2022 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

2022 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Ⅰ，午後Ⅱ試験の平均点は，午後Ⅰが 48.0 点，午後Ⅱが 41.8 点でした。2022 年春期の公開模試は，午後Ⅰの平均点が 38.9 点，午後Ⅱの平均点が 34.7 点でしたから，平均点だけで評価すると，かなり向上したといえます。問題別の平均点は，午後Ⅰの問 1 が 17.6 点，問 2 が 27.6 点，問 3 が 25.1 点でした。午後Ⅱは，問 1 が 39.2 点，問 2 が 45.8 点で，問 2 の方が高いという結果になりました。

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，記述式の問題においては，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解答を作成するとよいでしょう。

次に，問題ごとの選択状況を紹介しておきます。午後Ⅰ試験は，3 問のうち 2 問を選択します。問 1（ファイルのダウンロードの見直し）と問 2（IoT 機器のセキュリティ）の選択者が 39.7%，問 1 と問 3（ネットワークのセキュリティ対策）が 16.8%，問 2 と問 3 が 43.5%という状況でした。問ごとでは，問 1 が 28.3%，問 2 が 41.8%，問 3 が 29.9%でした。10 月 9 日に実施予定の本試験において，3 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Ⅰ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Ⅱ試験は，問 1（マルウェア対策の点検と見直し）の選択者が 60.4%，問 2（クラウドサービスのセキュリティ）が 39.6%でした。午後Ⅱ試験は，様々なセキュリティ分野の知識が問われる総合問題として出題されることが多いので，午後Ⅰ試験と同様に，できるだけ各自が得意とする分野から構成されている問題を選択するとよいでしょう。また，IPA では「試験結果に問題の難易差が認められた場合には，基準点の変更を行うことがあります」としています。このため，午後Ⅱ試験においては，問 1 と問 2 の難易差をあまり気にせず，一度選択すると決めた問題を最後までやり遂げることが大切です。問題選択に迷うと，2 問とも手をつけ，かえって失敗することになってしまいます。

午後Ⅰ，午後Ⅱ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，本試験では，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。

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，午後Ⅱ試験の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。

＜午後Ⅰ＞

問1 ファイルのダウンロードの見直し

【採点基準】

[設問1]

（1）a 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 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）b は，解答例どおりに対し 3 点。

[設問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）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）c 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 6 点。その他は，基本的に 0 点。

（3）d は，解答例どおりに対し 2 点。

（4）e，f は，解答例と同様の意味をもつ字句に対し各 3 点。例えば，e は MAC 鍵，f は時刻，時間情報なども 3 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。

【講評】

平均点は 17.6 点（平均正答率は 35.2%）でした。全体的に正答率が低く，午後 I の 3 問の中では最も低い点数でした。

設問 1 の正答率は，全体として平均的でしたが，(3)は，低かったと思います。CSRF 脆弱性は，偽装された HTTP リクエストを，Web サイトが正規のリクエストとして処理してしまう脆弱性です。その対策として Web サイトでは，Web アプリが送信した秘密の情報を検証しますが，この検証によって何が確認できるかを問うものです。攻撃者は，正規の利用者のブラウザを経由して HTTP リクエストを送信するので，これが偽装されたリクエストであるかどうかを判別する必要があります。こうした考え方を把握しておけば解答を導きやすいと思います。日頃から，基本的な知識を常にインプットし，レベルアップしておくことがよいでしょう。

設問 2 も，正答率が低かったようです。この設問は，ダウンロード用の URL が推測困難な場合という条件が示されていますから，URL のパス名を手あたり次第，試す方法を答えればよいのです。設問で何が問われているかを，十分に確認するようにしましょう。

設問 3 のうち，(2)～(4)の正答率は平均的でしたが，(1)と(5)の正答率は，低かったと思います。(1)は，図 2 で説明されている署名付き URL とは何かを十分に理解することが必要です。試験では，新しい技術に関する問題も出題されますので，問題で記述された内容を理解できるだけの知識を身に付けておくことが必要です。(5)は，cookie に関する問題です。cookie のやり取りには Set-Cookie と Cookie ヘッダが使用されるほか，その属性には Secure，HttpOnly，Domain，Path，Expires などがあります。ブラウザから cookie を送信するための条件を，それぞれの属性によって指定します。これらの知識については，一朝一夕で身に付けることはできません。地道に一つ一つの知識を積み重ねていく努力も忘れないようにしましょう。

問2 IoT 機器のセキュリティ

【採点基準】

［設問1］

（1）a は，解答例どおりに対し 2 点。
（2）解答例どおりに対し 3 点
（3）b 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。

［設問2］

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

［設問3］

（1）f 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 6 点。その他は，基本的に 0 点。
（3）g は，解答例どおりに対し 3 点。作成方法は，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。

