2023 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

2023 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，48.8 点でした。問題別の平均点は，問 1 が 26.1 点，問 2 が 26.1 点，問 3 が 15.5 点，問 4 が 22.3 点という結果でした。

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（インシデント対応体制の整備）と問 2（モバイル環境のセキュリティ）の選択者が 32.4%，問 1 と問 3（Web サイトの機能追加）が 3.7%，問 1 と問 4（クラウドサービスの利用）が 51.6%，問 2 と問 3 が 2.1%，問 2 と問 4 が 5.9%，問 3 と問 4 が 4.3%という状況でした。問ごとでは，問 1 が 44.0%，問 2 が 20.2%，問 3 が 5.0%，問 4 が 30.8%でした。

10 月 8 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できるだけの知識が必要とされます。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，問題文で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，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 インシデント対応体制の整備

【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 ～ e は，解答例どおりに対し各 2 点。

［設問2］

(1) 五つの IP アドレスが全て指摘されているものに対し 5 点。その他は 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（「HTTP で Web サーバに接続，又は不正な HTTP リクエストを送信」,「開発ツール P の脆弱性 Y を悪用」,「プログラム A を起動し AC-B を作成」の三つを指摘したもの）に対し 8 点。前述の三つのうち，指摘内容が二つのものなどは 4 点。脆弱性 Z を指摘したものなどは 0 点。

（3）f，g は，解答例どおりに対し各 3 点。

（4）解答例どおり（完答）に対し 5 点。その他は 0 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）解答例どおりに対し各 2 点。

【講評】

平均点は 26.1 点と，問 2 とほぼ同じで，4 問の中では，最も高い点数でした。選択者数についても，受験者全体の 44.0%が問 1 を選択していました。

設問 1 (1)の正答率は高かったです。不正ログインに使用された送信元 IP アドレスが，ほかに存在していないことを確認することがポイントです。(2)の正答率も高かったと思います。空欄 c は，パスワードスプレーという答案が散見されましたが，パスワードスプレーは，総当たりではなく，アカウントロックを回避しながら試行

することが特徴です。いずれにしても，用語の意味を正確に覚えておくことは，解答作成の基本になりますから，日頃から一つ一つの知識を積み重ねていくことを忘れないようにしましょう。

設問 2 (1)の正答率は平均的でした。条件に合う IP アドレスを一つ一つ確認しながら，丁寧に答えていくようにしましょう。(2)の正答率は低かったです。問 1 の中では，比較的難度の高いものでしたが，時間の許す限り，インシデントの発生状況を十分に確認し，どのようなステップを踏んで，AC-B が作成されたかを考えることが必要です。(3)の空欄 f の正答率は高かった半面，空欄 g の正答率は平均的でした。(4)の正答率は比較的低かったようです。ポイントは，送信元 IP アドレスを L 社ネットワークと M 社ネットワークに限定することと，サービスは HTTP，HTTPS，SSH の三つを許可することが必要です。

設問 3 (1)の正答率は比較的低かったようです。設問では，「脆弱性への対応を見送った判断の中で問題とされる事項」を問いましたが，「複数の脆弱性を悪用されることが考慮されていなかった」など，判断が適切でないことを指摘した答案が散見されました。(2)の正答率は比較的高かったですが，「パスワード」，「電話番号」，「認証コード」などの答案も散見されました。(2)は，認証の 3 要素のうち，どの要素とどの要素が該当するかを答えるものです。

問2 モバイル環境のセキュリティ

【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 4 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。

（3）c は，解答例どおりに対し 2 点。

［設問2］

（1）d，e は，解答例どおりに対し各 3 点。

（2）f，g 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 6 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。

［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）解答例どおりに対し各 3 点。その他は 0 点。

【講評】

平均点は 26.1 点であり，問 1 と同様に高い点数でした。選択者数の比率は，セキュリティプロトコルを中心にした問題でしたから，20.2%にとどまりました。

設問 1 (1)の正答率は，高かったです。プロキシサーバにおける URL フィルタリングの機能については，十分に理解されています。(2)の空欄 a の正答率は，空欄 b に比較すると，かなり低かったです。空欄 a を含む記述全体から，適切な字句を解答群の中から選ぶのではなく，FW に関連する字句として WAF が選ばれたような印象を受けました。(3)の正答率は，低かったです。

