2019 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

2019 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 26.9 点，午後Ⅱが 31.5 点でした。2019 年春期の公開模試は，午後Ⅰの平均点が 44.7 点，午後Ⅱの平均点が 41.9 点でしたから，平均点で評価すると，午後Ⅰは 18 点弱，午後Ⅱは 10 点強と，大きく低下しました。問題別では，午後Ⅰの問 1 が 14.5 点，問 2 が 11.5 点，問 3 が 15.3 点でした。午後Ⅱは，問 1 が 27.3 点，問 2 が 36.4 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（SSL/TLS）と問 2（無線 LAN におけるセキュリティ対策）の選択者が 53.6%，問 1 と問 3（Web アプリケーションのセキュリティ対策）が 15.8%，問 2 と問 3 が 30.6%という状況でした。問ごとに見ると，問 1 が 35.0%，問 2 が 41.9%，問 3 が 23.1%でした。10 月 20 日に実施される本試験において，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，このようなことが可能になるには，問題の記述内容を十分に把握できるだけの知識が，まず必要とされます。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 53.6%，問 2（マルウェアの感染と対策）が 46.4%でした。選択者数の比率としては，ほぼ同数といえます。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 SSL/TLS

【採点基準】

[設問1]

（1）RSA，DH とも，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。

[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，b 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3]

（1）c，d 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）注意すべき事項，必要な作業とも，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。

【講評】

平均点は 14.5 点（平均正答率は 29.0%）であり，午後 I の中では，問 3 に次ぐ点数になっています。

設問 1 (1)，(2)の正答率は，ともに低かったと思います。RSA，DH は，公開鍵暗号方式に位置付けられていますが，衝突発見困難性などハッシュ関数のもつ性質を答えたものが散見されました。また，PFS については，かなり理解されていると考えていましたが，答案を見る限り，そうではなかったようです。

設問 2 (1)は，SNI を知っているかどうかがポイントでしたから，正答率は低かったです。URL の FQDN とサーバ証明書のコモンネームが一致しないなどの答案が散見されました。(2)の空欄 a は，まずまずの正答率でしたが，空欄 b の正答率は良くなかったと思います。OCSP は，本試験の午前Ⅱ試験でも出題されています。(3)の DV 証明書，OV 証明書，EV 証明書の違いについては，よく理解されていると思います。

設問 3 は，全体的に正答率が低かったと思います。(1)の空欄 c は，HTTPS のポート番号を答えるものでしたが，443 と答えられていなかったようです。(2)は，CONNECT メソッドを使用した場合，ブラウザからプロキシサーバ（SWG）に送られる情報を基にして解答を作成する設問です。CONNECT メソッドに関しては，既に平成 28 年度春期午後 I 問 2，平成 30 年度春期午後 I 問 2 などでも出題されています。過去問題を学習していれば，CONNECT メソッドを使用した場合，SWG に送られる情報には制限があることが分かります。図 2 を見ても，FQDN だけでパス名が指定されていません。このため，FQDN 単位でのフィルタリングは可能ですが，ディレクトリ単位でフィルタリングができないという解答を導くことができると思います。(3)は，SWG で TLS 通信をいったん終端するケースにおいて，Web サーバのサーバ証明書をブラウザが検証する際に注意すべきポイントです。頻出問題の一つですから，十分に理解しておきましょう。

問2　無線 LAN 環境におけるセキュリティ対策

【採点基準】

［設問1］

（1）a，b は，解答例どおりに対し各 3 点。

（2）c 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 4 点。その他は，基本的に 0 点。

（4）生成されるものは，解答例どおりに対し 3 点。行うべき設定は，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。指摘内容が今一歩のものは 3 点。その他は 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 6 点。その他は，基本的に 0 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ものに対し 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。