【講評】

平均点は 27.6 点（平均正答率は 55.20%）でした。全体的に正答率が高く，午後 I の 3 問の中では，最も高い点数になりました。

設問 1 は，(1)～(3)の正答率が高かった半面，(4)の正答率は，やや低かったと思います。(4)は，ヘルスケア機器は，ヘルスケアサーバとの TLS セッション確立時にサーバ認証を行うと，表 1 中に記載されています。問題を丁寧に読んで，条件を確認した上で，解答を導いていくことが原則です。試験で解答の作成に困った際には，必ず設問で問われていることを確認し，関連する問題の記述内容を見直すという手順を踏むようにしましょう。

設問 2 は，全体的に正答率が高かったです。特に(2)の CRYPTREC，耐タンパは，それほど正答率は高くならないだろうと考えていましたが，正確に解答されていました。

設問 3 (1)，(2)の正答率が高かった半面，(3)の正答率は低かったです。例えば，空欄 g に入れる字句は，署名などの解答が見られました。署名については，基本的に何の（誰の）署名かを明確にすることが必要です。空欄 g は，アップデート版の専用 OS を配布する手順に関することなので，専用 OS を配布する開発元の真正性とコードが改ざんされていないことを保証するため，専用 OS に対するコード署名を付加することが必要です。答案の中には，コード署名証明書という解答が散見されましたが，コード署名証明書は，コード署名証明書に対応する秘密鍵が漏えいするなど，危殆化しない限りは，再発行することはありません。こうした基本的な事項については，しっかり押さえていくことが必要です。

問3 ネットワークのセキュリティ対策

【採点基準】

[設問1]

(1) a，b は，解答例どおりに対し各 2 点。

(2) 項番 7，項番 8 のルールは，解答例どおりに対し各 3 点（項番 7，項番 8 は順不同）。

(3) c，d（完答），e，f，g（完答）は，解答例どおりに対し各 3 点。

(4) h は，解答例どおりに対し 3 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) i，j は，解答例どおりに対し各 2 点。

(7) 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 4 点。その他は，基本的に 0 点。

(2) k，l は，解答例どおりに対し各 2 点。

(3) 項番 9 のルールは，解答例どおりに対し 3 点。

【講評】

平均点は 25.1 点（平均正答率は 50.2%）で，午後 I の中では，問 2 の次に高い点数でした。この結果，問 2 と問 3 の選択者に対する午後 I 試験の評価は，高めの評価になるはずです。

設問 1 は，(1)，(3)，(4)，(6)の正答率は，高かったと思います。一方，(2)の FW のフィルタリングルールについては，表 2 の注記 2 で「FW は，ステートフルインスペクション型である」と記述されているにもかかわらず，行きのパケットに対する，帰りのパケットを通過させるルールを答えた答案が散見されました。FW のステートフルインスペクションは，行きのパケットを通過させるルールを設定すれば，帰りのパケットについては，整合性のあるものを通過させるルールを動的に作り出すようにします。このため，帰りのパケットを通過させるルールを静的に設定することは，基本的にありません。(5)は，難度の高い設問でしたから，必ずしも正解できなくてもよい問題です。設問によっては，高度の技術知識を要求されることがありますから，このような設問には時間を浪費しないことが得策です。(5)は，DoT や DoH が適用される範囲は，どの装置とどの装置の間になるかを，よく理解しておくとよいでしょう。

設問 2 (1)の正答率は高かったですが，(2)，(3)は，やや低いように感じました。(2)の DNS のゾーンファイルで指定される値については，それぞれの決まりがありますので，正確に理解するようにしましょう。(3)は，プライマリ DNS サーバとセカンダリ DNS サーバの関係がよく理解されていないような印象を受けました。

＜午後Ⅱ＞

問1 マルウェア対策の点検と見直し

【採点基準】

[設問1]

(1) a 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 8 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 8 点。その他は，基本的に 0 点。

(4) b は，解答例どおりに対し 3 点。

(5) c は，解答例と同様の趣旨（パッチが未適用）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。

(6) d は，解答例どおりに対し 3 点。e 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。

(7) 理由は，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 6 点。その他は，基本的に 0 点。対処方法は，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。

[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) f は，解答例どおりに対し 3 点。

(3) 解答例（完答）どおりに対し 6 点。

(4) 解答例（完答）どおりに対し 5 点。

(5) g，h は，解答例どおりに対し各 3 点。

(6) i は，解答例どおりに対し 3 点。

[設問3]

j ～ m は，解答例どおりに対し各 3 点。

[設問4]

(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 8 点。指摘内容が今一歩のものは 4 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 8 点。その他は，基本的に 0 点。

