SC

# 令和４年度　春期
# 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〕　春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　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可能性が高い脆弱性はどれか。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，属性情報と認可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　暗号化装置における暗号化処理時の消費電力を測定するなどして，当該装置内部の秘密情報を推定する攻撃はどれか。

ア　キーロガー　　イ　サイドチャネル攻撃

ウ　スミッシング　　エ　中間者攻撃

問４　パスワードに使用できる文字の種類の数を M，パスワードの文字数を n とするとき，設定できるパスワードの理論的な総数を求める数式はどれか。

ア　$M^n$　　イ　$\frac{M!}{(M-n)!}$

ウ　$\frac{M!}{n!\,(M-n)!}$　　エ　$\frac{(M+n-1)!}{n!\,(M-1)!}$

問５　標的型攻撃における攻撃者の行動をモデル化したものの一つにサイバーキルチェーンがあり，攻撃者の行動を 7 段階に分類している。標的とした会社に対する攻撃者の行動のうち，偵察の段階に分類されるものはどれか。

ア　攻撃者が，インターネットに公開されていない社内ポータルサイトから，会社の組織図，従業員情報，メールアドレスなどを入手する。

イ　攻撃者が，会社の役員が登録している SNS サイトから，攻撃対象の人間関係，趣味などを推定する。

ウ　攻撃者が，取引先になりすまして，標的とした会社にマルウェアを添付した攻撃メールを送付する。

エ　攻撃者が，ボットに感染した PC を遠隔操作して社内ネットワーク上の PC を次々にマルウェア感染させて，利用者 ID とパスワードを入手する。

問６　量子暗号の特徴として，適切なものはどれか。

ア　暗号化と復号の処理を，量子コンピュータを用いて瞬時に行うことができるので，従来のコンピュータでの処理に比べて大量のデータの秘匿を短時間で実現できる。

イ　共通鍵暗号方式であり，従来の情報の取扱量の最小単位であるビットの代わりに量子ビットを用いることによって，瞬時のデータ送受信が実現できる。

ウ　量子雑音を用いて疑似乱数を発生させて共通鍵を生成し，公開鍵暗号方式で共有することによって，解読が困難な秘匿通信が実現できる。

エ　量子通信路を用いて安全に共有した乱数列を使い捨ての暗号鍵として用いることによって，原理的に第三者に解読されない秘匿通信が実現できる。

問７　安全・安心なIT社会を実現するために創設された制度であり，IPA“中小企業の情報セキュリティ対策ガイドライン”に沿った情報セキュリティ対策に取り組むことを中小企業などが自己宣言するものはどれか。

ア　ISMS適合性評価制度

イ　ITセキュリティ評価及び認証制度

ウ　MyJVN

エ　SECURITY ACTION

問８　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 機器に対して，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９　経済産業省と IPA が策定した“サイバーセキュリティ経営ガイドライン（Ver 2.0)”に関する記述のうち，適切なものはどれか。

ア　経営者が，実施するサイバーセキュリティ対策を投資ではなくコストとして捉えることを重視し，コストパフォーマンスの良いサイバーセキュリティ対策をまとめたものである。

イ　経営者が認識すべきサイバーセキュリティに関する原則と，経営者がリーダシップを発揮して取り組むべき項目を取りまとめたものである。

ウ　事業の規模やビジネスモデルによらず，全ての経営者が自社に適用すべきサイバーセキュリティ対策を定めたものである。

エ　製造業のサプライチェーンを構成する小規模事業者の経営者が，サイバー攻撃を受けた際に行う事後対応をまとめたものである。

問10　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を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11　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）攻撃に有効なインターネットバンクでの対策はどれか。

ア　インターネットバンキングでの送金時に接続する Web サイトの正当性を利用者が確認できるよう，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導入する。

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ように Web サイトを設定する。

問12　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13　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14　HTTP Strict Transport Security (HSTS) の動作はどれか。

ア　HTTP over TLS (HTTPS) によって接続しているとき，EV SSL 証明書であることを利用者が容易に識別できるように，Web ブラウザのアドレス表示部分を緑色に表示する。

イ　Web サーバからコンテンツをダウンロードするとき，どの文字列が秘密情報かを判定できないように圧縮する。

ウ　Web サーバと Web ブラウザとの間の TLS のハンドシェイクにおいて，一度確立したセッションとは別の新たなセッションを確立するとき，既に確立したセッションを使って改めてハンドシェイクを行う。

エ　Web サイトにアクセスすると，Web ブラウザは，以降の指定された期間，当該サイトには全て HTTPS によって接続する。

問15　TLS に関する記述のうち，適切なものはどれか。

ア　TLS で使用する Web サーバのデジタル証明書には 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，デジタル証明書を再度取得する必要がある。

