2021 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

2021 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 40.3 点，午後Ⅱが 38.7 点でした。2021 年春期の公開模試は，午後Ⅰの平均点が 42.0 点，午後Ⅱの平均点が 36.9 点でしたから，平均点だけで評価すると，前回とほぼ同程度といえます。問題別の平均点は，午後Ⅰの問 1 が 20.6 点，問 2 が 21.6 点，問 3 が 15.7 点でした。午後Ⅱは，問 1 が 34.9 点，問 2 が 41.6 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（標的型攻撃への対応）と問 2（セキュリティインシデント対応）の選択者が 64.4%，問 1 と問 3（データアクセスの見直し）が 18.0%，問 2 と問 3 が 17.6%という状況でした。問ごとでは，問 1 が 41.3%，問 2 が 40.8%，問 3 が 17.9%でした。10 月 10 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（Web サイトのセキュリティ）の選択者が 42.6%，問 2（サービスの運用と利用におけるセキュリティ）が 57.4%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 標的型攻撃への対応

【採点基準】

[設問1]

（1）a，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。指摘内容が今一歩のものは 3 点。その他は 0 点。

（3）b～e は，解答例どおりに対し各 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 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2]

（1）解答例と同様の趣旨（マルウェア A のハッシュ値で検索）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。

【講評】

平均点は 20.6 点（平均正答率は 41.2%）であり、午後 I の中では，問 2 に次いで高い点数でした。

設問 1 (1)の a の正答率は，f，g に比べて低かったと思います。(2)の VDI（仮想デスクトップ環境）では，ユーザが利用する PC の実体は，VDI サーバ上に存在します。つまり，VDI サーバには複数の仮想デスクトップが存在するので，例えば「VDI サーバの LAN ケーブルを抜く」といった方法では，全ての仮想デスクトップが使用できなくなります。また，それは利用者が行う対処でもありません。そこで，この設問では，利用者側で感染の疑いのある仮想デスクトップだけを隔離する対処を述べたものだけを正解にしています。

設問 1 (3)の送信ドメイン認証に関する用語は，よく理解されていました。一方，d の SMTP のコマンドを答えるものは，少し正答率が低かったです。午後問題では，単なる用語ではなく，SPF や DKIM などの仕組みなどを問う問題が増えてきます。技術の仕組みなどの詳細な知識を含め，十分に学習しておくとよいでしょう。(4)，(5)，(6)の記述式の問題は，(5)を除き，まずまずの正答率だったと思います。

設問 2 (1)，(2)は，問題の条件を的確に整理する必要のある設問でしたから，正答率は低かったです。例えば，(1)は，マルウェア A に感染した PC を特定する方法を問うています。問題の条件を整理すると，マルウェア A（ファイル）のハッシュ値が管理サーバに登録されると，ファイルの読み書き時などにおいてマルウェア A を検知できることが分かります。このため，マルウェア A のハッシュ値が登録される以前は，ファイルの読み書きが行われても，管理サーバではマルウェア A を検知できません。そこで，マルウェア A に感染した PC を特定するには，管理サーバの C ログを検索することが必要になります。このように，マルウェアに関連する問題に取り組む際には，問題の記述内容を丁寧に整理していくことが大切です。このようなことを念頭に置き，解答を作成するように心掛けてください。

問2　セキュリティインシデント対応

【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（ホスト名の部分に格納する）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 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。指摘内容が今一歩のものは 3 点。その他は 0 点。

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

（2）c は，解答例どおりに対し 3 点。

（3）内部 DNS サーバ 1，内部 DNS サーバ 2 にもたせる機能とも，解答例どおりに対し各 3 点。

（4）（d，e）の組みと（f，g）の組みは，解答例どおりに対し各 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 21.6 点（平均正答率は 43.2%）でした。比較的、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 (1)の正答率は少し低く，(2)の正答率も低かったと思います。(2)のポイントは，C&C サーバが DNS サーバとして動作している場合，マルウェアに感染した PC が，C&C サーバに接続するためには，必ず C&C サーバのドメイン名を用いることが必要です。これが DNS における名前解決の基本的な仕組みです。こうした仕組みについては，しっかりと整理し，応用が利くようにしておくとよいでしょう。

設問 1 (3)の正答率は高く，(4)，(5)の正答率は低かったと思います。(4)のように具体的に述べよと指示されている設問（FW に記録されるログ）については，送信元，宛先，サービスは何かを明確に答えることが必要です。(5)の ISAC に伝えるべき情報については，(3)で ISAC から提供された情報として，マルウェア Q のハッシュ値を選択された方は，今度は，D 社がマルウェア R のハッシュ値を提供する必要があるということに気付いてほしかったと思います。

設問 2 (1)～(3)は，まずまずの正答率だったと思います。(3)については，スタブリゾルバ，フルサービスリゾルバ，権威 DNS サーバの役割を，もう一度整理しておくとよいでしょう。(4)，(5)の正答率は高かったと思います。特に，(4)については，フルサービスリゾルバと権威 DNS サーバの機能を把握して設定するルールを考えれば，もっと正答率は高くなると感じられました。(5)は，DMZ にある DNS サーバを，インターネット側から DNS の再帰的問合せを受けるように設定した場合に

発生するセキュリティ上の問題点については，よく理解されていました。

問3 データアクセスの見直し

【採点基準】

［設問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。

［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) a は，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) c は，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 8 点。その他は，基本的に 0 点。
(6) 解答例どおりに対し 4 点。
(7) 解答例どおりに対し 4 点。