設問 2 (1)の空欄 d の正答率は低く，「プロキシサーバ」，「サブネットマスク」などの答案が散見されました。空欄 e の正答率は，比較的高かったと思います。(2)の空欄 g の正答率は，空欄 f に比較すると，低かったようです。インターネットなどのオープンな通信路を使って，通信する 2 者間で，暗号化するための共通鍵や，メッセージ認証を行う認証鍵などを作成する鍵交換方式は，セキュリティ上の重要な知識の一つですから，よく理解するようにしましょう。(3)は，鍵交換に必要とされる PFS とは何かを問いましたが，正答率は，必ずしも高いものではありませんでした。改めて，どのような役割をもつものか，PFS の性質をもつ鍵交換方式には，どのようなものがあるか，TLS 1.3 で使用される鍵交換方式は，どのような仕様が必要になるかなどを，整理しておきましょう。(4)は，まずまずの正答率でした。IPsec は，レイヤー3 のプロトコルですから，TCP/UDP のヘッダー情報をもたないので，NAPT 変換を行うことができません。また，IPsec は，TCP/UDP 全体を暗号化しますので，ポート番号を読み取ることができません。このため，「TCP/UDP のポート番号が暗号化されており，NAPT できない」旨の答案も正解です。(5)の正答率は，低かったです。L2TP over IPsec では，L2TP で通信するために，トンネル用の IP ヘッダーが付加されます。このため，IPsec でもトンネル用の IP ヘッダーを付加する必要がないので，トランスポートモードを使用すればよいということです。

設問 3 (1)の正答率は低かったです。モバイル端末から VPN-GW 経由して内部セグメントにあるホストに通信を行う場合には，FW には，モバイル端末から VPN-GW への通信ログが残されます。しかし，VPN-GW でソース NAT を行わない場合には，送信元 IP アドレスは，モバイル端末のままです。そして，内部セグメントのホストから応答パケットを返す場合には，宛先 IP アドレスにはモバイル端末の IP アドレス，送信元 IP アドレスは内部セグメントのホストです。この応答パケットを受信した FW は，モバイル端末→内部セグメントのホ

ストへの通信を許可していないので，FW はそれを拒否するということです。(2)の正答率は比較的高かったと思います。

問3 Web サイトの機能追加

【採点基準】

［設問1］

（1）解答例どおりに対し 3 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。その他は，基本的に 0 点。

［設問2］

（1）b ～ d は，解答例どおりに対し各 1 点。

（2）e ～ g（完答）は，解答例どおりに対し 3 点。

（3）h は，解答例どおりに対し 3 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3］

（1）i は，解答例どおりに対し 2 点。

（2）Web アプリの見直し内容，DB サーバの設定とも，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）解答例どおりに対し各 2 点。ただし，三つ以上，解答した場合には，一つにつき 2 点減点。

（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。

【講評】

平均点は 15.5 点で，午後 I の中では，最も低い点数でした。選択者数も 5.0%で，4 問の中では，最も少ない比率になりました。

設問 1 (1)の正答率は，低かったです。問題文では「ブラウザ上のクリックなどの操作の有無にかかわらず」と記述されていますが，クリックによって動作するものを答えたものも見られました。(2)の正答率は平均的でしたが，(3)の正答率は，少し低かったように思います。

