2024 秋 情報処理安全確保支援士 全国統一公開模試 講評と採点基準

2024 年 9 月 25 日 (株)アイテック IT 人材教育研究部

■ 全体講評

今回の公開模試における午後試験の平均点は，38.9 点でした。問題別の平均点は，問 1 が 13.4 点，問 2 が 19.4 点，問 3 が 21.6 点，問 4 が 20.7 点という結果でした。2024 年春の公開模試における午後試験の平均点は 38.9 点でしたから，全く同じ結果でした。

午後試験において合格基準点をクリアするには，記述式の問題に対する取組み方が重要になってきます。記述式の問題の多くは，下線に関するものが出題されます。すると，解答を作成する際，どうしても下線部だけに注目しがちです。しかし，下線部だけに注目してしまうと，その前後にある条件などを見落としてしまい，的を射た解答をなかなか作成することができません。今回の模試でも，こうした解答が少なからず見られました。設問で何が問われているかを十分に確認し，下線部の記述だけではなく，その前後に記述された内容なども含め，よく整理し解答を作成することが大切です。なお，記述式の問題については，それぞれの設問で求める解答は基本的に一つの内容を答えさせるように条件が付けられています。このため，主語と述語，あるいは目的語は何かなどを明確にした上で，採点者に理解されやすい解答を作成するようにしましょう。

次に，問題ごとの選択状況を紹介します。問 1（Web アプリケーションの開発と運用）と問 2（データセキュリティ）の選択者が 20.2%，問 1 と問 3（IoT 機器のセキュリティ）が 3.8%，問 1 と問 4（無線 LAN 及び EC サイトのセキュリティ）が 3.3%，問 2 と問 3 が 36.6%，問 2 と問 4 が 23.0%，問 3 と問 4 が 13.1%という状況でした。問ごとでは，問 1 が 13.6%，問 2 が 40.1%，問 3 が 26.7%，問 4 が 19.6%でした。

10 月 13 日に実施予定の本試験において，4 問のうち 2 問を選択する方法としては，各自が得意とする分野の問題をいち早くみつけ出し，それに集中して取り組むとよいでしょう。例えば，得意分野の問題で 40 点近くの点数を獲得できれば，もう一つの問題で 20 点強を得点するだけで，午後試験はクリアすることができます。しかし，こうしたことを達成するには，問題の記述内容を十分に把握するだけの知識が要求されます。本試験実施日までの期間で，より一層のレベルアップを図るようにしましょう。

午後試験の記述式問題の多くは，問題文の中に解答を導くためのヒントが記述されています。一定の知識レベルに達していれば，問題文に記述された内容を基にして正解を導き出すことができます。しかし，下線に関する設問の場合，その下線部だけに着目して答案を作成するという傾向が見られます。すると，問題に設定されている条件をほとんど考慮することなく，ご自身の知識や下線に関する内容から思いつくことだけを解答してしまいます。前述したように，午後試験では，設問で問われていることを十分に確認した上で，問題の条件を適宜，チェックしながら，合理的に導かれる解答を作成していくことが極めて重要です。技術・知識面だけではなく，こうした訓練を積み重ねていくことも必要になります。

いずれにしても，試験当日は集中力，精神力，体力の勝負になります。必ず合格するという強い意志をもって，最後まで全力を出し切り（あきらめずに）問題に取り組んで，ぜひ合格するようにしましょう。

問1 Web アプリケーションの開発と運用

【採点基準】

[設問1]

（1）解答例と同様の趣旨が適切に指摘されているものに対し 6 点。その他は，基本的に 0 点。

（2）解答例と同様の趣旨が適切に指摘されているものに対し 6 点。その他は，基本的に 0 点。

（3）解答例と同様の趣旨（レスポンスボディへの出力要素に対するエスケープ処理）が適切に指摘されているものに対し 6 点。その他は，基本的に 0 点。

[設問2]

（1）a は，解答例どおりに対し 2 点。

（2）解答例と同様の趣旨が適切に指摘されているものに対し 6 点。その他は，基本的に 0 点。

[設問3]

（1）オープンリダイレクトの脆弱性を悪用し，攻撃者が偽サーバに誘導する手口と，偽サーバにおいて利用者のログイン情報を窃取する方法を分かりやすく説明したものに対し 8 点。指摘内容が今一歩のものは 4 点。その他は 0 点。

（2）b は，解答例どおりに対し 2 点。

[設問4]