【講評】

平均点は 11.5 点（平均正答率は 23.1%）で，午後 I の 3 問の中では，最も低い点数でした。

設問 1 は，全体的に正答率が低かったと思います。(1)の空欄 a は，難なくパーソナルが選択できると考えていましたが，その他の記号も多く解答されていました。空欄 b は，暗号利用モードを答えるものですから，正確に覚えていなければ正解できません。(2)の空欄 c は，思いのほか正答率が低かったです。CBC-MAC の MAC とあれば，メッセージ認証コードの MAC を思い浮かべてほしかったと思います。(3)は，問題前文に「個人所有の PC を社内の無線 LAN に接続することも禁止されている」という条件が明示されていますので，容易に正解できると想定していましたが，そうではありませんでした。(4)は，クライアント秘密鍵を用いて作成されるものが問われていますので，素直にクライアントのディジタル署名と答えてほしかったと思います。TLS の通信シーケンスでは，サーバ認証はサーバ証明書を検証することによって行われます。一方，クライアント認証は，クライアント側でディジタル署名を作成し，サーバはその署名を検証することによって行います。こうした基本的な知識は，しっかりと整理しておきましょう。

設問 2 も，正答率は低かったです。(1)は，DHCP 機能で配布されるネットワーク情報に着目することが必要になります。本試験でも，DHCP 機能については十分に理解しているという前提で，問題が出題されています。技術的な仕組みを学習しておくとよいでしょう。(2)は，図 2 並びにその説明から，パスフレーズから PSK が作成され，PSK をそのまま PMK として用います。そして，平文でやり取りされる乱数 A，MAC2，乱数 S，MAC 1 を傍受すれば，第三者も PTK が作成できることを読み取ってほしかったと思います。

設問 3 も，正答率は低かったようです。(2)は，現在無効化されている接続元制限機能に着目すれば，正解を

導くことができます。解答を導くためのヒントは，いろいろなところに散りばめられていることもありますので，問題文の記述内容をチェックしながら問題を読んでいくとよいでしょう。(3)は，問題前文の「クラウドサービスへの通信では，HTTP over TLS，SMTP，POP3 の 3 種類のプロトコルが使用される」という記述に気付くかどうかがポイントでした。

問3 Web アプリケーション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）解答例どおりに対し 4 点。
（3）d は，解答例どおりに対し 2 点。
（4）e は，解答例どおりに対し 4 点。
（5）行番号は，解答例どおりに対し 2 点。特徴は，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。
（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）解答例どおりに対し 4 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）f 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各 4 点。その他は，基本的に 0 点。

【講評】

平均点は 15.3 点（平均正答率は 30.6%）でした。午後 I の 3 問の中では，選択者数が最も少なかった半面，点数は若干ですが，最も高い点数になりました。

設問 1 (1)～(3)の正答率は，比較的高かったことから，平均点を押し上げる結果になったと思われます。(4)は，設問の指示が「解答群の中から全て選び」となっていますが，正解は一つだけのときもあります。解答群を一つ一つ吟味し，該当するものを確定するようにしましょう。(5)の特徴については，a タグの href 属性に関する特徴を述べるものです。href 属性では参照する URL を指定しますが，その形式としては「http://」や「https://」だけではなく，「javascript:」や「mailto:」なども指定できます。このため，「javascript:」によって不正なスクリプトが実行されるリスクがあるので，注意することが必要です。

設問 2 は，(3)の空欄 f を除き，正答率は低かったと思います。例えば，(2)の「トークンを cookie に埋め込む実装が適切ではない」理由を述べる設問では，cookie が盗聴されるなどの解答が散見されました。cookie が盗聴されるリスクを低減させるためには，Set-Cookie ヘッダで secure 属性を指定することが必要です。しかし，この設問では，トークンを cookie に埋め込む実装が適切ではない理由を述べるものです。そこで，どのような条件であれば cookie が Web サーバに送信されるかという基本に立ち返って考えることが必要です。domain 属性などの属性が一致すれば，cookie は HTTP リクエストに無条件に付加されます。cookie の仕組みも，頻出テーマの一つですから，十分に理解しておきましょう。

