2024 春 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 3 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 18.8 点，問 2 が 17.5 点，問 3 が 21.6 点，問 4 が 17.8 点という結果でした。2023 年秋の公開模試における午後試験の平均点の 48.8 点に比較すると，約 10 点低下しています。

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を含め，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 アプリケーション開発のセキュリティ）と問 2（データアクセスのセキュリティ）の選択者が 5.5%，問 1 と問 3（クラウドサービスへの移行）が 3.7%，問 1 と問 4（フィッシングメールの対策）が 1.8%，問 2 と問 3 が 30.1%，問 2 と問 4 が 8.6%，問 3 と問 4 が 44.8%という状況でした。問ごとでは，問 1 が 8.3%，問 2 が 23.8%，問 3 が 40.4%，問 4 が 27.5%でした。

4 月 21 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見つけ出し，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 アプリケーション開発のセキュリティ

【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）a，b は，解答例どおりに対し各 2 点。

［設問2］

（1）解答例どおり（完答）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（入力パラメータをそのまま用いて SQL 文を組み立てる旨）に対し 4 点。その他は，基本的に 0 点。

（3）c，d は，解答例どおりに対し各 2 点。

［設問3］

（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 4 点。その他は，基本的に 0 点。

（3）e は，解答例どおりに対し 2 点。

（4）f は，解答例どおりに対し 2 点。

（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各 4 点。その他は，基本的に 0 点。

［設問4］

（1）g は，解答例どおりに対し 2 点。

（2）h は，解答例どおりに対し 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。

【講評】

平均点は 18.8 点であり，全体として平均正答率は少し低かったようです。選択者数についても，全体の 8.3%に過ぎず，多くの受験者は問 1 を敬遠していたといえます。

設問 1 (1)の正答率は低かったと思います。他人の会員情報を不正に取得する方法を，論理的に考えられなかったのでしょうか。また，(2)の正答率もよくなかったです。抽出条件として何を設定すればよいかなど，問題の条件を十分に確認しながら，考察していくとよいでしょう。しかし，問題の条件を的確に把握するには，それに見合う知識が必要です。Web 関連の問題を選択する場合には，IPA が公開している「安全なウェブサイトの作り方」，「安全な SQL の呼び出し方」などの資料を学習し，基本的な知識を十分に把握するようにしましょう。

設問 2 (1)の正答率は低かったです。頭の中だけでなく，組み立てられる文字列を実際に書いてみると，見落としが少なくなるはずです。(2)は，採点者が理解できるような表現の答案が少なかったと思います。(3)も，正答率は低かったです。

設問 3 (1)の正答率は高かったです。CSRF トークンの検証方法は理解されていると感じられました。(2)の正答率は低かったと思います。SameSite 属性の意味は理解されていますが，その値を“Strict”にした場合の効果が，具体的に表現されていなかったと思います。(3)～(5)の正答率も比較的低かったようです。(3)のサーバサイドリクエストフォージェリは，まだ馴染みが少ないようでした。(4)の HTTP の認証に関するヘッダーは，紛らわしいものが多いので，日頃から一つ一つの知識を積み重ねていくことを大切にするとよいでしょう。(5)では，「(い) の影響につながる HTTP リクエストの特徴」を問いましたが，「(い) の影響」とは何かを確認しないで答案が作成されているように見受けられました。

設問 4 (1)の正答率は低かったです。“Included in 1”における“1”が何を示すかを把握するのが難しかったようです。中には正解されている方もいましたが，表の中の依存関係にある値を単純に答えてしまいますので，日頃から柔軟に考える能力を鍛えておきましょう。(2)，(3)も正答率は低かったです。

問2 データアクセスのセキュリティ

【採点基準】

［設問1］

（1）a は，解答例どおりに対し 2 点。

（2）b は，解答例どおりに対し 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 6 点。指摘内容が今一歩のものは 3 点。その他は 0 点。

［設問2］

（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 4 点。IP アドレスを指摘したものなどは，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 4 点。その他は，基本的に 0 点。