（1）c，d は，解答例どおりに対し各 2 点。

（2）解答例と同様の趣旨が適切に指摘されているものに対し 5 点。その他は，基本的に 0 点。

（3）解答例と同様の趣旨が適切に指摘されているものに対し 5 点。その他は，基本的に 0 点。

【講評】

平均点は 13.4 点と，4 問の中では最も低い点数にとどまりました。選択者数についても，全体の 13.6%であ

り，Web アプリケーションの問題は敬遠される傾向にあります。

設問 1 の正答率は，総じて低かったと思います。例えば，(1)は adr1，adr2，adr3 を連結した後，script を除くことについては指摘されていましたが，その script を除いた後に現れる script を削除する必要があることについては，考えが及ばなかったようです。(2)は，格納型 XSS の特徴を解答した答案も散見されましたが，図 1 の表示画面が参照される画面はどの画面かなどを見極めた上で，解答を考えるとよかったのではないでしょうか。(3)は，入力データに対するエスケープ処理には言及されていましたが，レスポンスボディの出力要素に対するエスケープ処理が必要になることを解答してほしかったと思います。

設問 2 の正答率は平均的だったと思われます。(2)は，想定より正答率は高かったのではないでしょうか。

設問 3 は，図 4 からリダイレクトさせる方法などを指摘したものなどが散見されましたが，問題文の〔脆弱性 3〕に「サイト X では，利用者がログイン前の状態で，メンバーメニューに含まれるページの URL を直接指定するなどしてアクセスし，エラーが発生した場合，リダイレクト機能を用いてログインページに誘導する」という説明があります。これを基にして，攻撃者がどのような手法を使えば，攻撃者の偽サーバに誘導できるかを考えてほしかったと思います。そして，利用者のログイン情報を窃取するためには，利用者に気付かれないようにする必要があることから，サイト X のログインページを真似たページを表示することもポイントになります。

設問 4 の正答率は平均的だったと思われます。(3)については，表 2「試験環境の主要な機器の概要」から，送信元のサーバが何になるかを見極め，どのように制限するのかという点を解答してほしかったと思います。

問2 データセキュリティ

【採点基準】

［設問1］

a～e は，解答例どおりに対し各 2 点。

［設問2］

(1) 解答例どおりに対し 2 点（完答）。

(2) i は，解答例と同様の趣旨が適切に指摘されているもの（HTTP レスポンスと HTTP リクエストの内容が適切なもの）に対し 6 点。その他は，基本的に 0 点。

(3) 解答例と同様の趣旨が適切に指摘されているもの（クライアント秘密鍵を TPM に格納するなど）に対し 4 点。「クライアント秘密鍵をインストールする」は 2 点。「クライアント証明書をインストールする」は 0 点。

(4) 解答例と同様の趣旨が適切に指摘されているものに対し 6 点。指摘内容が今一歩のものは 3 点。その他は 0 点。

［設問3］

(1) 公開鍵，秘密鍵は，解答例どおりに対し各 2 点。

(2) 解答例と同様の趣旨が適切に指摘されているものに対し 5 点。その他は，基本的に 0 点。

(3) 解答例と同様の趣旨が適切に指摘されているものに対し 5 点。その他は，基本的に 0 点。

［設問4］

(1) j は，解答例と同様の意味合いをもつに対し 4 点。その他は，基本的に 0 点。

(2) 解答例と同様の意味合いをもつに対し 4 点。その他は，基本的に 0 点。

【講評】

平均点は 19.4 点であり，4 問の中では，問 1 に次いで低い点数でした。一方，選択者数の比率は 40.1%でしたから，8 割の受験者が，この問題を選択していたことになります。

設問 1 の正答率は高かったです。基本的な用語は，正確に覚えられていたと思います。

設問 2 (2)は，問題に記述されている「IDaaS-U を利用する IdP-Initiated 方式では，利用者の認証処理に成功すると，登録されている SaaS が一覧表示され，従業員は，その中から利用する」という条件を反映していない答案が散見されましたが，シーケンスを考える際には問題の条件を素直に取り入れることが必要です。(3)の正答率も低かったです。「クライアント証明書をインストールする」旨の答案が散見されましたが，TLS クライアント認証において，許可された D-PC に限定するためには，その D-PC が秘密鍵を所持しているかどうかによって決まります。例えば，秘密鍵をコピーして，別の D-PC にインストールされてしまうと，別の D-PC もサービスを利用できるので，こうした事態が起こらないようにする必要があります。その対策として，秘密鍵を TPM（Trusted Platform Module）に格納することがよく行われています。いずれにしても，クライアント証明書の公開鍵に対応する秘密鍵は，その本人しか保有していないので，秘密鍵を所有しているかどうかが判別するためのポイントになります。この点については，よく理解しておくことが必要です。

