2020 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

2020 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 38.7 点，午後Ⅱが 42.4 点でした。2019 年秋期の公開模試は，午後Ⅰの平均点が 26.9 点，午後Ⅱの平均点が 31.5 点でしたから，平均点だけで評価すると，午後Ⅰは約 12 点，午後Ⅱは約 11 点，アップしています。問題別の平均点は，午後Ⅰの問 1 が 19.2 点，問 2 が 21.8 点，問 3 が 13.9 点でした。午後Ⅱは，問 1 が 43.4 点，問 2 が 41.8 点で，問 1 の方が少し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ようにしましょう。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 問を選択しますから，問 1（セキュリティ対策の強化）と問 2（セキュリティインシデント対応）の選択者が 61.9%，問 1 と問 3（Web サイトにおけるコンテンツ公開）が 9.7%，問 2 と問 3 が 28.4%という状況でした。問ごとに見ると，問 1 が 35.8%，問 2 が 45.2%，問 3 が 19.0%でした。4 月 19 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，こうしたことを実行していくためには，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（ホテル予約サイトのセキュリティ）の選択者が 40.0%，問 2（サービスのセキュリティ）が 60.0%でした。選択者数の比率は，4 対 6 になりました。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。問題選択に迷ってしまうと，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到達していれば，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，受験者によっては問題文の記述内容をそのまま引用して解答を作成している例も多く見られます。単なる引用では正解になることは極めて少ないので，設問で問われていることを十分に確認しながら，問題の記述内容と照らし合わせて論理的に考えていくとよいでしょう。

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 セキュリティ対策の強化

【採点基準】

[設問1]

(1) a，b とも，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。

[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。その他は，基本的に 0 点。

(3) 機能の名称は，解答例どおりに対し 2 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 4 点。その他は，基本的に 0 点。

(4) c 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 4 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）e，f は，解答例どおりに対し各 2 点。
（3）問題は，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。情報は，解答例どおりに対し 2 点。

【講評】
平均点は 19.2 点（平均正答率は 38.5%）であり，午後 I の中では，問 2 に次ぐ点数でした。
設問 1 (1)の正答率は，高かった半面，(2)の正答率は想定よりも低かったと思います。587 番ポートによってメールサーバに接続した際には，SMTP-AUTH によって利用者認証が行われます。利用者認証に成功すると，メールサーバに対してメールを送信することが可能になります。(3)は，SPF 認証の基本的な仕組みを答えるものですが，ドメイン名を比較するなどといった答案が散見されました。SPF 認証に失敗する理由については，既に令和元年度秋期試験の午後 I 問 1 で出題されましたから，次回の本試験で出題されることはないと思いますが，基本的な知識は，十分に整理しておきましょう。
設問 2 (1)は，CONNECT メソッドを悪用する方法を問うものでしたが，正答率は低かったと思います。(2)は，CONNECT メソッドを悪用されないようにするために，プロキシサーバ（クラウドプロキシサービス）での対策を問いましたが，(1)と同様に正答率は低かったようです。(5)は，プロキシ認証を行う場合，マルウェアが認証情報を窃取するリスクがあることについては，よく理解されていました。
設問 3 は，全体的に正答率が低かったと思います。(3)は，送信元 IP アドレスが全て FW のグローバル IP アドレスになって，どの利用者がアクセスしてきたかが特定できないという問題です。「送信元が全て同じ IP アドレスになる」旨の答案が散見されましたが，これでは事象を指摘しただけになっています。何が問題になるかを具体的に述べ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 ～ d は，解答例どおりに対し各 2 点。
（2）解答例どおりに対し 5 点。
（3）解答例どおりに対し 5 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。単に「445/TCP ポートの通信を遮断する」旨を指摘したものは 3 点。その他は 0 点。
［設問2］
（1）解答例どおりに対し各 2 点。
（2）監視すべきトラフィックは，解答例どおりに対し 2 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）e 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 4 点。その他は，基本的に 0 点。

