SC

平成22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. 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，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，読み取れないことがあります。
   (2) B 又は HB の黒鉛筆を使用してください。シャープペンシルを使用しても構いませんが，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。
   (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　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 サーバを異なるインターネットドメインに配置する必要がある。

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2　作成者によってディジタル署名された電子文書に，タイムスタンプ機関がタイムスタンプを付与した。この電子文書を公開する場合のタイムスタンプの効果のうち，適切なものはどれか。

ア　タイムスタンプを付与した時刻以降に，作成者が，電子文書の内容をほかの電子文書へコピーして流用することを防止する。

イ　タイムスタンプを付与した時刻以降に，第三者が，電子文書の内容をほかの電子文書へコピーして流用することを防止する。

ウ　電子文書が，タイムスタンプの時刻以前に存在したことを示し，作成者が，電子文書の作成を否認することを防止する。

エ　電子文書が，タイムスタンプの時刻以前に存在したことを示し，第三者が，電子文書を改ざんすることを防止する。

問3　FIPS 140-2 を説明したものはどれか。

ア　暗号モジュールのセキュリティ要求事項
イ　情報セキュリティマネジメントシステムに関する認証基準
ウ　ディジタル証明書や証明書失効リストの標準仕様
エ　無線 LAN セキュリティ技術

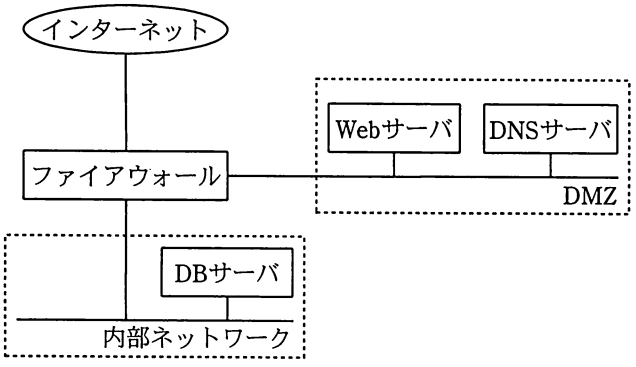
問4　米国 NIST が制定した AES における鍵長の条件はどれか。

ア　128 ビット，192 ビット，256 ビットから選択する。
イ　256 ビット未満で任意に指定する。
ウ　暗号化処理単位のブロック長より 32 ビット長くする。
エ　暗号化処理単位のブロック長より 32 ビット短くする。

問5　JIS Q 27001:2006 における情報システムのリスクとその評価に関する記述のうち，適切なものはどれか。

ア　脅威とは，脆弱(ぜい)性が顕在化する確率のことであり，情報システムに組み込まれた技術的管理策によって決まる。
イ　脆弱性とは，情報システムに対して悪い影響を与える要因のことであり，自然災害，システム障害，人為的過失及び不正行為に大別される。
ウ　リスクの特定では，脅威が情報資産の脆弱性に付け込み，情報資産に与える影響を特定する。
エ　リスク評価では，リスク回避とリスク低減の二つに評価を分類し，リスクの大きさを判断して対策を決める。

問6　DMZ 上に公開している 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。インターネットから DMZ を経由してなされる DB サーバへの不正侵入対策の一つとして，DMZ と内部ネットワークとの間にファイアウォールを設置するとき，最も有効な設定はどれか。



ア　DB サーバの受信ポート番号を固定し，Web サーバから DB サーバの受信ポート番号への通信だけをファイアウォールで通す。

イ　DMZ から DB サーバへ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番号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番号を使った通信を拒否する。

