2022 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

2022 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Ⅰ，午後Ⅱ試験の平均点は，午後Ⅰが 38.9 点，午後Ⅱが 34.7 点でした。2021 年秋期の公開模試は，午後Ⅰの平均点が 40.3 点，午後Ⅱの平均点が 38.7 点でしたから，平均点だけで評価すると，前回から少し落ち込みました。問題別の平均点は，午後Ⅰの問 1 が 17.6 点，問 2 が 22.5 点，問 3 が 16.8 点でした。午後Ⅱは，問 1 が 31.6 点，問 2 が 40.8 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，こうした解答が数多く見られました。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（電子メールのセキュリティ対策）と問 2（Web サイトのセキュリティ診断）の選択者が 54.6%，問 1 と問 3（クラウド環境のセキュリティ対策）が 16.6%，問 2 と問 3 が 28.8%という状況でした。問ごとでは，問 1 が 36.0%，問 2 が 41.5%，問 3 が 22.5%でした。4 月 17 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（情報セキュリティ対策の強化）の選択者が 66.1%，問 2（クラウドサービスを活用したテレワーク環境）が 33.9%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 電子メールのセキュリティ対策

【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) b，c は，解答例どおりに対し各 3 点。

[設問2]

(1) d 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。

(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) f，g は，解答例どおりに対し各 2 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。

(7) SPF，DKIM とも，解答例どおりに対し各 3 点。

(8) h，i は，解答例どおりに対し各 2 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，問 3 とともに低い点数でした。

設問 1 (1)の DNSBL については，よく理解されていました。(2)は，S/MIME 証明書は，サーバ証明書などと同様，PKI を構成する要素の一つですから，認証局に CSR（証明書署名要求）を行い，発行してもらうことが基本です。(3)は，少し難しかったようで，正答率は高くはありませんでした。

設問 2 (2)の正答率は低かったです。送信ドメイン認証に限らず，認証の考え方は，二つの認証対象を比較し，それらが一致するかどうかによって判断します。SPF の認証対象の一つは，送信側のドメインに登録された SPF レコードから得られる IP アドレス，もう一つは，送信メールサーバの IP アドレスです。この設問は，送信メールサーバの IP アドレスが詐称されたものではなく，正しいといえる理由を述べるものです。例えば，送信メールサーバの IP アドレスを詐称することができれば，簡単に SPF 認証を破ることができます。TCP/IP 通信の基本に立ち返って考えれば，正解できるはずです。このため，送信メールサーバは，自身の IP アドレスを必ず用いる必要があるので，攻撃者が SPF 認証を突破するために考えることは，DNS キャッシュポイズニングによって，DNS サーバに登録された SPF レコードを書き換えることです。

設問 2 (4)～(6)は，DKIM 署名の検証に失敗する事例に関するものです。一つ目は，メーリングリストサーバにおける処理によって，サブジェクトやメール本文が修正される例です。二つ目は，メールサーバを経由するごとに，メールヘッダが追加されたり，変更されたりする例です。(7)は，SPF，DKIM を有効に機能させるために，対応が必要になるサーバを答える問題でしたが，メールの受信側（この問題では取引先）の DNS サーバを答えたものが散見されました。受信側では，受信メールのドメインに対して SPF レコード，DKIM レコードを問い合わせますから，取引先の DNS サーバを含め解答したと考えられます。しかし，ドメイン名の名前解決については，既にメールサーバ側で行われる通常の処理です。こうした点に注意して考えることが必要です。

問2 Web サイトのセキュリティ診断

【採点基準】

［設問1］

a，b は，解答例どおりに対し各 3 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) 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) 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) d 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。

(3) 解答例と同様の趣旨（送信元が診断用 PC，宛先ポートが全て）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) 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 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。

【講評】

平均点は 22.5 点（平均正答率は 45.0%）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 の a の正答率は高かった半面，b の正答率は低かったと思います。b は，HTTP ヘッダインジェクションなどの解答が散見されました。

設問 2 (1)の正答率は，平均的でした。(2)，(3)は，ともに問題文の記述を基にして，解答を作成するものでしたから，正答率は比較的高かったと思います。しかし，問題の記述内容のどこに着目するかによって，正解できるかどうかの分かれ目になります。例えば，(2)は，図 1 の注記 2 に「検証環境は，本番環境と同一の Web アプリと，同一機種の FW，NIDS，リバースプロキシ，Web サーバ及び DB サーバで構成されている」と記述されているので，「本番環境と同一の Web アプリ」か，「本番環境と同一の機種構成」かのどちらに着目するかがポイントです。c に入れる字句としては，リリース済みの Web 診断に関することなので，前者を答える必要があると判断できます。このように，c に入れる字句だけに着目して考えるのではなく，問題の流れを考慮した上で，どちらが適切かを判断するとよいでしょう。

設問 3 (1)の正答率は平均的でしたが，(2)の正答率は，想定よりも低かったです。例えば，「サーバソフトのバージョンを最新のものにする」などの答案が散見されました。脆弱性は，サーバソフトのバージョンを出力することです。この点を答えることが必要です。(3)は，問題の条件を的確に考慮する必要がある設問でしたから，正答率は低かったです。このため，何がポイントになるか

を見極めるように，問題文の読み方などを工夫していくことも必要です。本試験に向けて，こうした点を改善していきましょう。(4)の正答率は高い半面，(5)の正答率は比較的低かったです。

問3　クラウド環境のセキュリティ対策

【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，c は，解答例どおりに対し各 2 点。

（2）d は，解答例どおりに対し 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。

（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各 4 点。その他は，基本的に 0 点。

［設問3］

（1）f，g 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 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。