＜午後Ⅱ＞

問1 Web サイトのセキュリティ

【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 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。
（3）a は，解答例どおりに対し 4 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）b は，切戻しのほか，リカバリ，復旧などの字句も正解（3 点）にしています。

［設問2］

（1）c 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各 6 点。その他は，基本的に 0 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）サーバ名は，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。
（6）e は，解答例どおりに対し 3 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 8 点。その他は，基本的に 0 点。

【講評】

問 1 の平均点は 26.9 点で，問 2 より 4.6 点低い点数になりました。

設問 1 は，全体として正答率は低かったようです。(1)は，D-アプリが改行コードを含んだ件名フィールドの文字列を，そのまま問合せメールのヘッダに出力した場合には，営業担当者以外のメールアドレスにも送信される可能性がありますので，この点を指摘してほしかったと思います。(2)は，認証と認可の意味が十分には理解されていないように感じられました。(4)のエクスプロイトコードは，悪用されると攻撃コードとして使用されます。それぞれの意味をよく整理しておきましょう。

設問 2 は，他の設問に比べ，正答率が高かったようです。強いていえば，(3)は，パッチを適用するまでの期間と，パッチが供給されるまでの期間に WAF を適用すれば，対策になることに気付いてほしかったと思います。

設問 3 (1)，(2)は，まずまずの正答率だったと思いますが，もう少し問題の記述内容を吟味しながら，解答を作成すれば，正答率はもっと上がってくると思われます。(3)は，設問 2 (3)とは異なり，パッチの適用ができない場合には，その回避策（ワークアラウンド）があるかどうかを確認し，対応策を考えることが必要になります。(4)は，正答率は低かったと思います。問題の記述内容を丁寧に読んで，CVSS 基本値を基にして D 社の環境に適用できるように，CVSS 環境値を算出する作業が必要になることに気付いてほしかったと思います。(5)，(7)も正答率は低かったようです。問題の記述内容と，設問で問われていることの整合性などをうまくチェックしながら，何を解答すべきかを常に考え，丁寧に解答を作成することを心掛けてください。

問2 マルウェアの感染と対策

【採点基準】

［設問1］

(1) a ～ c 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) 解答例どおりに対し 4 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) d ～ 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) 名称は，解答例どおりに対し 3 点。処理は，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。

(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3］

(1) g ～ l 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 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。自動転送を行っている旨だけを指摘したものは 3 点。その他は 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 5 点。その他は，基本的に 0 点。

(5) m，n は，解答例どおりに対し各 3 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。

【講評】

問 2 の選択者数は，問 1 よりも少なかった半面，平均点は 31.5 点で，問 1 より高くなりました。

設問 1 (1)では，空欄 b の正答率が低かったと思います。(3)は，Web サーバへの攻撃などを防ぐためには，WAF が必須です。日本語で答えると，20 字近く必要になるので，指定された文字数を意識せず，単純に答えることが必要です。

設問 2 (1)の正答率は，想定していたものよりも低いという印象を受けました。基本的な用語については正確に覚えるようにしましょう。(2)，(3)も同様に，想定していたものより低かったと思います。(3)の SSH の認証方式には，パスワード認証と公開鍵認証の二つがあります。公開鍵認証方式では，クライアントの公開鍵を SSH サーバに登録することが必要です。

設問 3 (1)の正答率は，50%に満たなかったものと想定されます。(2)は，基本的なものでしたから，正答率は高かったです。(3)，(4)の正答率は高くありませんでしたが，(5)は比較的よくできていました。(6)は，センサと W-AP 間は暗号化されているので，マルウェアを検出できない旨の解答が見られましたが，この設問ではマルウェアの挙動を監視する方法が問われています。このため，L3SW におけるポートミラーリングでは，マルウェア感染によるトラフィックを監視することが難しい理由を答えることが必要です。

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しましょう。

以上