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

問7　ファイアウォールにおいて，自ネットワークのホストへの侵入を防止する対策のうち，IP スプーフィング（spoofing）攻撃に有効なものはどれか。

ア　外部から入る TCP コネクション確立要求パケットのうち，外部へのインターネットサービスの提供に必要なもの以外を阻止する。

イ　外部から入る UDP パケットのうち，外部へのインターネットサービスの提供や利用したいインターネットサービスに必要なもの以外を阻止する。

ウ　外部から入るパケットのあて先 IP アドレスが，インターネットとの直接の通信をすべきでない自ネットワークのホストのものであれば，そのパケットを阻止する。

エ　外部から入るパケットの送信元 IP アドレスが自ネットワークのものであれば，そのパケットを阻止する。

問8　SQL インジェクション攻撃を防ぐ方法はどれか。

ア　入力から，上位ディレクトリを指定する文字列（../）を取り除く。

イ　入力中の文字がデータベースへの問合せや操作において特別な意味をもつ文字として解釈されないようにする。

ウ　入力に HTML タグが含まれていたら，解釈，実行できないほかの文字列に置き換える。

エ　入力の全体の長さが制限を超えていたときは受け付けない。

問9　通信を要求した PC に対し，ARP の仕組みを利用して実現できる通信の可否の判定方法のうち，最も適切なものはどれか。

ア　PC にインストールされているソフトウェアを確認し，登録されているソフトウェアだけがインストールされている場合に通信を許可する。

イ　PC の MAC アドレスを確認し，事前に登録されている MAC アドレスをもつ場合だけ通信を許可する。

ウ　PC の OS のパッチ適用状況を確認し，最新のパッチが適用されている場合だけ通信を許可する。

エ　PC のマルウェア対策ソフトの定義ファイルを確認し，最新になっている場合だけ通信を許可する。

問10　暗号方式に関する記述のうち，適切なものはどれか。

ア　AES は公開鍵暗号方式，RSA は共通鍵暗号方式の一種である。

イ　共通鍵暗号方式では，暗号化及び復号に使用する鍵が同一である。

ウ　公開鍵暗号方式を通信内容の秘匿に使用する場合は，暗号化鍵を秘密にして，復号鍵を公開する。

エ　ディジタル署名に公開鍵暗号方式が使用されることはなく，共通鍵暗号方式が使用される。

問11 社内とインターネットの接続点にパケットフィルタリング型ファイアウォールを設置したネットワーク構成において，社内の PC からインターネット上の SMTP サーバに電子メールを送信するとき，ファイアウォールで通過許可とする TCP パケットのポート番号の組合せはどれか。

		送信元	あて先	送信元 ポート番号	あて先 ポート番号
ア	発信	PC	SMTP サーバ	25	1024 以上
	応答	SMTP サーバ	PC	1024 以上	25
イ	発信	PC	SMTP サーバ	1024 以上	25
	応答	SMTP サーバ	PC	25	1024 以上
ウ	発信	SMTP サーバ	PC	110	1024 以上
	応答	PC	SMTP サーバ	1024 以上	110
エ	発信	SMTP サーバ	PC	1024 以上	110
	応答	PC	SMTP サーバ	110	1024 以上

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情報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 付加されたディジタル署名を受信側が検証する。

問13　ISP 管理下の動的 IP アドレスを割り当てられた PC からのスパムメール送信を防止する対策 OP25B はどれか。

ア　管理下の動的 IP アドレスから，管理外のグローバル IP アドレスへの POP 通信を拒否する。

イ　管理下の動的 IP アドレスから，管理外のグローバル IP アドレスへの SMTP 通信を拒否する。

ウ　メールサーバで，受信メールのあて先電子メールアドレスが管理外のドメインを指す場合，電子メールの受信を拒否する。

エ　メールサーバで，スパムメール受信時に送信元の電子メールアドレスをブラックリストに登録しておき，スパムメール送信元からの電子メールの受信を拒否する。

問14　無線 LAN における通信の暗号化の仕組みに関する記述のうち，適切なものはどれか。

ア　EAP は，クライアント PC とアクセスポイントとの間で，あらかじめ登録した共通鍵による暗号化通信を実現する。

イ　ESS-ID は，クライアント PC ごとの秘密鍵を定めたものであり，公開鍵暗号方式による暗号化通信を実現する。

ウ　WEP では，クライアント PC とアクセスポイントとの間で公開鍵暗号方式による暗号化通信を実現できる。

エ　WPA2 では，IEEE 802.1X の規格に沿って機器認証を行い，動的に更新される暗号化鍵を用いて暗号化通信を実現できる。

問15 SSLの利用に関する記述のうち，適切なものはどれか。

ア　SSL で使用する個人認証用のディジタル証明書は，IC カードなどに格納できるので，格納場所を特定の PC に限定する必要はない。

イ　SSL は Web サーバを経由した特定の利用者間の通信のために開発されたプロトコルであり，Web サーバ提供者への事前の利用者登録が不可欠である。

ウ　SSL を利用する Web サーバのディジタル証明書には IP アドレスの組込みが必須なので，Web サーバの IP アドレスを変更する場合は，ディジタル証明書を再度取得する必要がある。

エ　日本国内では，SSL で使用する共通鍵の長さは，128 ビット未満に制限されている。

問16 WAF（Web Application Firewall）のブラックリスト又はホワイトリストの説明のうち，適切なものはどれか。

ア　ブラックリストは，脆弱(ぜい)性のあるサイトの IP アドレスを登録したものであり，該当する通信を遮断する。

イ　ブラックリストは，問題のある通信データパターンを定義したものであり，該当する通信を遮断するか又は無害化する。

ウ　ホワイトリストは，脆弱性のないサイトの FQDN を登録したものであり，該当する通信を遮断する。

エ　ホワイトリストは，問題のある送信データをどのように無害化するかを定義したものであり，該当するデータを無害化する。

問17 1台のサーバと複数台のクライアントが，100Mビット／秒のLANで接続されている。業務のピーク時には，クライアント1台につき1分当たり600kバイトのデータをサーバからダウンロードする。このとき，同時使用してもピーク時に業務を滞りなく遂行できるクライアント数は何台までか。ここで，LANの伝送効率は50%，サーバ及びクライアント内の処理時間は無視できるものとし，1Mビット／秒＝10^6ビット／秒，1kバイト＝1,000バイトとする。

