2021 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

2021 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 42.0 点，午後Ⅱが 36.9 点でした。2020 年秋期の公開模試は，午後Ⅰの平均点が 45.6 点，午後Ⅱの平均点が 42.8 点でしたから，平均点だけで評価すると，午後Ⅰ，午後Ⅱとも低下しています。問題別の平均点は，午後Ⅰの問 1 が 22.9 点，問 2 が 17.6 点，問 3 が 23.8 点でした。午後Ⅱは，問 1 が 40.8 点，問 2 が 34.9 点で，問 1 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（クラウドサービスのセキュリティ）と問 2（IoT 機器のセキュリティ）の選択者が 61.0%，問 1 と問 3（Web アプリケーションのセキュリティ対策）が 22.0%，問 2 と問 3 が 17.0%という状況でした。問ごとでは，問 1 が 41.6%，問 2 が 38.9%，問 3 が 19.5%でした。4 月 18 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 サイトの点検とセキュリティ対策）の選択者が 34.5%，問 2（マルウェア感染への対応とセキュリティの強化）が 65.5%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 クラウドサービスのセキュリティ

【採点基準】

[設問1]

対策は，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 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 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) a は，解答例どおりに対し 3 点。

(4) 解答例と同様の趣旨（マルウェアスキャンの実行）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。

(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) b ～ e は，解答例どおりに対し各 2 点。

(7) f，g は，解答例どおりに対し各 3 点。

[設問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 22.9 点（平均正答率は 45.9%）でした。全体的に正答率が高く，午後 I の 3 問の中では，問 3 と，ほぼ同程度の点数になりました。

設問 1 の対策は，プロキシサーバにおける URL フィルタリングを指摘した答案は，必ずしも多くはありませんでした。理由の方は，正答率は高かったと思います。

設問 2 (1)の正答率は高かったようです。(2)は，想定していたよりも正答率は良かったと思います。(3)の CASB についても，よく理解されているようでした。(4)の，クラウド P で TLS 通信を終端し，復号した後にマルウェアスキャンを行うことについては，正答率が低かったと思います。プロキシサーバで行われる処理などについては，十分に理解を深めておきましょう。(5)は，「証明書 2 をインストールする」などの答案が散見され，正答率は低かったです。クラウド P では，証明書 1 のコモンネームと同じ値を入れた証明書 2 を動的に生成して利用者端末の Web ブラウザに送信します。つまり，クラウド P が証明書 2 を新たに発行するわけですから，証明書 2 を検証するためのルート証明書が必要になります（証明書 2 はクラウド P から送られてきますので，インストールする必要はありません）。こうしたサーバ証明書に関する検証の問題は，よく出題されますので，正確に理解しておきましょう。(6)の正答率は，高かったです。(7)の正答率は，比較的良かったと思います。

設問 3 の正答率は，想定していたよりも良かったと思います。問題の記述内容を把握しながら解答を作成された結果と思います。

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) b は，解答例どおりに対し 2 点。
(3) c は，解答例どおりに対し 2 点。
(4) d，e は，解答例どおりに対し各 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 6 点。その他は，基本的に 0 点。

［設問2］

(1) 不足している情報は，解答例どおりに対し 2 点。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。
(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。秘密鍵が指摘されていないものは 3 点。その他は 0 点。
(4) f は，解答例どおりに対し 2 点。

［設問3］

(1) コード署名，コード署名証明書ともに，解答例どおりに対し各 3 点。
(2) g 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。

【講評】

平均点は 17.6 点（平均正答率は 35.1%）であり，午後 I の中では，最も低い点数でした。

設問 1 (1)～(3)の正答率は，高かったと思います。(4)は，センサシステムの構成要素の役割を把握すれば，正解できる問題です。本試験では，落ち着いて考えるようにしましょう。(5)の正答率は，低かったです。クライアント認証を行うためには，クライアントからクライアント証明書が送られてきます。そして，サーバではクライアント証明書の検証を行いますから，検証に成功すれば，証明書内にある情報は改ざんされていないと判断できます。こうした視点に立って解答を作成してほしかったと思います。

設問 2 (1)は，問題文からセンサアプリの契約期間に気付くことでき，正答率は比較的良かったと思います。(2)は，問題の記述内容をうまく整理できなかったようで，正答率は低かったです。(3)は，センサの SSD からクライアント証明書をコピーする旨は指摘されていました。クライアント認証を行うためには，クライアント側ではクライアント証明書と秘密鍵のセットを格納しています。こうした問題では，秘密鍵を指摘することがポイントになります。(4)は，用語の選択問題です。消去法によって対象の用語をできるだけ絞るようにしましょう。

設問 3 は，全体的に正答率が低かったと思います。特に，(3)はコード署名とコード署名証明書（コードサイニング証明書）を混同した答案や，コード署名を作成する際に使用する鍵を明記していない答案も散見されました。コード署名証明書は，ディジタル証明書（公開鍵証明書）の一つです。こうした基本的な知識をベースにしながら，論理的に考えていく姿勢を身に付け，正解を導いていくようにしましょう。

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 は，解答例どおりに対し 2 点。
(2) b，c は，解答例どおりに対し各 2 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 2 点。効果は，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。
(5) f 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2］

(1) g は，解答例どおりに対し 2 点。
(2) adr1，adr3 とも，解答例どおりに対し各 4 点。
(3) h は，解答例どおりに対し 2 点。i 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) j は，解答例どおりに対し 2 点。
(5) b，c 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。指摘内容が今一歩のものは 3 点。その他は 0 点。

