SC

令和２年度
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〕　春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 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　Web サーバのログを分析したところ，Web サーバへの攻撃と思われる HTTP リクエストヘッダが記録されていた。次の HTTP リクエストヘッダから推測できる，攻撃者が悪用しようとしていた脆弱性はどれか。ここで，HTTP リクエストヘッダ中の“%20”は空白を意味する。

〔HTTP リクエストヘッダの一部〕

```
GET /cgi-bin/submit.cgi?user=;cat%20/etc/passwd HTTP/1.1
Accept: */*
Accept-Language: ja
UA-CPU: x86
Accept-Encoding: gzip, deflate
User-Agent:  (省略)
Host: test.example.com
Connection: Keep-Alive
```

ア　HTTP ヘッダインジェクション（HTTP Response Splitting）

イ　OS コマンドインジェクション

ウ　SQL インジェクション

エ　クロスサイトスクリプティング

問2　SAML（Security Assertion Markup Language）の説明として，最も適切なものはどれか。

ア　Web サービスに関する情報を公開し，Web サービスが提供する機能などを検索可能にするための仕様

イ　権限がない利用者による読取り，改ざんから電子メールを保護して送信するための仕様

ウ　ディジタル署名に使われる鍵情報を効率よく管理するための Web サービスの仕様

エ　認証情報に加え，属性情報とアクセス制御情報を異なるドメインに伝達するための Web サービスの仕様

問3　エクスプロイトコードの説明はどれか。

ア　攻撃コードとも呼ばれ，ソフトウェアの脆弱性を悪用するコードのことであり，使い方によっては脆弱性の検証に役立つこともある。

イ　マルウェア定義ファイルとも呼ばれ，マルウェアを特定するための特徴的なコードのことであり，マルウェア対策ソフトによるマルウェアの検知に用いられる。

ウ　メッセージとシークレットデータから計算されるハッシュコードのことであり，メッセージの改ざん検知に用いられる。

エ　ログインのたびに変化する認証コードのことであり，窃取されても再利用できないので不正アクセスを防ぐ。

問4　サイドチャネル攻撃に該当するものはどれか。

ア　暗号アルゴリズムを実装した攻撃対象の物理デバイスから得られる物理量（処理時間や消費電力など）やエラーメッセージから，攻撃対象の秘密情報を得る。

イ　企業などの秘密情報を窃取するソーシャルエンジニアリングの手法の一つであり，不用意に捨てられた秘密情報の印刷物をオフィスの紙ごみの中から探し出す。

ウ　通信を行う 2 者間に割り込んで，両者が交換する情報を自分のものとすり替えることによって，その後の通信を気付かれることなく盗聴する。

エ　データベースを利用する Web サイトに入力パラメタとして SQL 文の断片を送信することによって，データベースを改ざんする。

問5　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正当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）ネットワーク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6　総務省及び国立研究開発法人情報通信研究機構（NICT）が 2019 年 2 月から実施している取組“NOTICE”に関する記述のうち，適切なものはどれか。

ア　NICT が運用するダークネット観測網において，Mirai などのマルウェアに感染した IoT 機器から到達するパケットを分析した結果を当該機器の製造者に提供し，国内での必要な対策を促す。

イ　国内のグローバル IP アドレスを有する IoT 機器に，容易に推測されるパスワードを入力することなどによって，サイバー攻撃に悪用されるおそれのある機器を調査し，インターネットサービスプロバイダを通じて当該機器の利用者に注意喚起を行う。

ウ　国内の利用者からの申告に基づき，利用者の所有する IoT 機器に対して無料でリモートから，侵入テストや OS の既知の脆弱性の有無の調査を実施し，結果を通知するとともに，利用者が自ら必要な対処ができるよう支援する。

エ　製品のリリース前に，不要にもかかわらず開放されているポートの存在，パスワードの設定漏れなど約 200 項目の脆弱性の有無を調査できるテストベッドを国内の IoT 機器製造者向けに公開し，市場に流通する IoT 機器のセキュリティ向上を目指す。