（4）c，d は，解答例どおりに対し各 2 点。

［設問3］

e は，解答例どおりに対し 4 点。その他は 0 点。

［設問4］

（1）f～j は，解答例どおりに対し各 2 点。ただし，h は“高速”と同様の意味合いをもつものも 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）k は，解答例どおりに対し 2 点。

【講評】

平均点は 17.5 点であり，4 問の中では，最も低い点数（低い正答率）でした。選択者数の比率は 23.8%と，平均的な選択率の 25.0%と同程度といえます。

設問 1 (1)の正答率は平均的でしたが，(2)の正答率は高かったです。(3)の正答率は低かったです。ディレクトリトラバーサル（パストラバーサル）攻撃については，よく理解されていますが，入力パラメータとして何を入力されると，どのようなことが引き起こされるかといったことなどが，具体的に表現できていないように思われました。

設問 2 (1)の正答率は低かったです。デジタル署名とは何かという基本に立ち返り，問題の記述内容に従って素直に解答を導いていくことが必要です。例えば，問題の図 3 の「1. 署名付き cookie の発行と検証」に「認証サービスは，（中略）署名付き cookie を発行する」，「ストレージサービスでは，リクエストの署名付き cookie の署名を検証する」とありますから，署名を検証するストレージサービスでは，公開鍵を登録しなければなりません。その署名を誰が付けているかというと，それは認証サービスですから，署名の作成に必要になる秘密鍵は，認証サービスにもたせる必要があります。このように解答に結び付く記述は，問題文中にあるはずですから，ポイントになる記述を見落とさないようにしましょう。(2)の正答率は平均的でしたが，(3)，(4)の正答率は低かったです。HTTP の cookie に関する問題は，比較的出題頻度の高い問題ですから，理解を深めておきましょう。

設問 3 の正答率は平均的でした。問題の条件から適切に解答されてました。

設問 4 (1)の f は「認証コード」という答案も見られましたが，正しくは「メッセージ認証コード」です。正しい名称で答えるようにしましょう。g，h の正答率は平均的でしたが，i，j の正答率は低かったと思います。(2)

の正答率は低かったです。su コマンドと sudo コマンドの違いなどの基本的な知識の理解を，徐々に深めていくことも忘れないようにしましょう。(3)の正答率は比較的低かったです。

問3 クラウドサービスへの移行

【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) a は，解答例どおりに対し 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 6 点。指摘内容が今一歩のものは 3 点。その他は 0 点。
(4) b は，解答例どおりに対し 2 点。
(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。

［設問2］

(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各 3 点。その他は，基本的に 0 点。
(2) c～e は，解答例どおりに対し各 2 点。

［設問3］

(1) f，g は，解答例どおりに対し各 2 点。
(2) 図 6 中の番号と state パラメータの確認方法について，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) 図 6 中の番号と，チャレンジコードと検証コードの関係について，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。

【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。選択者数も 4 問の中では，最も多い 40.4%に達し，クラウドサービスの認証連携などの問題は，対策がかなり行き届いていると感じられました。

設問 1 (1)の正答率は平均的でした。CDN では，インターネット上に分散配置されたキャッシュサーバが，利用者からの要求を受け付けることが特徴です。(2)の正答率は平均的でした。ドメインフロンティング攻撃については，その理解が徐々に進んでいると思われます。(3)の正答率は少し低かったように思います。この設問は，どのように答案を作成するか，苦労する面があったと思いますが，採点者は答案用紙に書かれた内容によって判断するしか方法がありません。そのため，採点者にとって分かりやすい内容で記述されているかを，見直すようにすれば，得点がアップすることも期待できます。(4)の正答率は平均的でした。(5)の正答率は比較的高かったと思います。HTTP リクエストの Host ヘッダーの使い方は，よく理解されていると感じられました。欲を言えば，設問では「TLS の何と，HTTP の何を比較」が問われていますので，図 3 中の「TLS の接続先サーバ名（SNI）」を指摘して欲しかったです。