【講評】

平均点は 16.8 点（平均正答率は 33.7%）でした。午後 I の中では，選択者数も少なく，点数的にも最も低い点数でした。

設問 1 (1)の正答率は，平均的でしたが，(2)の正答率は比較的低かったと思います。問題の条件が，十分に読み取られていないように感じられました。

設問 2 の正答率は，全体として低かったです。(1)～(3)の正答率は，平均的でした。(4)の CONNECT メソッドを使用した際に，PC からプロキシサーバに対して送られる情報については，十分に理解されていないように見受けられました。(5)も，プロキシサーバで TLS 通信を終端するケースにおいて，ブラウザがサーバ証明書を検証する際に必要となる知識の一つです。証明書の検証に関する知識は必須ですから，十分に理解しておくことが必要です。(6)の正答率も，低かったと思います。例えば，PC のデフォルトゲートウェイを SD-WAN に変更する答案も散見されました。PC のデフォルトゲートウェイは，図 1 から本社の PC は L3SW，営業所の PC は WAN ルータ（図 2 では SD-WAN）ですから，何も変更する必要はありません。

設問 3 の正答率は，全体的に低かったと思います。特に，(2)の業務サーバからインターネット内にある ZTNA の方向にセッションを張る必要性については，内部ネットワークのセキュリティを維持することにほかなりません。それは，外部からの通信をできるだけ許可しないことが基本だからです。

＜午後Ⅱ＞

問1　情報セキュリティ対策の強化

【採点基準】

［設問1］

a，b は，解答例どおりに対し各 3 点。

［設問2］

（1）c は，解答例どおりに対し 3 点。

（2）影響，特徴とも，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 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）解答例どおりに対し 4 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）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）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 6 点。その他は，基本的に 0 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 6 点。その他は，基本的に 0 点。

（2）d 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）理由，内容とも，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 6 点。その他は，基本的に 0 点。

（4）e は，解答例どおりに対し 3 点。

【講評】

問 1 の選択者数は，問 2 の約 2 倍でしたが，平均点は

31.6 点と，問 2 よりも約 9 点低い結果になりました。

設問 1 の正答率は，平均的でした。

設問 2 (1)の正答率は，比較的高かったです。(2)の影響を答える設問は，比較的高い正答率でしたが，利用者登録処理の特徴の方の正答率は，低かったです。設問では，表 1 における利用者登録処理の特徴を読み取ることが必要でしたが，ログイン処理の特徴を述べた答案が散見されました。設問で問われていることを丁寧に読み取って，それに対応しているものを答えることがポイントです。(4)～(6)の正答率は，低かったです。特に(6)は，署名の検証に関するもので，署名は送信者の真正性とメッセージの完全性を保証する効果があります。このため，メッセージの改ざんなどの答案が散見されました。しかし，この設問では，具体的に述べよと指示されていますので，どのような内容のメッセージが該当するかを答えることがポイントです。

設問 3 は，全体的に正答率が，低かったと思います。特に，(2)は，プロキシサーバを経由して C&C サーバと通信する際には，プロキシサーバが C&C サーバの名前解決を行うことが必要ですから，最初にキャッシュ DNS サーバに対して DNS クエリを送ります。こうした基本的な知識に基づいて考えていくことが，様々な事項に対する理解を深めていくことにつながります。(3), (4)は，マルウェアの動作に関するものですから，問題に記述されたマルウェアの動作を確認しながら，丁寧に解答を作成することが求められます。

設問 4 (1)，(2)の正答率は，平均的でしたが，(3)の理由を述べる設問は，正答率が低かったです。L2SW を越えて通信する際には，送信元 MAC アドレスは L2SW のものになります。こうした基本的な知識は，一つ一つ積み重ねていくしか方法がありません。

問2 クラウドサービスを活用したテレワーク環境

【採点基準】

［設問1］

(1) a，b 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 8 点。その他は，基本的に 0 点。

(3) VD，T-PC 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 6 点。その他は，基本的に 0 点。

［設問2］

(1) c ～ e 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) 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。「行方不明の T-PC に対しリモートワイプによってデータを消去する」旨を指摘したものは 3 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 7 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 8 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4］

(1) h，i は，解答例どおりに対し各 3 点。

(2) 収集方法の変更内容，必要となる作業手順とも，解答例どおりに対し各 6 点。その他は，基本的に 0 点。

【講評】

平均点は 40.8 点で，問 1 よりも取り組みやすい問題だったと思われます。

設問 1 (1)，(2)の正答率は，比較的良かったと思います。(3)は，下線②の前にある“図 2 の事例 2”に着目すれば，正解を導けると考えていましたが，下線②だけに着目し，一般論から考えられる答案を作成されたような印象を受けました。個別のことだけに着目するのではなく，全体の記述内容を把握しながら何を解答すべきかを，適切に見極めるようにすることが大切です。

設問 2 の正答率は，全体的にまずまずでした。

設問 3 (1)は，リダイレクトの基本的な問題でしたから，正答率は高くなると考えていましたが，そうではありませんでした。(2)の正答率は低かったです。署名の検証は，誰の公開鍵を用いるかがポイントです。図 4 の中でトークンの検証を行うのは SaaS ですから，誰が署名を行ったかを見極めれば，正解できるはずです。ポイントになるところを，押さえながら解答を考えるとよいでしょう。(3)，(4)の正答率は，想定よりも低かったと考えています。(5)の正答率は，高かったと思います。

設問 4 (1)，(2)の正答率は，比較的良かったと思います。

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的確に応えていくようにしましょう。

以上