問７　経済産業省が“サイバー・フィジカル・セキュリティ対策フレームワーク（Version 1.0）”を策定した主な目的の一つはどれか。

ア　ICT を活用し，場所や時間を有効に活用できる柔軟な働き方（テレワーク）の形態を示し，テレワークの形態に応じた情報セキュリティ対策の考え方を示すこと

イ　新たな産業社会において付加価値を創造する活動が直面するリスクを適切に捉えるためのモデルを構築し，求められるセキュリティ対策の全体像を整理すること

ウ　クラウドサービスの利用者と提供者が，セキュリティ管理策の実施について容易に連携できるように，実施の手引を利用者向けと提供者向けの対で記述すること

エ　データセンタの利用者と事業者に対して“データセンタの適切なセキュリティ”とは何かを考え，共有すべき知見を提供すること

問８　CRYPTREC の主な活動内容はどれか。

ア　暗号技術の技術的検討並びに国際競争力の向上及び運用面での安全性向上に関する検討を行う。

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て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　3D セキュアは，ネットショッピングでのオンライン決済におけるクレジットカードの不正使用を防止する対策の一つである。3D セキュアに関する記述のうち，適切なものはどれか。

ア　クレジットカードの PIN（Personal Identification Number：暗証番号）を入力させ，検証することによって，なりすましによる不正使用を防止する。

イ　クレジットカードのセキュリティコード（カードの裏面又は表面に記載された 3 桁又は 4 桁の番号）を入力させ，検証することによって，クレジットカードの不正使用を防止する。

ウ　クレジットカードの有効期限を入力させ，検証することによって，期限切れクレジットカードの不正使用を防止する。

エ　クレジットカード発行会社にあらかじめ登録したパスワードなど，本人しか分からない情報を入力させ，検証することによって，なりすましによるクレジットカードの不正使用を防止する。

問10　インターネットバンキングの利用時に被害をもたらす MITB（Man in the Browser）攻撃に有効な対策はどれか。

ア　インターネットバンキングでの送金時に接続する Web サイトの正当性を確認できるよう，EV SSL サーバ証明書を採用する。

イ　インターネットバンキングでの送金時に利用者が入力した情報と，金融機関が受信した情報とに差異がないことを検証できるよう，トランザクション署名を利用する。

ウ　インターネットバンキングでのログイン認証において，一定時間ごとに自動的に新しいパスワードに変更されるワンタイムパスワードを用意する。

エ　インターネットバンキング利用時の通信を SSL ではなく TLS を利用して暗号化する。

問11　JIS X 9401:2016（情報技術－クラウドコンピューティング－概要及び用語）の定義によるクラウドサービス区分の一つであり，クラウドサービスカスタマが表中の項番 1 と 2 の責務を負い，クラウドサービスプロバイダが項番 3 ～ 5 の責務を負うものはどれか。

項番	責　務
1	アプリケーションソフトウェアに対して，データ利用時のアクセス制御と暗号化の設定を行う。
2	アプリケーションソフトウェアに対して，セキュアプログラミングとソースコードの脆弱性診断を行う。
3	DBMS に対して，修正プログラム適用と権限設定を行う。
4	OS に対して，修正プログラム適用と権限設定を行う。
5	ハードウェアに対して，アクセス制御と物理セキュリティ確保を行う。

ア　HaaS　　イ　IaaS　　ウ　PaaS　　エ　SaaS

問12　Web サーバが HTTP over TLS（HTTPS）通信の応答で cookie に Secure 属性を設定するときの Web サーバ及び Web ブラウザの処理はどれか。

ア　Web サーバでは，cookie 発行時に“Secure=”に続いて時間を設定し，Web ブラウザでは，指定された時間を参照し，指定された時間を過ぎている場合にその cookie を削除する。

イ　Web サーバでは，cookie 発行時に“Secure=”に続いてホスト名を設定し，Web ブラウザでは，指定されたホスト名を参照し，指定されたホストにその cookie を送信する。