設問 2 (1) の正答率は想定していたよりも低かったです。デジタル署名は，送信元の真正性と，署名対象データの完全性を保証する技術であることは，十分に理解されていますが，この設問では「SAML Response に含まれるデジタル署名を検証する」について，確認できる事項が二つ問われています。このため，問題に記述されている内容に基づいて，デジタル署名の送信元は誰で，署名対象データは何かを明確に答えることが必要です。例えば，署名対象データについては，「SAML Response が改ざんされていないこと」などの答案も見られましたが，表 1 の処理 3 には「SAML アサーションと，それに対するデジタル署名を含めた SAML Response の送信フォームを生成する」と記述されています。つまり，署名対象データは，SAML アサーションであることが分かります。このように，記述式の設問に対する答案は，丁寧に作成することが大切ですから，本番の試験では注意して取り組んでみてください。(2)の正答率は，平均的でした。なお，e については，デジタル署名という答案も見られましたが，デジタル署名を検証するための公開鍵証明書（デジタル証明書）が必要になることに気付いてほしいと思います。

設問 3 (1)の正答率は高かったです。(2)の正答率も高かったです。state パラメータの使い方は，よく理解されていますが，F サービスで送信元（Web ブラウザ）の確認を行うには，図 6 中の何番と何番のデータを比較することが必要になるかを考えることが必要です。(3)の正答率は低かったと思います。チャレンジコードは検証コードを基にして生成されることは理解されていましたが，この設問は，スマホアプリの確認を行うためには，図 6 中の何番と何番のデータを比較すればよいかという判断が，適切に行われていなかったようです。

問4 フィッシングメールの対策

【採点基準】

［設問1］

(1) a，b は，解答例どおりに対し各 2 点。
(2) c，d は，解答例どおりに対し各 2 点。
(3) e は，解答例どおりに対し 2 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。その他は，基本的に 0 点。
(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 4 点。その他は，基本的に 0 点。

［設問2］

（1）f 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 4 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 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 6 点。その他は，基本的に 0 点。

（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）g～n は，解答例どおりに対し各 1 点。

【講評】

平均点は 17.8 点でした。午後の 4 問の中では，問 2 とほぼ同程度であり，低い正答率に止まったといえます。選択者数の比率は 27.5%でしたから，平均的な選択率の 25.0%とほぼ同程度です。

設問 1 (1)の正答率は，高かったです。その半面，(2)の正答率は低かったです。公開鍵証明書の一つである，S/MIME 証明書の公開鍵は，誰の（何の）公開鍵の正当性を保証するかという問題です。サーバ証明書の場合はサーバの公開鍵と分かりますが，S/MIME 証明書と聞かれた場合には，十分に理解していなかったようです。(3)の正答率は低かったです。Web of Trust（エ）ではなく，PKI で使用される Trust Anchor（ウ）の方が多かったと思います。(4)，(5)の正答率は比較的低かったと思います。

設問 2 (1)の正答率は低かったです。図 2 を参考にし，IP アドレスを指定する場合には，それぞれの IP アドレスごとに，機構の“+ip4: ”を付けることが必要です。(2)は，メールの転送に当たって，転送メールサーバが介在する場合に SPF の認証に失敗することは，よく知られています。このため，この設問では，「転送メールサーバがどのようにメールを転送しているか」を問いました。少し視点を変えた出題だったためか，正答率は低かったです。(3)の正答率は，想定よりも低かったです。DKIM は，メールヘッダー及びメール本文を対象にしてデジタル署名を付与します。メールヘッダーには，中継するメールサーバが追加する Received フィールドなどがありますので，これらも署名対象にすると，署名の検証に失敗するという基本的なものです。(4)の正答率は低かったです。DMARC 認証では，From ヘッダーのメールアドレスのドメインが認証の対象になっていることに気付いて欲しかったと思います。一方，(5)の正答率は比較的高かったです。問題の記述内容を基にして，適切に答案がまとめられていました。(6)の正答率は想定よりも低かったです。S/MIME では，メールアドレス単位に証明書が発行されますので，クライアントである PC が対象になるということが，十分に理解されていなかったようです。また，送信ドメイン認証に対応するためには，外部メールサーバと外部 DNS サーバとの関係も，必ずしも整理できていないように見受けられました。

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，問題選択に充てる時間として，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持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，4 月 21 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，解決の糸口を見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，粘り強く取り組むことを忘れないようにしましょう。

以上