SC

令和４年度　秋期
情報処理安全確保支援士試験
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，読み取れないことがあります。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注意してください。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) 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〕　秋期の情報処理安全確保支援士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　送信者から受信者にメッセージ認証符号（MAC：Message Authentication Code）を付与したメッセージを送り，さらに受信者が第三者に転送した。そのときのMACに関する記述のうち，適切なものはどれか。ここで，共通鍵は送信者と受信者だけが知っており，送信者と受信者のそれぞれの公開鍵は３人とも知っているとする。

ア　MACは，送信者がメッセージと共通鍵を用いて生成する。MACを用いると，受信者がメッセージの完全性を確認できる。

イ　MACは，送信者がメッセージと共通鍵を用いて生成する。MACを用いると，第三者が送信者の真正性を確認できる。

ウ　MACは，送信者がメッセージと受信者の公開鍵を用いて生成する。MACを用いると，第三者がメッセージの完全性を確認できる。

エ　MACは，送信者がメッセージと送信者の公開鍵を用いて生成する。MACを用いると，受信者が送信者の真正性を確認できる。

問２　PKI（公開鍵基盤）を構成するRA（Registration Authority）の役割はどれか。

ア　デジタル証明書にデジタル署名を付与する。

イ　デジタル証明書に紐(ひも)づけられた属性証明書を発行する。

ウ　デジタル証明書の失効リストを管理し，デジタル証明書の有効性を確認する。

エ　本人確認を行い，デジタル証明書の発行申請の承認又は却下を行う。

問３　標準化団体OASISが，Webサイトなどを運営するオンラインビジネスパートナー間で認証，属性及び認可の情報を安全に交換するために策定したものはどれか。

ア　SAML　　イ　SOAP　　ウ　XKMS　　エ　XML Signature

問４　DoS 攻撃の一つである Smurf 攻撃はどれか。

ア　TCP 接続要求である SYN パケットを攻撃対象に大量に送り付ける。

イ　偽装した ICMP の要求パケットを送って，大量の応答パケットが攻撃対象に送られるようにする。

ウ　サイズが大きい UDP パケットを攻撃対象に大量に送り付ける。

エ　サイズが大きい電子メールや大量の電子メールを攻撃対象に送り付ける。

問５　送信元 IP アドレスが A，送信元ポート番号が 80/tcp，宛先 IP アドレスが未使用の IP アドレス空間内の IP アドレスである SYN/ACK パケットを大量に観測した場合，推定できる攻撃はどれか。

ア　IP アドレス A を攻撃先とするサービス妨害攻撃

イ　IP アドレス A を攻撃先とするパスワードリスト攻撃

ウ　IP アドレス A を攻撃元とするサービス妨害攻撃

エ　IP アドレス A を攻撃元とするパスワードリスト攻撃

問6　パスワードスプレー攻撃に該当するものはどれか。

ア　攻撃対象とする利用者 ID を一つ定め，辞書及び人名リストに掲載されている単語及び人名並びにそれらの組合せを順にパスワードとして入力して，ログインを試行する。

イ　攻撃対象とする利用者 ID を一つ定め，パスワードを総当たりして，ログインを試行する。

ウ　攻撃の時刻と攻撃元 IP アドレスとを変え，かつ，アカウントロックを回避しながらよく用いられるパスワードを複数の利用者 ID に同時に試し，ログインを試行する。

エ　不正に取得したある他のサイトの利用者 ID とパスワードとの組みの一覧表を用いて，ログインを試行する。

問7　シングルサインオン（SSO）に関する記述のうち，適切なものはどれか。

ア　SAML 方式では，インターネット上の複数の Web サイトにおける SSO を，IdP（Identity Provider）で自動生成された URL 形式の 1 人一つの利用者 ID で実現する。

イ　エージェント方式では，クライアント PC に導入したエージェントが SSO の対象システムのログイン画面を監視し，ログイン画面が表示されたら認証情報を代行入力する。