【講評】

平均点は 23.8 点（平均正答率は 47.6%）でした。午後 I の中では，最も高い点数でした。

設問 1 (1)～(3)は，正答率は高かったと思いますが，(2)は，HttpOnly 属性と Secure 属性を逆に答えた答案も散見されました。Cookie の属性などについては，Web アクセスにおける基本的な仕組みの一つですから，十分に理解しておきましょう。(4)は，問題の条件が十分に読み取られていないような答案も散見されました。試験では，問題の記述内容から適切な対応とは何かを考えることがポイントになります。(5)の正答率は，低かったです。HTTP ヘッダインジェクションとは何か，%0d%0a をデコードとすると CR/LF（Carriage Return/Line Feed）になることなどの様々な知識を，できるだけ多く習得していくように努めましょう。

設問 2 (1)，(2)，(4)，(5)の正答率は，比較的が高かったようですが，(3)，(6)の正答率は低かったと思います。

いずれにしても Web 関連の問題を選択する場合には，Web アプリに対する様々な攻撃のほか，Same-Origin Policy などの Web アクセスに関するセキュリティ上の考え方をはじめ，Web 技術全般に関する知識が要求されます。IPA が公開している資料などを基にして，さらに理解を深めていくようにしましょう。

＜午後Ⅱ＞

問1 Web サイトの点検とセキュリティ対策

【採点基準】

［設問1］

(1) 理由，運用管理方法とも，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 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2］

(1) 解答例どおりに対し各 2 点。三つ以上，答えたものは，一つにつき 2 点の減点。
(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) a 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) b ～ d は，解答例どおりに対し各 3 点。
(2) キーレコード内の情報，DM に含まれる情報とも，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。指摘内容が今一歩のものは 3 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 4 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。指摘内容が今一歩のものは 3 点。その他は 0 点。
(2) 解答例どおりに対し各 3 点。三つ以上，答えたものは，一つにつき 3 点の減点。
(3) e ～ g，h ～ j，k ～ m は，それぞれ完答で各 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5］

(1) n ～ p は，解答例どおりに対し各 2 点。
(2) q 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。

【講評】

問 1 の平均点は 40.8 点で，問 2 よりも約 6 点高くなりました。

設問 1 (1)は，理由とともに，その状況を改善するための運用管理方法を問いましたが，運用管理方法ではなく，対策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よく確認した上で，解答を作成するようにしてください。(2)も同様です。

設問 2 (1)は，想定よりも正答率は低かったですが，(2)の正答率は高かったと思います。(3)は，ほぼ想定どおりの正答率でした。

設問 3 (1)，(2)の正答率は，比較的高かったと思います。(3)は，具体的に述べよという条件がありますから，

「メールサーバの IP アドレスを指定した SPF レコード」などにように解答することが必要です。(4)の正答率は，比較的良かったと思います。

設問 4 (1)は，少し複雑な問題でしたから，正答率は低かったです。(2)は，専門的な知識が必要ですから，正答率は高くはありませんでした。(3)は，正答率がかなり低くなると考えていましたが，条件をよく考慮されていたようで，まずまずの結果でした。(4)の正答率は，比較的良かったと思います。

設問 5 (1)の n，o は，OV と EV を逆に答えたものが散見されましたが，まずまずの正答率でした。p の正答率は低かったです。(2)の正答率は低かったと思いますが，(3)は，よくできていました。

問2 マルウェア感染への対応とセキュリティの強化

【採点基準】

[設問1]

(1) a，b 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各 5 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。

[設問2]

c，d は，解答例どおりに対し各 3 点。

[設問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4]

(1) e 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。

[設問5]

(1) f，g は，解答例どおりに対し各 3 点。

(2) h 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。

(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6]

(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) 監視，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 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。

(4) i は，解答例どおりに対し 3 点。

(5) 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。

(6) k ～ m は，完答で 4 点。

【講評】

平均点は 34.9 点で，問 1 よりも約 6 点低い結果でした。一方，問 1 と問 2 の選択者数の比率は 1 対 2 で，約 2 倍の受験者が問 2 を選択していました。

設問 1 (1)は，a，b ともネットワークの専門知識に関するものですから，必要なキーワードを適切に答えることが必要です。a は，内部ネットワークからの DNS 問合せもありますので，外部からの再帰的な DNS 問合せというように答えることがポイントです。(2)は，設問の条件を加味しないで，FW を通過する通信の例を挙げた答案が散見されました。

設問 2 の正答率は，それほど高くはありませんでした。c が FW，d がプロキシサーバという答案が散見されました。問題をよく読んで条件を満たすように，空欄に入れる適切な字句を考えるようにしましょう。

設問 3 は，図 2 のマルウェア P の概要を把握しながら解答を作成することがポイントです。単に証拠保全の目的を述べたような答案が見受けられました。

設問 4 (1)，(2)の正答率は，低かったと思います。CONNECT メソッドの使い方，その仕様などは基本知識の一つになっています。また，CONNECT メソッドは悪用されるおそれがあることなども，よく理解しておきましょう。

設問 5 (1)～(3)は，まずまずの正答率でしたが，(4)の正答率は，低かったと思います。午後Ⅱは問題分量が多いので大変ですが，設問で問われていることに合致する記述を，問題文の中から丁寧に見つけ出していくことが大切です。

設問 6 (1)，(4)，(5)，(6)の正答率は，比較的高かったと思います。(2)は，問題の記述内容に基づき，端末へのログイン監視を行う旨を指摘した答案は，少なかったようです。(3)は，監視を見直すことが問われていますが，対策を述べたものが散見されました。設問で問われていることに対して，適切に答えるようにしましょう。

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，セキュリティだけではなく，ネットワーク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