ア 10　　イ 625　　ウ 1,250　　エ 5,000

問18 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 トークンアクセス方式では，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19 DNSSECの説明として，適切なものはどれか。

ア DNSサーバへのDoS攻撃を防止できる。

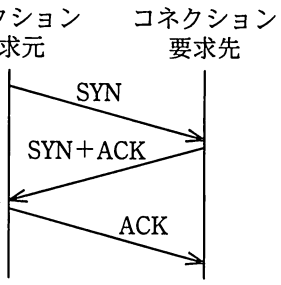
イ IPsecによる暗号化通信が前提となっている。

ウ 代表的なDNSサーバの実装であるBINDの代替として使用する。

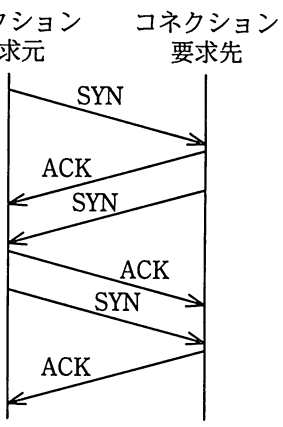
エ ディジタル署名によってDNS応答の正当性を確認できる。

問20 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。

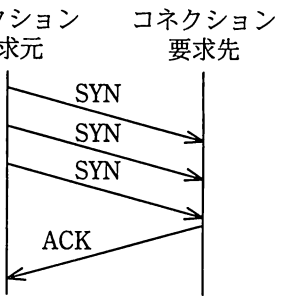
ア



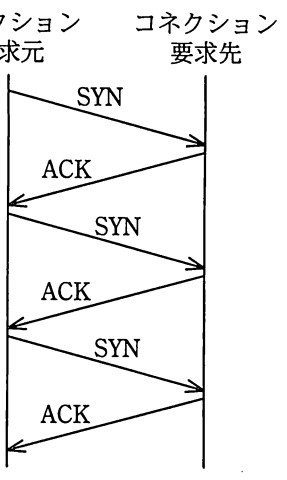
イ



ウ



エ



問21 和両立である表 R (ID, NAME), S (NO, NAMAE) がある。差集合 R−S を求める SELECT 文とするために, a に入れるべき適切な字句はどれか。ここで, 下線部は主キーを表す。また, NAME と NAMAE は NULL 不可とする。

```
SELECT * FROM R WHERE [ a ]
   (SELECT * FROM S WHERE S.NO = R.ID AND S.NAMAE = R.NAME)
```

ア EXISTS　　イ NOT EXISTS　　ウ NOT IN　　エ R.ID NOT IN

問22 ソフトウェアの保守作業の効率向上施策として，最も適切なものはどれか。

ア　エンドユーザによる動作確認テスト
イ　コーディング規約に準拠したプログラムの作成
ウ　最適化コンパイルによる性能改善
エ　発生したバグの要因分類による傾向分析

問23 SOA（Service Oriented Architecture）でサービスを設計する際の注意点のうち，適切なものはどれか。

ア　可用性を高めるために，ステートフルなインタフェースとする。
イ　業務からの独立性を確保するために，サービスの命名は役割を表すものとする。
ウ　業務の変化に対応しやすくするために，サービス間の関係は疎結合にする。
エ　セキュリティを高めるために，一度開発したサービスは再利用しない方がよい。

問24 レプリケーションが有効な対策となるものはどれか。

ア　悪意によるデータの改ざんを防ぐ。
イ　コンピュータウイルスによるデータの破壊を防ぐ。
ウ　災害発生時にシステムが長時間停止するのを防ぐ。
エ　操作ミスによるデータの削除を防ぐ。

問25　請負契約でシステム開発を委託している案件について，委託元のシステム監査人の指摘事項に該当するものはどれか。

ア　委託した開発案件の品質を委託元の管理者が定期的にモニタリングしている。

イ　委託元の管理者が委託先の開発担当者を指揮命令している。

ウ　契約書に機密保持のための必要事項が盛り込まれている。

エ　特定の委託先との契約が長期化しているので，その妥当性を確認している。

〔 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，B 又は HB の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。

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。