【講評】
平均点は 21.8 点（平均正答率は 43.6%）で，午後 I の 3 問の中では，最も高い点数でした。
設問 1 (1)は，空欄 c の正答率が低かったようです。(2)は，ランサムウェア W に感染した PC を特定するために，どの機器のログを調査すべきかを問いましたが，正答率は低かったようです。PC に割り当てた IP アドレスを調べるためには，DHCP サーバのログを確認することが必要です。(3)は，IP アドレスの有効期間（リース期間）の条件を考慮していない答案が散見されました。(4)は，表 1 にファイルサーバは「ファイル共有プロトコルは SMBv2，SMBv3 が使用されている」という条件が示されています。このため，「ファイルサーバとの通信以外の 445/TCP ポートの通信を遮断する」などのように表現することが必要です。「ファイルサーバとの通信以外」と的確に解答したものは，少数でした。
設問 2 は，全体的に正答率が低かったと思います。(1)のネットワークアドレスについては，表 1 の L3SW に「社内の各セグメントは VLAN によって 24 ビットマスクのネットワークに分割している」と記述されていますので，条件を読み取って解答することが必要です。
設問 3 (1)は，正答率が低かったようです。(1)のように，用語を答える形で出題されることがありますので，用語については，できるだけ正確に覚えておくようにしましょう。(2)，(3)は正答率が高く，このことが，平均点を押し上げることにつながったと思われます。

問3 Web サイトにおけるコンテンツ公開

【採点基準】
［設問1］
a，b は，解答例どおりに対し各 2 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，解答例どおりに対し 3 点。
（3）d は，解答例どおりに対し 2 点。

（4）理由，目的とも，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 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）f は，解答例どおりに対し 3 点。

【講評】

平均点は 13.9 点（平均正答率は 27.7%）でした。午後 I の 3 問の中では，選択者数が最も少なく，点数も，最も低いものでした。

設問 1 は，想定よりも低い正答率だったと思います。

設問 2 は，全体的に正答率が低かったようです。(1)は，鍵の使用目的を含め，鍵ペアに関して必要な設定作業が問われています。下線①の前には「署名付き URL 又は署名付き Cookie を使用するための鍵ペアは，……，コンテンツサーバ上で生成される」と記述されていますので，鍵ペアはコンテンツサーバ上で作成されることが分かります。署名を作成する際には，鍵ペアのうち，秘密鍵が使用されます。また，図 1 や図 2 を見ると，署名を作成するサーバは，Web サーバであることが分かります。このように，一つ一つのことを丁寧に結び付けていくと，解答を導くことができます。安易に解答を作成しようとするのでなく，問題の記述内容を一つ一つ確認しながら考察するという習慣を身に付けていくとよいでしょう。(4)は，Cookie の Domain 属性に関するもので，基本的な知識問題と考えていました。しかし，Cookie の盗聴や漏えいなどとの関係に着目した答案が散見され，正答率は低かったようです。Cookie の属性については，頻出問題の一つですから，しっかりと理解しておくようにしましょう。

設問 3 は，(3)を除き，正答率は低かったと思います。(2)については，署名付き Cookie を共通鍵で暗号化した場合，その共通鍵を配布する運用が難しい理由を問いました。この設問に関連することですが，通信経路上において，Cookie は HTTPS によって暗号化されるので，Cookie の安全性は確保されます。にもかかわらず，さらに Cookie を共通鍵で暗号化する必要はあるのかという疑問があるかもしれません。その理由については，解説で補足していますので，参考にしてください。

＜午後Ⅱ＞

問1 ホテル予約サイトのセキュリティ対策

【採点基準】

［設問1］
（1）a ～ 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 3 点。

［設問2］
e ～ 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 3 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 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 6 点。その他は，基本的に 0 点。

［設問5］
（1）k 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。
（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 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6］
（1）条件，目的とも，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 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 6 点。その他は，基本的に 0 点。