ウ　Web サーバでは，cookie 発行時に“Secure”を設定し，Web ブラウザでは，それを参照し，HTTPS 通信時にだけその cookie を送信する。

エ　Web サーバでは，cookie 発行時に“Secure”を設定し，Web ブラウザでは，それを参照し，Web ブラウザの終了時に cookie の他の属性によらず，その cookie を削除する。

問13　ディジタルフォレンジックスに該当するものはどれか。

ア　画像や音楽などのディジタルコンテンツに著作権者などの情報を埋め込む。

イ　コンピュータやネットワークのセキュリティ上の弱点を発見するテスト手法の一つであり，システムを実際に攻撃して侵入を試みる。

ウ　巧みな話術や盗み聞き，盗み見などの手段によって，ネットワークの管理者や利用者などから，パスワードなどのセキュリティ上重要な情報を入手する。

エ　犯罪に関する証拠となり得るデータを保全し，調査，分析，その後の訴訟などに備える。

問14　セキュリティ対策として，次の条件の下でデータベース（DB）サーバを DMZ から内部ネットワークに移動するようなネットワーク構成の変更を計画している。このとき，ステートフルパケットインスペクション型のファイアウォール（FW）において，必要となるフィルタリングルールの変更のうちの一つはどれか。

〔条件〕

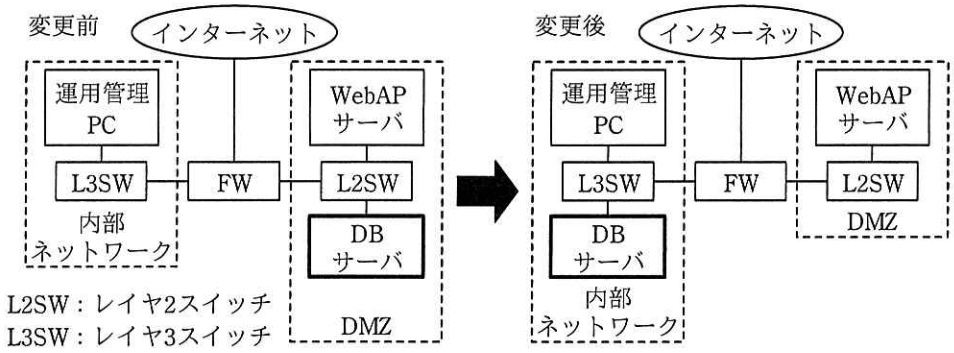
(1)　Web アプリケーション（WebAP）サーバを，インターネットに公開する。

(2)　WebAP サーバ上のプログラムだけが DB サーバ上の DB に接続でき，ODBC（Open Database Connectivity）を使用して特定のポート間で通信する。

(3)　SSH を使用して各サーバに接続できるのは，運用管理 PC だけである。

(4)　フィルタリングルールは，必要な通信だけを許可する設定にする。

〔ネットワーク構成〕



	ルールの変更種別	ルール			
		送信元	宛先	サービス	制御
ア	削除	インターネット	WebAP サーバ	HTTP	許可
イ	削除	運用管理 PC	変更前の DB サーバ	SSH	許可
ウ	追加	WebAP サーバ	変更後の DB サーバ	SSH	許可
エ	追加	インターネット	WebAP サーバ	ODBC	許可

問15　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 の入力誤りを悪用して，偽サイトに誘導する攻撃の検知

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　インターネットサービスプロバイダ（ISP）が，スパムメール対策として導入するIP25Bに該当するものはどれか。