ウ　代理認証方式では，SSO の対象サーバに SSO のモジュールを組み込む必要があり，システムの改修が必要となる。

エ　リバースプロキシ方式では，SSO を利用する全てのトラフィックがリバースプロキシサーバに集中し，リバースプロキシサーバが単一障害点になり得る。

問８　前方秘匿性（Forward Secrecy）の説明として，適切なものはどれか。

ア　鍵交換に使った秘密鍵が漏えいしたとしても，それより前の暗号文は解読されない。

イ　時系列データをチェーンの形で結び，かつ，ネットワーク上の複数のノードで共有するので，データを改ざんできない。

ウ　対となる二つの鍵の片方の鍵で暗号化したデータは，もう片方の鍵でだけ復号できる。

エ　データに非可逆処理をして生成される固定長のハッシュ値からは，元のデータを推測できない。

問９　IT 製品及びシステムが，必要なセキュリティレベルを満たしているかどうかについて，調達者が判断する際に役立つ評価結果を提供し，独立したセキュリティ評価結果間の比較を可能にするための規格はどれか。

ア　ISO/IEC 15408　　イ　ISO/IEC 27002

ウ　ISO/IEC 27017　　エ　ISO/IEC 30147

問10　セキュリティ対策として，CASB（Cloud Access Security Broker）を利用した際の効果はどれか。

ア　クラウドサービスプロバイダが，運用しているクラウドサービスに対して，CASBを利用して DDoS 攻撃対策を行うことによって，クラウドサービスの可用性低下を緩和できる。

イ　クラウドサービスプロバイダが，クラウドサービスを運用している施設に対して，CASB を利用して入退室管理を行うことによって，クラウドサービス運用環境への物理的な不正アクセスを防止できる。

ウ　クラウドサービス利用組織の管理者が，従業員が利用しているクラウドサービスに対して，CASB を利用して脆弱性診断を行うことによって，脆弱性を特定できる。

エ　クラウドサービス利用組織の管理者が，従業員が利用しているクラウドサービスに対して，CASB を利用して利用状況の可視化を行うことによって，許可を得ずにクラウドサービスを利用している者を特定できる。

問11　クリックジャッキング攻撃に有効な対策はどれか。

ア　cookie に，HttpOnly 属性を設定する。

イ　cookie に，Secure 属性を設定する。

ウ　HTTP レスポンスヘッダーに，Strict-Transport-Security を設定する。

エ　HTTP レスポンスヘッダーに，X-Frame-Options を設定する。

問12　ブロックチェーンに関する記述のうち，適切なものはどれか。

ア　RADIUS を必須の技術として，参加者の利用者認証を一元管理するために利用する。

イ　SPF を必須の技術として，参加者間で電子メールを送受信するときに送信元の真正性を確認するために利用する。

ウ　楕円曲線暗号を必須の技術として，参加者間の P2P（Peer to Peer）通信を暗号化するために利用する。

エ　ハッシュ関数を必須の技術として，参加者がデータの改ざんを検出するために利用する。

問13　PC からサーバに対し，IPv6 を利用した通信を行う場合，ネットワーク層で暗号化を行うときに利用するものはどれか。

ア　IPsec　　イ　PPP　　ウ　SSH　　エ　TLS

問14　SMTP-AUTH の特徴はどれか。

ア　ISP 管理下の動的 IP アドレスから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メール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から，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，利用者 ID とパスワードなど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15　SPF によるドメイン認証を実施する場合，SPF の導入時に，電子メール送信元アドレスのドメイン所有者側で行う必要がある設定はどれか。

ア　DNS サーバに SPF レコードを登録する。

イ　DNS の問合せを受け付けるポート番号を変更する。

ウ　メールサーバにデジタル証明書を導入する。

エ　メールサーバの TCP ポート 25 番を利用不可にする。

問16　電子メール又はその通信を暗号化する三つのプロトコルについて，公開鍵を用意する単位の組合せのうち，適切なものはどれか。

	PGP	S/MIME	SMTP over TLS
ア	メールアドレスごと	メールアドレスごと	メールサーバごと
イ	メールアドレスごと	メールサーバごと	メールアドレスごと
ウ	メールサーバごと	メールアドレスごと	メールアドレスごと
エ	メールサーバごと	メールサーバごと	メールサーバごと