【講評】

問 1 の平均点は 43.4 点で，問 2 より 1.6 点高い点数でした。

設問 1 (1)は，正答率は高かった半面，(2)は用語を答える形式でしたから，正答率は低かったと思います。

設問 2 は，おおむねよくできていました。

設問 3 (2)は，入力パラメタが無害化されていない旨の答案が散見されました。これを空欄 j に当てはめると，

「入力パラメタが無害化されていないことが分かり，不正なパラメタを無効化できていない」という文章になり，表現がおかしくなってしまいます。そこで，適切な表現になるように文章を考え直すことが必要になります。

設問 4 (1)は，正答率は高かった半面，(2)は，下線②の「URL のパスを任意に書き換えるスクリプトを使用する」に着目することなく，偽の画面に誘導する方法を述べた答案が散見されました。

設問 5 は，比較的正答率が高かったと思います。しかし，(4)の HttpOnly 属性の効果を問う設問では，Secure 属性の効果を述べたような答案が散見されました。午後Ⅰ問 3 でも指摘したことですが，Cookie の属性については，正しく理解しておくようにしましょう。

設問 6 (1)，(2)の正答率は高かったです。しかし，(3)は，攻撃者が同じツールを使用し攻撃してきた場合を想定し，事前に Web アプリの脆弱性を修正し攻撃に対応できることに気付いてほしかったと思います。(4)は，要件定義や設計工程の成果物に対するレビューを実施することが大切ですから，忘れないようにしましょう。

問2 サービスのセキュリティ

【採点基準】

［設問1］

a ～ d は，解答例どおりに対し各 2 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) e，f は，解答例どおりに対し各 2 点。

(3) g 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3］

(1) h は，解答例どおりに対し 5 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 6 点。その他は，基本的に 0 点。

［設問4］

(1) サーバ証明書の検証，コモンネームの照合とも，解答例どおりに対し各 3 点。

(2) i は，解答例どおりに対し 3 点。

(3) 理由，方法とも，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) 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) j，k は，解答例どおりに対し各 3 点。

(3) l，m は，解答例どおりに対し各 2 点。

【講評】

問 2 の選択者数は，問 1 の選択者数の 1.5 倍でした。平均点は 41.8 点で，問 1 よりも 1.6 点低くなりました。

設問 1 は，空欄 c の正答率が低かったと思います。

設問 2 (1)は，送信元が FW-A の IP アドレスではなく，社内利用者 LAN5 としたものが散見されました。図 1 の注記 2 に「F 社から外部へのアクセスは，全て FW-A の NAPT 機能によって a.a.a.10 に変換される」と記述されています。条件を見極めた上で解答を作成すれば，ミスによる失点を防ぐことができます。

設問 3 は，全体的に想定していた以上に，正答率が高かったと思います。

設問 4 (1)のサーバ証明書の検証，コモンネームの照合の二つとも正解した答案は，極めて少なかったようです。サーバ証明書などの公開鍵証明書の検証方法は，頻出テーマですから，どのような形で出題されても正解できるようにしておくことが望まれます。(6)は，パスワードリスト攻撃ではなく，リバースブルートフォース攻撃を説明した答案が散見されました。基本的な攻撃手法については，用語だけではなく，その内容も理解しておくことが必要です。

設問 5 (1)の正答率は高かったと思います。しかし，(2)，(3)の正答率は低かったようです。特に(3)は，暗号鍵などの共通鍵を公開鍵暗号方式で送信する際には，通信相手の公開鍵で暗号化し，それを受け取った側は，自身の秘密鍵で復号します。また，J 社の公開鍵で暗号化し，F 社の秘密鍵で復号するといった答案も散見されましたが，公開鍵暗号方式では，同じ鍵ペアを使用します。こうした基本的なことはよく理解しておきましょう。

本番の午後試験において合格基準点をクリアするには，問題の記述内容をベースにしながら，設問で問われていることを十分に確認し，素直に解答を作成していくことが必要です。本試験に向け，セキュリティに関する知識のレベルを向上させ，解答の作成能力などに磨きをかけて，必ず合格するように努力していきましょう。

以上