イ　TLS で使用する共通鍵の長さは，128 ビット未満で任意に指定する。

ウ　TLS で使用する個人認証用のデジタル証明書は，IC カードにも格納することができ，利用する PC を特定の PC に限定する必要はない。

エ　TLS は Web サーバと特定の利用者が通信するためのプロトコルであり，Web サーバへの事前の利用者登録が不可欠である。

問16　電子メールをスマートフォンで受信する際のメールサーバとスマートフォンとの間の通信を，メール本文を含めて暗号化するプロトコルはどれか。

ア　APOP　　イ　IMAPS

ウ　POP3　　エ　SMTP Submission

問17　利用者認証情報を管理するサーバ1台と複数のアクセスポイントで構成された無線LAN環境を実現したい。PCが無線LAN環境に接続するときの利用者認証とアクセス制御に，IEEE 802.1XとRADIUSを利用する場合の標準的な方法はどれか。

ア　PCにはIEEE 802.1Xのサプリカントを実装し，かつ，RADIUSクライアントの機能をもたせる。

イ　アクセスポイントにはIEEE 802.1Xのオーセンティケータを実装し，かつ，RADIUSクライアントの機能をもたせる。

ウ　アクセスポイントにはIEEE 802.1Xのサプリカントを実装し，かつ，RADIUSサーバの機能をもたせる。

エ　サーバにはIEEE 802.1Xのオーセンティケータを実装し，かつ，RADIUSサーバの機能をもたせる。

問18　IEEE 802.11a/b/g/nで採用されているアクセス制御方式はどれか。

ア　CSMA/CA　　イ　CSMA/CD

ウ　LAPB　　エ　トークンパッシング方式

問19　インターネットに接続されたPCの時刻合わせに使用されるプロトコルはどれか。

ア　NNTP　　イ　RTCP　　ウ　SNTP　　エ　TFTP

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が発生することがある。そ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　データウェアハウスのメタデータに関する記述のうち，データリネージはどれか。

ア　誰がどのデータを見てよいかを示す情報であり，適切なアクセス制御を目的として設定される。

イ　データが誰によって作られ管理されているかを示す情報であり，データ構造やデータ辞書を見ても意味が分からないときの問合せ先を表す。

ウ　データがどこから発生し，どのような変換及び加工を経て，現在の形になったかを示す情報であり，データの生成源の特定又は障害時の影響調査に利用できる。

エ　データ構造がどのように定義されているかを示す情報であり，Web サイトなどに公開して検索できるようにする。

問22　システムに規定外の無効なデータが入力されたとき，誤入力であることを伝えるメッセージを表示して正しい入力を促すことによって，システムを異常終了させない設計は何というか。

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　JIS X 0160:2021（ソフトウェアライフサイクルプロセス）によれば，ライフサイクルモデルの目的及び成果を達成するために，ライフサイクルプロセスを修正するか，又は新しいライフサイクルプロセスを定義することを何というか。

ア　シミュレーション　　イ　修整（Tailoring）
ウ　統治（Governance）　　エ　ベンチマーキング

問24　サービス提供時間帯が毎日 0～24 時の IT サービスにおいて，ある年の 4 月 1 日 0 時から 6 月 30 日 24 時までのサービス停止状況は表のとおりであった。システムバージョンアップ作業に伴う停止時間は，計画停止時間として顧客との間で合意されている。このとき，4 月 1 日から 6 月 30 日までの IT サービスのサービス可用性は何%か。ここで，サービス可用性（%）は小数第 3 位を四捨五入するものとする。

〔サービス停止状況〕

| 停止理由 | 停止時間 |
|---|---|
| システムバージョンアップ作業に伴う停止 | 5 月 2 日 22 時から 5 月 6 日 10 時までの 84 時間 |
| ハードウェア故障に伴う停止 | 6 月 26 日 10 時から 20 時までの 10 時間 |

ア　95.52　　イ　95.70　　ウ　99.52　　エ　99.63

問25　金融庁“財務報告に係る内部統制の評価及び監査に関する実施基準（令和元年）”におけるアクセス管理に関して，内部統制のうちの IT に係る業務処理統制に該当するものはどれか。

ア　組織としてアクセス管理規程を定め，統一的なアクセス管理を行う。

イ　組織としてアクセス権限の設定方針を定め，周知徹底を図る。

ウ　組織内のアプリケーションシステムに，業務内容に応じた権限を付与した利用者 ID とパスワードによって認証する機能を設ける。

エ　組織内の全ての利用者に対して，アクセス管理の重要性についての教育を行う。

〔 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。