問17　無線 LAN のアクセスポイントがもつプライバシーセパレータ機能（アクセスポイントアイソレーション）の説明はどれか。

ア　アクセスポイントの識別子を知っている利用者だけに機器の接続を許可する。

イ　同じアクセスポイントに無線で接続している機器同士の通信を禁止する。

ウ　事前に登録された MAC アドレスをもつ機器だけに無線 LAN への接続を許可する。

エ　建物外への無線 LAN 電波の漏れを防ぐことによって第三者による盗聴を防止する。

問18　IPv6 の特徴として，適切なものはどれか。

ア　IPv6 アドレスから MAC アドレスを調べる際に ARP を使う。

イ　アドレス空間は IPv4 の 2^{128} 倍である。

ウ　経路の途中でフラグメンテーションを行うことが可能である。

エ　ヘッダーは固定長であり，拡張ヘッダー長は 8 オクテットの整数倍である。

問19　クラス D の IP アドレスを使用するのはどの場合か。

ア　端末数が 250 台程度までの比較的小規模なネットワークのホストアドレスを割り振る。

イ　端末数が 65,000 台程度の中規模なネットワークのホストアドレスを割り振る。

ウ　プライベートアドレスを割り振る。

エ　マルチキャストアドレスを割り振る。

問20　IP ネットワークにおいて，クライアントの設定を変えることなくデフォルトゲートウェイの障害を回避するために用いられるプロトコルはどれか。

ア　RARP　　イ　RSTP　　ウ　RTSP　　エ　VRRP

問21　表Rと表Sに対して，次のSQL文を実行した結果はどれか。

R

X	Y
A001	10
A002	20
A003	30
A005	50

S

X	Z
A002	20
A003	30
A004	40

〔SQL文〕

```
SELECT R.X AS A, R.Y AS B, S.X AS C, S.Z AS D
     FROM R LEFT OUTER JOIN S ON R.X = S.X
```

ア

A	B	C	D
A001	10	NULL	NULL
A005	50	NULL	NULL

イ

A	B	C	D
A002	20	A002	20
A003	30	A003	30
NULL	NULL	A004	40

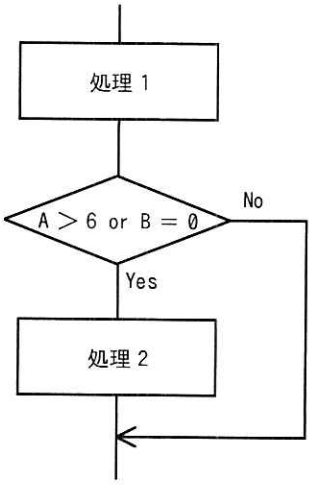
ウ

A	B	C	D
A001	10	NULL	NULL
A002	20	A002	20
A003	30	A003	30
A005	50	NULL	NULL

エ

A	B	C	D
A001	10	NULL	NULL
A002	20	A002	20
A003	30	A003	30
NULL	NULL	A004	40
A005	50	NULL	NULL

問22　あるプログラムについて，流れ図で示される部分に関するテストケースを，判定条件網羅（分岐網羅）によって設定する。この場合のテストケースの組合せとして，適切なものはどれか。ここで，（ ）で囲んだ部分は，一組みのテストケースを表すものとする。



ア　(A＝1, B＝1), (A＝7, B＝1)　　イ　(A＝4, B＝0), (A＝8, B＝1)

ウ　(A＝4, B＝1), (A＝6, B＝1)　　エ　(A＝7, B＝1), (A＝1, B＝0)

問23　SD メモリカードに使用される著作権保護技術はどれか。

ア　CPPM (Content Protection for Prerecorded Media)

イ　CPRM (Content Protection for Recordable Media)

ウ　DTCP (Digital Transmission Content Protection)

エ　HDCP (High-bandwidth Digital Content Protection)

問24　ある業務を新たにシステム化するに当たって，A～D のシステム化案の初期費用，運用費及びシステム化によって削減される業務費を試算したところ，表のとおりであった。システムの利用期間を 5 年とするとき，最も投資利益率の高いシステム化案はどれか。ここで，投資利益率は次式によって算出する。また，利益の増加額は削減される業務費から投資額を減じたものとし，投資額は初期費用と運用費の合計とする。

投資利益率 = 利益の増加額 ÷ 投資額

単位　百万円

システム化案	初期費用	1 年間の運用費	削減される 1 年間の業務費
A	30	4	25
B	20	6	20
C	20	4	15
D	15	5	22

ア　A　　イ　B　　ウ　C　　エ　D

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 〕

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。