番号を使用し，ファイアウォールでは，いったん終了した通信と同じ発信ポートを使った通信を拒否する。

エ　Web サーバの発信ポートを固定し，その発信ポートの通信だけをファイアウォールで通す。

問10　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，発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11　メールサーバ（SMTP サーバ）の不正利用を防止するために行う設定はどれか。

ア　ゾーン転送のアクセス元を制御する。

イ　第三者中継を禁止する。

ウ　ディレクトリに存在するファイル名の表示を禁止する。

エ　特定のディレクトリ以外での CGI プログラムの実行を禁止する。

問12　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か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 などに不正に組み込んだものを隠ぺいする機能をまとめたツール

問13　TCP/IP のネットワークにおける ICMP の説明として，適切なものはどれか。

ア　MAC アドレスだけが分かっているときに IP アドレスの解決を可能にする。
イ　グローバル IP アドレスとプライベート IP アドレスを相互に変換する。
ウ　送信元ホストへ，IP パケットの送信エラー報告などの制御メッセージを通知する。
エ　ネットワーク内の IP アドレスを一元管理し，クライアントに動的に割り当てる。

問14　TCP/IP のネットワークにおいて，TCP のコネクションを識別するために必要なものの組合せはどれか。

ア　あて先 IP アドレス，あて先 TCP ポート番号
イ　あて先 IP アドレス，あて先 TCP ポート番号，送信元 IP アドレス，送信元 TCP ポート番号
ウ　あて先 IP アドレス，送信元 IP アドレス
エ　あて先 MAC アドレス，あて先 IP アドレス，あて先 TCP ポート番号，送信元 MAC アドレス，送信元 IP アドレス，送信元 TCP ポート番号

問15　TCP ヘッダ中のウィンドウサイズの説明として，適切なものはどれか。

ア　受信エラー時の再送に備えて送信側が保持しているデータのサイズを受信側に知らせるために使用される。
イ　受信側からの確認応答を待たずに，データを続けて送信できるかどうかの判断に使用される。
ウ　送信側と受信側の最適なバッファサイズを接続開始時のハンドシェイクで決定するために使用される。
エ　複数セグメントから成るデータの送信時，後続するセグメント数を受信側に知らせるために使用される。

問16　RDBMS の表へのアクセスにおいて，特定の利用者だけにアクセス権を与える方法として，適切なものはどれか。

ア　CONNECT 文で接続を許可する。
イ　CREATE ASSERTION 文で表明して制限する。
ウ　CREATE TABLE 文の参照制約で制限する。
エ　GRANT 文で利用を許可する。

問17　DBMS の排他制御機能に関する記述のうち，適切なものはどれか。

ア　排他制御機能によって，同時実行処理でのデータの整合性を保つことができる。
イ　排他制御機能の使用によって，デッドロックを防止できる。
ウ　排他制御は DBMS が自動的に行い，アプリケーションプログラムからロック，アンロックの指示はできない。
エ　バッチによる更新処理では排他制御を行う必要はない。

問18　システム開発で行われる各テストについて，そのテスト要求事項が定義されるアクティビティと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19　ハードウェアの保守点検及び修理作業を実施するときに，運用管理者が実施すべき，事前又は事後の確認に関する説明のうち，適切なものはどれか。

ア　システムが自動的に回復処置を行った障害については，障害前後のエラーログが残っているので，障害原因や対応処置の報告ではなく，ログの分析結果を確認する。

イ　定期保守時の点検項目は事前に分かっているので，事前と事後の確認は省略できるが，作業の開始と終了については，保守作業者に確認する。

ウ　予防保守を遠隔保守方式で行う場合，遠隔地のシステムへの影響は出ないので，作業内容などの事前確認は行わず，事後に作業実施結果を確認する。

エ　臨時保守の場合，事前に保守作業者が障害の発生状況を確認したことを確認し，事後に障害原因や作業実施結果を確認する。

問20　ソフトウェア開発のプロセスモデルのうち，開発サイクルを繰り返すことによって，システムの完成度を高めていくプロセスモデルはどれか。

ア　RAD モデル　　イ　ウォータフォールモデル

ウ　スパイラルモデル　　エ　プロトタイピングモデル

問21　ソフトウェアを保守するときなどに利用される技術であるリバースエンジニアリングの説明はどれか。

ア　ソースプログラムを解析してプログラム仕様書を作る。

イ　ソースプログラムを探索して修正箇所や影響度を調べる。

ウ　ソースプログラムを見直して構造化プログラムに変換する。

エ　ソースプログラムを分かりやすい表現に書き換える。

問22　ITILにおけるインシデント管理プロセスの役割として，適切なものはどれか。

ア　新しいサービスの要求を利用者から受け付け，企画立案すること
イ　一時的回避策で対処した問題を分析し，恒久対策を検討すること
ウ　潜在的な問題を事前に発見し，変更要求としてとりまとめること
エ　低下したサービスレベルを回復させ，影響を最小限に抑えること

問23　データベースサーバのハードディスクに障害が発生した場合でもサービスを続行できるようにするための方策として，最も適切なものはどれか。

ア　共通データベースの格納場所を複数のハードディスクに分散させる。
イ　サーバのディスクを二重化し，通常稼働時は同時に二つのディスクに書き込む。
ウ　サーバの予備機を設置し，OSとアプリケーションソフトを本番機と同じ構成にして待機させておく。
エ　別のディスクにデータベースを毎週末にコピーする。

問24　アクセス権限を管理しているシステムの利用者IDリストから，退職による権限喪失者が削除されていることを検証する手続として，最も適切なものはどれか。

ア　アクセス権限削除申請書の全件について，利用者IDリストから削除されていることを確認する。
イ　最新の利用者IDリストの全件について，対応するアクセス権限削除申請書が存在しないことを確認する。
ウ　人事発令簿の退職者の全件について，利用者IDリストから削除されていることを確認する。
エ　利用者IDリストの更新履歴の全件について，対応するアクセス権限削除申請書の存在を確認する。

問25　外部保管のために専門業者にバックアップ媒体を引き渡す際の安全性について，セキュリティ監査を実施した。指摘事項となる状況はどれか。

ア　委託元責任者が，一定期間ごとに，専門業者における媒体保管状況を確認している。

イ　委託元責任者が，専門業者との間で，機密保持条項を盛り込んだ業務委託契約を結んだ上で引き渡している。

ウ　委託元担当者が，専用の記録簿に，引渡しの都度，日付と内容を記入し，専門業者から受領印をもらっている。

エ　委託元担当者が，バックアップ媒体を段ボール箱に入れ，専門業者に引き渡している。

〔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，黒鉛筆又はシャープペンシル，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。