［設問3］

(1) d は，解答例と同様の趣旨が適切に指摘されている字句に対し 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。

【講評】

平均点は 15.7 点（平均正答率は 31.4%）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 の正答率は，低かったと思います。セッション ID の固定化（セッションフィクセーション）とセッションハイジャックの違いについては，よく整理しておくとよいでしょう。

設問 2 の正答率は，全体として低かったです。(1)は，鍵ペアに関して必要な作業を問うものです。「ストレージサービスに鍵ペアを登録する」などの答案が見られました。鍵ペアは公開鍵と秘密鍵のことですから，秘密鍵を，本人以外の機器に登録することになります。このように，第三者に秘密鍵を渡すという行為は，なりすましなどに悪用されるので，セキュリティ上，絶対にやってはいけないことです。(3)～(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。中でも(5)は，SameSite 属性を設定した場合の動作を問うものです。これまでの本試験では出題されたことはありませんが，cookie 関連については，理解を深めていきましょう。(6)，(7)は，図 2 のストレージサービスへのアクセスのシーケンスを見ながら，判断することが必要です。

設問 3 (1)，(2)の正答率は，低かったと思います。

＜午後Ⅱ＞

問1 Web サイトのセキュリティ

【採点基準】

［設問1］

(1) a は，解答例どおりに対し 3 点。
(2) b，c は，解答例どおりに対し各 3 点。
(3) d は，解答例（又は，持続型，蓄積型）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 6 点。その他は，基本的に 0 点。
(6) e は，解答例どおりに対し 3 点。

［設問2］

(1) 方法，対策とも，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。
(2) f は，解答例どおりに対し 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) g，h は，解答例どおりに対し各 3 点。

［設問3］

(1) i は，解答例どおりに対し 6 点。
(2) j 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。

［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各 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。

［設問5］

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

【講評】

問 1 の平均点は 34.9 点で，問 2 よりも約 7 点低く、選択者数も問 2 よりも少ない状況でした。

設問 1 (1)～(3)の正答率は，想定していたよりも低かったです。(4)は「全ての要素ではなく，ブラウザから受信した入力パラメタを対象としたエスケープ処理では

対策として不十分な理由」を問いましたが，この意味が必ずしも理解されていないような答案が散見されました。本試験では，設問で問われていることを必ず確認するようにしましょう。(5)の正答率は，ほぼ想定どおりでしたが，(6)は，Secure という答案も散見されました。cookie に関連する事項は，正確に理解しておくことが大切です。

設問 2 (1)は，問題文の状況から SQL インジェクションではない攻撃の方法を問うものでしたが，SQL インジェクションを用いた方法を述べたものが散見されました。問題文の条件などから設問で問われていることを正しく把握することが得点のアップにつながります。(2)～(4)の正答率は，比較的高かったと思います。

設問 3 (1)，(2)の正答率は，ともに低かったと思います。一つ一つの知識を積み重ねていくことが，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。

設問 4 (1)は，問題文に記述された E 社の現状を踏まえて解答するものでしたが，動的検査と静的検査の比較を解答したものが散見されました。(2)は，問題文に記述された課題を答えるものでしたが，検査の実施内容を述べた答案が散見されました。(3)の正答率は，高かったと思います。

設問 5 (1)，(2)は，まずまずの正答率でした。

問2 サービスの運用と利用におけるセキュリティ

【採点基準】

［設問1］

a は，解答例どおりに対し 4 点。

［設問2］

(1) b～d は，解答例どおりに対し各 3 点。

(2) 理由，ルールとも，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) e は，解答例と同様の趣旨が適切に指摘されている字句に対し 4 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。

［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) f 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4］

(1) g は，解答例どおりに対し 3 点。

(2) h は，解答例どおりに対し 3 点。

(3) i～k は，解答例どおりに対し各 2 点。

［設問5］

(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) l は，解答例どおりに対し 3 点。

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

［設問6］

(1) 運用に関する効果，利用に関する効果とも，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。

(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各 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 6 点。その他は，基本的に 0 点。

【講評】

平均点は 41.6 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 の営業秘密の正答率については，比較的良かったと思います。

設問 2 (1)の正答率は，まずまずでした。(2)の理由，ルールの正答率は，それほど高くはありませんでした。特にルールについては，変更する内容に矛盾がないように記述することが必要です。(3)の e の正答率は高かった半面，理由の正答率は，低かったです。TLS を利用すれば，通信の暗号化だけではなく，通信相手を認証することもできます。

設問 3 は，全体的に正答率が低かったです。(1)は，サーバ証明書の署名は，誰が付与しているかという問題です。現在の中間 CA 証明書が廃止されると，中間 CA の秘密鍵で署名されたサーバ証明書も使えなくなります。(3)のポイントは，ハッシュ関数の危殆化などによって，異なるサーバ証明書が作り出されるリスクがあるので，こうした危険性を回避するために，サーバ証明書の有効期間を短くしようとする考え方です。

設問 4 は，少し技術的な問題でしたから，ほぼ想定どおりの正答率だったと思います。

設問 5 (1)，(2)の正答率は，比較的高かったようですが，(3)は，表 4 の公開フォルダの「検索エンジンでも検索が可能である」という条件を見落としたと考えられる答案が散見されたので，正答率は低かったです。

設問 6 (1)，(2)の正答率は，比較的高かったと思います。(3)は，URL フィルタリングが適用されることを指摘した答案は，それほど多くなかったと思います。

以上