【講評】

問 1 の選択者数は，全体の 6 割を占め，平均点は 48.0 点と，問 2 よりも約 6 点高いという結果でした。

設問 1 は，全体的に正答率が低かったようです。(2)では，P 社の外部メールサーバで SPF の検証を行った際に，検証に成功するのは，どのような場合かが問われています。このため，マルウェアに侵入された組織から P 社にメールを送信するという条件で考えることが必

要です。SPF 検証の仕組みを答えた答案も見られましたが，問題の設定を十分に把握した上で，解答を作成するようにしましょう。(3)は，メールによる感染拡大を防止するためには，内部メールサーバでスキャンを行うことが一つのポイントです。(5)は，パッチが提供されているという条件ですが，この条件が考慮されていなかったように思われます。(7)は，図 4 の 1 点目にある「VPN-GW にログインしなくても（中略）任意のファイルが読み出される可能性がある」に着目してほしかったと思います。図 4 の 2 点目に着目した答案も見られましたが，こちらは VPN-GW に接続した端末が対象になっています。

設問 2 も，全体的に正答率は低かったようです。(1)は，「アクセス可能なサーバが増えて被害が拡大する」ことによるリスクを問うていますが，他の部にも感染が拡大する旨の答案が散見されました。設問で問われていることを十分に確認した上で解答を作成するようにしましょう。(3)～(5)は，条件を整理した上で丁寧に考えていくことが必要です。

設問 3 の正答率は，やや低かったと思います。字句として，private key（公開鍵暗号方式で用いる秘密鍵），secret key（共通鍵暗号式で用いる秘密鍵）を用いたためと思いますが，この際，整理しておきましょう。

設問 4 は，(1)，(2)とも，正答率はやや低かったと思います。(1)は，「優先順位の高い事象を絞り込んで件数を少なくする」など，具体的な内容を指摘していない答案が散見されましたが，設問の指示を考慮して答案を作成することを心掛けるようにしましょう。

問2 クラウドサービスのセキュリティ

【採点基準】

［設問1］

（1）a，b は，解答例どおりに対し各 3 点。
（2）c は，解答例どおりに対し 3 点。
（3）d は，解答例どおりに対し 3 点。

［設問2］

（1）e，f は，解答例どおりに対し各 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 6 点。その他は，基本的に 0 点。
（3）g ～ i は，解答例どおりに対し各 4 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。許可する SaaS をホワイトリストに登録する旨を指摘したものは 3 点。その他は 0 点。
（2）k（完答）は，解答例どおりに対し 3 点。理由は，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 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）l は，解答例どおりに対し 3 点

［設問4］

（1）m，n は，解答例どおりに対し各 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 6 点。その他は，基本的に 0 点。
（3）o は，解答例どおりに対し 4 点。ログだけを指摘したものは 2 点。その他は 0 点。

［設問5］

（1）p ～ t は，解答例どおりに対し各 2 点。
（2）u ～ w 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 8 点。その他は，基本的に 0 点。

【講評】

平均点は 41.8 点で，問 1 よりも約 6 点低い点数になりました。

設問 1 は，全体的に正答率が高かったようです。

設問 2 (1)の正答率は高かったです。(2)は，ブラウザが行う接続先に関する整合性の基本的な問題ですから，ある程度の正答率を期待していましたが，必ずしもそうではありませんでした。FQDN，サブジェクトの CN とは何か，サーバ証明書の検証方法などを十分に整理しておきましょう。(3)の正答率は平均的でしたが，空欄 h に入れる署名については，サーバの署名なのか，CA の署名なのかなどを，区別することが必要です。

設問 3 (1)は，禁止する SaaS の URL フィルタリングを問うていますので，ブラックリストを用いることが必要です。許可する SaaS をホワイトリストに登録する答案も散見されましたが，ホワイトリストを用いると，登録されたもの以外は，全てアクセスできなくなりますので，注意が必要です。(2)，(4)は，条件を整理しながら考える必要がある問題でしたから，正答率はやや低かったようですが，(3)の正答率は，やや高かったです。

設問 4 の正答率は，全体的に平均的でした。

設問 5 (1)の正答率は，高かったと思います。(2)の正答率はやや低めでした。(3)は，アクセス権限を委譲する仕組みの問題で，顧客の属性情報については，顧客がリソースのオーナですから，顧客がサイト X に対して顧客の属性情報を取得する権限を与えることが必要になります。こうした基本的な事項を一つ一つ積み上げ，知識をできるだけ多く蓄積していくようにしましょう。

最後に，本試験では問題を丁寧に読んで，設問で問われていることを十分に確認し，問われていることに対して的確に答えていくとよいでしょう。

以上