設問 3 (1)，(2)の正答率は，やや低かったです。(2)は，デジタル署名を用いずにトークンだけをパラメータに付加することによって，ダウンロード用 URL を推測することが困難になる理由を問うものでしたが，設問で問

われていることを十分に把握されていないような印象を受けました。(3)は，図 4 の URL パラメータとして付加される情報を把握した上で，解答が作成されていたように思われます。このため，(3)の正答率は，(2)の正答率よりも，少し高かったと思います。

設問 4 (1)は，空欄に入れる適切な字句を 25 字以内で答えるものでしたから，正答率は，やや低かったと思います。(2)の正答率は，平均的でした。

問3 IoT 機器のセキュリティ

【採点基準】

［設問1］

a～e は，解答例どおりに対し各 2 点。

［設問2］

(1) 解答例どおりに対し 2 点。

(2) 解答例と同様の趣旨が適切に指摘されているものに対し 6 点。その他は，基本的に 0 点。

(3) 解答例と同様の趣旨が適切に指摘されているものに対し 6 点。その他は，基本的に 0 点。

(4) f～h は，解答例どおりに対し各 2 点。

［設問3］

(1) 解答例どおりに対し 6 点（完答）。

(2) 解答例と同様の趣旨が適切に指摘されているものに対し 6 点。その他は，基本的に 0 点。

(3) 解答例と同様の趣旨が適切に指摘されているものに対し 6 点。その他は，基本的に 0 点。

(4) i は，解答例どおりに対し 2 点。

【講評】

平均点は 21.6 点で，午後 I の中では，最も高い点数でした。選択者数は，26.7%でした。4 問の中から，2 問を選択するので，ほぼ半数の受験者が選択していたことになります。

設問 1 の正答率は高かったです。パスワードとして使用される文字数と，パスワード長の文字数を，混同することなく，正しく計算されていたと思います。

設問 2 (1)，(2)は，ともに正答率は高かったです。(2)の DNS キャッシュポイズニング攻撃の対策の一つとして行われている，送信元ポート番号のランダム化については，十分に理解されているようでした。(3)の正答率は平均的でした。サーバ証明書の検証方法は，「サーバ証明書の有効期限が切れていないこと」，「サーバ証明書が失効していないこと」，「サーバ証明書が信頼された認証局から発行されたものであること」，「サーバ証明書のサブジェクト代替名あるいはコモンネームと，アクセス先の URL の FQDN が一致すること」という四つについて検証が行われます。基本的な事項の一つですから，正確に覚えておきましょう。(4)は，基本的な用語問題でしたから，正答率は高かったです。

設問 3 (1)の正答率は低かったです。Linux でコマンドを続けて実行させるためには“;”を用いることが必要です。(2)の正答率は，やや低かったと思います。入力されるデータの特徴を見極めれば，正解できると思っていましたが，そうではありませんでした。(3)，(4)の正答率は，ともに平均的でした。

問4 無線 LAN 及び EC サイトのセキュリティ

【採点基準】

［設問1］

(1) a，c は，解答例どおりに対し各 2 点。

(2) 解答例どおりに対し 4 点。

(3) b は，解答例どおりに対し 2 点。目的は，解答例と同様の趣旨が適切に指摘されているものに対し 4 点。その他は，基本的に 0 点。

(4) 解答例と同様の趣旨が適切に指摘されているものに対し 4 点。その他は，基本的に 0 点。

［設問2］

(1) d，e は，解答例どおりに対し各 3 点。

(2) f～h は，解答例どおりに対し各 2 点。

(3) 解答例と同様の趣旨が適切に指摘されているものに対し 4 点。その他は，基本的に 0 点。

(4) 解答例どおりに対し 4 点（完答）。

(5) 解答例と同様の趣旨が適切に指摘されているものに対し 6 点。その他は，基本的に 0 点。

(6) 解答例と同様の趣旨が適切に指摘されているものに対し 6 点。その他は，基本的に 0 点。

【講評】

平均点は 20.7 点でした。午後の 4 問の中では，問 3 の次に高い点数になりました。選択者数の比率は 19.6%でしたから，比率としてはやや低い選択率の問題といえます。