ア　自社ISPのネットワークの動的IPアドレスから他社ISPの管理するメールサーバへのSMTP通信を制限する。

イ　自社ISPのメールサーバで受信した電子メールのうち，スパムメールのシグネチャに一致する電子メールを隔離する。

ウ　他社ISPのネットワークの動的IPアドレスから自社ISPのメールサーバへのSMTP通信を制限する。

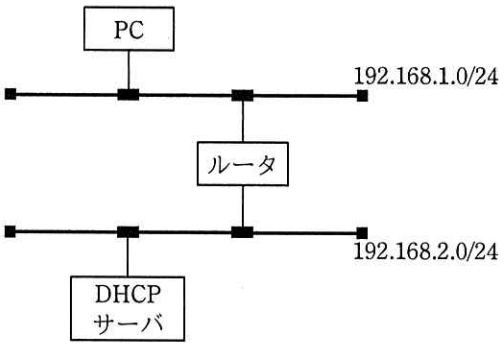
エ　他社ISPのメール不正中継の脆弱性をもつメールサーバから自社ISPのメールサーバに送信された電子メールを隔離する。

問18　図のように，サブネット 192.168.1.0/24 に PC を接続し，サブネット 192.168.2.0/24 にある DHCP サーバによって PC の IP アドレスの設定を行いたい。このとき，PC から DHCP サーバに対する最初の問合せの宛先 IP アドレスとして，適切なものはどれか。ここで，PC から DHCP サーバに対する最初の問合せにはブロードキャスト通信が使われ，更に次の条件を満たす。

〔条件〕

(1)　ルータでは DHCP リレーエージェントが動作している。

(2)　PC は自分自身のサブネット情報を知らない。



ア　192.168.1.0　　イ　192.168.1.255

ウ　192.168.2.255　　エ　255.255.255.255

問19　リモートアクセス環境において，認証情報やアカウンティング情報をやり取りするプロトコルはどれか。

ア　CHAP　　イ　PAP　　ウ　PPTP　　エ　RADIUS

問20　複数台のレイヤ 2 スイッチで構成されるネットワークが複数の経路をもつ場合に，イーサネットフレームのループの発生を防ぐための TCP/IP ネットワークインタフェース層のプロトコルはどれか。

ア　IGMP　　イ　RIP
ウ　SIP　　エ　スパニングツリープロトコル

問21　DBMS がトランザクションのコミット処理を完了するタイミングはどれか。

ア　アプリケーションプログラム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　ソフトウェアの要件定義における利用者の分析で活用される，ソフトウェアの利用者を役割ごとに典型的な姿として描いた仮想の人物を何と呼ぶか。

ア　エピック　　イ　ステークホルダ
ウ　プロダクトオーナ　　エ　ペルソナ

問23　アジャイル開発のプラクティスの一つである“ふりかえり（レトロスペクティブ）”を行う適切なタイミングはどれか。

ア　“タスクボード”に貼ったタスクカードが移動されたとき
イ　各“イテレーション”の最後
ウ　毎日行う“朝会”
エ　毎日メンバの気持ちを見える化する“ニコニコカレンダー”に全チームメンバが記入し終えたとき

問24　新システムの開発を計画している。提案された 4 案の中で，TCO（総所有費用）が最小のものはどれか。ここで，このシステムは開発後，3 年間使用されるものとする。

単位 百万円

	A案	B案	C案	D案
ハードウェア導入費用	30	30	40	40
システム開発費用	30	50	30	40
導入教育費用	5	5	5	5
ネットワーク通信費用／年	20	20	15	15
保守費用／年	6	5	5	5
システム運用費用／年	6	4	6	4

ア　A案　　イ　B案　　ウ　C案　　エ　D案

問25　プライバシーマークを取得している A 社は，個人情報管理台帳の取扱いについて内部監査を行った。判明した状況のうち，監査人が指摘事項として監査報告書に記載すべきものはどれか。

ア　個人情報管理台帳に，概数でしかつかめない個人情報の保有件数は概数だけで記載している。

イ　個人情報管理台帳に，ほかの項目に加えて，個人情報の保管場所，保管方法，保管期限を記載している。

ウ　個人情報管理台帳の機密性を守るための保護措置を講じている。

エ　個人情報管理台帳の見直しは，新たな個人情報の取得があった場合にだけ行っている。

〔 メ モ 用 紙 〕

〔 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。