設問 2 (1) の正答率は，平均的でした。Same-Origin になる条件については，再度，確認しておくとよいでしょう。(2)の正答率は，比較的高かったです。(3)の正答率は，想定よりも低かったです。図 2（CORS によるサイト間の情報連携のメッセージングの例（抜粋））を基にして，スクリプト X を送信するのは，サイト T かサイト S のどちらであるかを見極め，プリフライトリクエストの Origin ヘッダーには，スクリプト X を送信する方のオリジンを設定します。このようにして，サイト T の URL か，サイト S の URL になるかを決めるようにするとよいでしょう。(4)の正答率は，条件整理などが複雑でしたから，低かったと思います。(5)の正答率も，少し低かったようです。CORS の設定不備としては，リクエストの Origin ヘッダーに正規のサイトのオリジンと異なるものが設定されている場合には，そのオリジンを受け付けないようにする実装が求められます。

設問 3 (1)の正答率は，高かったです。(2)の Web アプリの見直しの方の正答率は，まずまずでしたが，DB サーバの設定の方の正答率は，表 1 の注 1) にある「Web サーバは，専用のファイル転送プロトコルを用いて DB サーバにアクセスする」という条件を見落としているように感じられ，低かったです。

設問 4 (1)の正答率は，まずまずでした。(2)は，FW で PF 診断のためのパケットの通過を禁止している場合には，脆弱性の検査を行うことはできないということに気付かなかったようで，正答率は低かったです。

問4 クラウドサービスの利用

【採点基準】

［設問1］

（1）a ～ c（完答）は，解答例どおりに対し 3 点。

（2）d，e 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 6 点。その他は，基本的に 0 点。

［設問2］

（1）解答例どおりに対し 2 点。その他は 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）f ～ h（完答）は，解答例どおりに対し 3 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3］

（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。指摘内容が今一歩のものは 3 点。その他は 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。

［設問4］

（1）i ～ k（完答）は，解答例どおりに対し 3 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 4 点。その他は，基本的に 0 点。

【講評】

平均点は 22.3 点でした。平均点として評価すると，ほぼ妥当な結果であると思われます。選択者数は 30.8%であり，問 1 に次いで多い比率になりました。

設問 1 (1)の正答率は，高かったです。(2)の空欄 d の正答率は高かった半面，空欄 e の正答率は低かったです。PATCH ではなく，UPDATE を選択した受験者が多く見られました。(3)の正答率はまずまずでしたが，ID 情報に関するセキュリティ問題としては，不要になった ID をいつまでも残しておくと，それを不正アクセスに利用されることが挙げられます。この点については，よく理解しておきましょう。

設問 2 (1)，(2)の正答率は，まずまずでしたが，(3)の正答率は，比較的低かったです。(3)は，図 4（OIDC の認可コードフローを用いるメッセージングの例）のフローと，問題文の説明とが，整合するように字句を当てはめていくことがポイントです。本試験では，なんとなく考えるのではなく，問題文の記述と合致する字句を選ぶことが重要ですから，実践してみてください。(4)の正答率は，低かったようです。nonce は，一度しか使用されない値（乱数）ですから，同じ値を使うリプレイアタックの対策として効果があるのです。

設問 3 (1)の正答率は平均的でしたが，(2)の正答率は低かったです。(2)で問われていることは，「表 2 中の項番 1, 項番 2 及び項番 5 の三つの機能を組み合わせると，シャドーIT 以外のどのような SaaS に対するどのような操作を検出できるか」です。シャドーIT 以外ですから，許可された SaaS に対して，どのような操作が該当するかを考えることが必要です。(3)の正答率は，想定よりも少し高いものになったと思われます。

設問 4 (1)の正答率は，高かったと思います。(2)の正答率も，想定していたものよりは高かったです。暗号鍵だけを抹消すれば，上書き処理よりも高速化できることに着眼することができていました。(3)の正答率は，比較的高かったです。

今回の本試験から，出題構成が変更になり，これまでの午後Ⅰ，午後Ⅱという二つの試験は，一つの午後試験として行われることになりました。また，試験時間は，2 時間 30 分になり，1 問当たり 75 分を割り当てることができるので，時間的な余裕ができると思います。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，1 問は容易に選択対象外にできますから，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が豊富であるかどうかによって決まってきます。このため，10 月 8 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，問題と向き合ってみると，これまでやってきたこととは違う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，解決の糸口が見つかるはずです。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