設問 1 (1)は，無線 LAN の規格に関するものでしたから，正答率は，少し低かったです。(2)の正答率は，想定していたよりも低かったです。何と何を比較して計算するのかといった点が整理できていなかったのではないでしょうか。(3)の正答率は，やや低かったと思います。SC 試験では，最近のセキュリティ技術に関する用語なども出題されるので，日頃から幅広い技術に対する関心を高めておくこともよいでしょう。(4)は，基本的な問題でしたから，正答率は高かったです。

設問 2 (1)の正答率は平均的でした。(2)は，基本的な用語問題でしたから，正答率は高かったです。(3)は，鍵交換アルゴリズムの問題です。TLS 1.3 で RSA，DH，

ECDH を廃止した理由を問うていますが，これらは，通信する 2 者間において，暗号化するための共通鍵やメッセージ認証を行うための認証鍵などを作成します。当初，RSA を鍵交換に使用することで問題はなかったのですが，RSA や DH などでは，一度，鍵交換を行った場合，その後，例えば，TLS ではクライアントでプリマスターシークレットを作成し，それをサーバの公開鍵で暗号化して，サーバに送信するので，プリマスターシークレット自身をクライアントとサーバで安全に共有することができていました。しかし，攻撃者がプリマスターシークレットを交換する過程のメッセージを全て保存し，一連のメッセージを分析することによって，鍵交換に使用している秘密鍵を特定できてしまうという問題が指摘されました。このため，鍵交換に使用する鍵ペアを，通信を行うセッションごとに作成し直すようになったのです。なお，鍵交換で使用する RSA や DH の鍵ペアが破られたとしてもセッションキー（共通鍵）の安全性が保たれるという性質のことを PFS（Perfect Forward Secrecy；前方秘匿性）と呼びます。(4)の正答率は，やや低かったと思います。この設問で問われていることは，問題の記述内容に基づき，TLS で使用する暗号を，セキュリティ面において最も優先すべきものを選択することです。問題の該当箇所を丁寧に読んでいけば，それぞれの候補を絞ることができると思います。(5)の正答率は低かったです。H 社のように，自社でプライベート CA を立ち上げてサーバ証明書を発行する場合，ブラウザには，基本的にプライベート CA のルート証明書が組み込まれているわけではありません。このような場合には，プライベート CA のルート証明書をブラウザにインストールする作業が発生します。(6)の正答率は，低かったです。

午後試験の試験時間は 2 時間 30 分，4 問の中から 2 問を選択して解答します。このため，1 問当たり 75 分を割り当てることができるので，時間的な余裕はあると思われます。例えば，最初に選択する問題を 2 問に絞ることができれば，その 2 問に集中することができます。おそらく，問題選択に当たって迷いが生じるのは，3 問の中から 2 問を選択する場合ではないでしょうか。このような場合には，問題選択に当てる時間として，20 分程度をあらかじめ見込んでおくこともよいかもしれません。

いずれにしても，解答する問題を決めると，その後は問題文を十分に読み込んでください。例えば，最初に読む際に，空欄に入れる字句が分かれば，その字句を入れておきましょう。一読した後，設問で問われていることを確認します。設問で問われている意味をよく理解し，その設問に関連する問題文を十分にチェックするようにしましょう。解答を導くための関係などを整理する際には，頭の中だけで考えるのではなく，メモのような形にして目に見えるようにして考えるとよいでしょう。そうすれば，条件の見落としなどが少なくなり，解答を作成しやすくなるはずです。

しかし，こうした作業がスムーズに実施できるようになるには，どうしてもセキュリティ関連の知識を十分にもち合わせているかどうかがポイントといえます。このため，10 月 13 日に行われる本試験の実施日に向けて，より多くの知識を吸収するなどして，さらなるレベルアップを図るようにしましょう。

試験当日において，問題に向き合ってみると，全く歯が立たないなどの印象を受けることがありますが，十分な実力を付けていれば，問題を丁寧に読んでいくことによって，解決の糸口をみつけられるはずです。そして，自分自身の考えがまとまれば，的確で理解しやすい内容の答案を作成するようにしましょう。たとえ，行き詰ったりしても，必ず合格するという強い気持ちをもって，粘り強く取り組んでいくことを忘れないようにしましょう。

以上