2023 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

2023 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 51.2 点，午後Ⅱが 41.1 点でした。2022 年秋期の公開模試は，午後Ⅰの平均点が 48.0 点，午後Ⅱの平均点が 41.8 点でしたから，平均点だけで評価すると，午後Ⅰは少し向上しました。問題別の平均点は，午後Ⅰの問 1 が 20.6 点，問 2 が 31.7 点，問 3 が 18.5 点でした。午後Ⅱは，問 1 が 34.1 点，問 2 が 43.9 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，こうした解答が少なからず見られました。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，採点者に理解されやすい解答を作成するようにしましょう。

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（サーバ証明書の検証）と問 2（PC のマルウェア対策）の選択者が 55.1%，問 1 と問 3（Web アプリケーションのセキュリティ強化）が 1.6%，問 2 と問 3 が 43.3%という状況でした。問ごとでは，問 1 が 28.4%，問 2 が 49.2%，問 3 が 22.4%でした。4 月 16 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 サイト及び社内システムのセキュリティ対策）の選択者が 27.8%，問 2（インシデント対応）が 72.2%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る」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（諦めずに）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 サーバ証明書の検証

【採点基準】

[設問1]

（1）解答例どおりに五つの情報が指摘されているものに対し 6 点。その他は 0 点。

（2）a ～ e は，解答例どおりに対し各 2 点。

（3）公開鍵，署名とも，解答例どおりに対し各 3 点。

[設問2]

（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（並列処理が可能である旨）に対し 6 点。その他は，基本的に 0 点。

（4）モードは，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。

(5) 解答例どおり（完答）に対し 6 点。その他は 0 点。

【講評】

平均点は 20.6 点（平均正答率は 41.2%）でした。全体的に正答率が低く，問 2 の平均点に比較すると，約 11 点低い結果になりました。

設問 1 (1)の正答率は，低かったです。DNS キャッシュポイズニング攻撃については，よく理解されていると思いますが，攻撃が成功する条件として，DNS 応答パケットのヘッダー情報を五つ全て答えることは，ネットワークの知識が必要でしたから，少し難しかったようです。(2)の正答率は，平均的でした。用語の意味を正確に覚えておくことは，解答作成の基本になりますから，日頃から一つ一つの知識を積み重ねていくことを忘れないようにしましょう。(3)のクロスルート証明書に設定する公開鍵と署名については，正答率が少し低かったようです。

設問 2 (1)の正答率は，平均的でした。(2)の正答率も，平均的でした。答案の中には「平文と暗号文が 1 対 1 に対応する」旨のものが散見されましたが，設問では，平文と暗号文が 1 対 1 に対応すると，どのようなセキュリティ上の問題が発生するかを問うています。セキュリティ上の問題を具体的に答えることが必要です。(3) の正答率は，比較的良かったと思います。(4)，(5)の正答率は，比較的低かったようです。特に，(5)は，TLS 1.3 で使用する共通鍵は，認証付き暗号（AEAD）だけが許可されているので，解答群の中では AES-CCM 又は AES-GCM に絞ったのち，PFS の性質をもつ鍵交換アルゴリズムの DHE 又は ECDHE を用いる暗号スイートを選べば，容易に解答できるはずです。答案の中には，正解の記号に加え，（イ）あるいは（カ）などを含めたものが散見されました。

問2 PC のマルウェア対策

【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 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) d，e 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。

[設問2]

(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（又は，VLAN を設定して各部 LAN 間の通信を遮断する）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。

【講評】

平均点は 31.7 点（平均正答率は 63.4%）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。また，ほぼ全ての受験者が選択しており，取り組みやすい問題だったといえます。

設問 1 (1)，(2)の正答率は高かったです。(3)の正答率は，平均的でした。(4)の正答率も高く，マルウェア A に対するフルスキャンの指示と，Z 社がマルウェア A の定義ファイルを配布した時系列を正しく把握して答えられていました。(5)の正答率は，平均的でした。(6)は少し考えにくいところもありましたが，正答率は比較的良かったです。

設問 2 (1)の正答率は，平均的でした。(2)の正答率も平均的でしたが，図 1 の注記 4 にある「L3SW はパケットフィルタリング機能をもつが，使用していない」に着目し，「パケットフィルタリング機能を有効化する」旨の答案が散見されました。着眼点は問題ありませんが，具体的にどのような通信を制御するのかが不明ですので，こうした設問には，制御する内容を必ず答えるようにしましょう。なお，問題では L3SW の機能について，パケットフィルタリングしか明記していませんでしたが，L3SW は一般に VLAN 機能を有していますので，VLAN に着目した解答も正解にしています。

設問 3 (1)の正答率は平均的でした。プロキシサーバには既に Z 社のマルウェア対策ソフトを導入していることに加え，W 社のマルウェア対策エンジンを導入する効果を問うものでしたが，「インターネットからの入り口での検出効果が期待できる」旨の答案も散見されました。(2)の正答率は高かったです。

問3 Web アプリケーションのセキュリティ強化

【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 6 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）解答例どおり（完答）に対し 5 点。その他は 0 点。

（2）d，e は，解答例と同様の意味合いをもつものに対し各 4 点。

［設問4］

（1）f は，解答例どおりに対し 3 点。

（2）g ～ i 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。

【講評】

平均点は 18.5 点（平均正答率は 36.9%）で，午後 I の 3 問の中では，最も低い点数でした。また，選択者数も 3 問の中で，最も少ない比率でした。

設問 1 の正答率は，平均的でした。

設問 2 の正答率は，(1)～(3)とも低かったようです。(2)については，“/ss”と解答すべきところを，“ss”と記入された答案が散見されました。本番の試験では，些細なミスが命とりになりますから，十分に注意しましょう。

設問 3 (1)の正答率は，まずまずでしたが，(2)の正答率は，低かったと思います。Web 関連のセキュリティ問題を選択する場合には，CSP（Content-Security-Policy）ヘッダーをはじめ，same origin などの基本的な用語を十分に把握するようにしましょう。

設問 4 (1)の正答率は，まずまずでした。(2)の正答率は，高くなると想定していましたが，そうではありませんでした。cookie のやり取りには Set-Cookie と Cookie ヘッダーが使用されるほか，その属性には Secure，HttpOnly，Domain，Path，Expires，SameSite などがあります。ブラウザが cookie を扱うための条件を，それぞれの属性によって指定します。一つ一つの知識を積み重ねながら的確に把握するようにしましょう。(3)は，WAF の一般的な導入効果を答えた答案が散見されましたが，この設問では，下線④に「N サイトにおける現在の課題を解決すること」とあるので，〔Web アプリのセキュリティ点検〕の E 主任の「主要ブラウザの仕様変更への対応が課題になっています」という発言に気づいてほしかったと思います。

＜午後Ⅱ＞

問1　Web サイト及び社内システムのセキュリティ対策

【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（パラメータ hist を書き換えること）に対し 8 点。指摘内容が今一歩のもの（履歴 Num を書き換えること）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 ～ j は，解答例どおりに対し各 1 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 8 点。その他は，基本的に 0 点。

［設問3］

（1）解答例どおり（完答）に対し 6 点。その他は 0 点。

（2）k，l 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 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 8 点。その他は，基本的に 0 点。

［設問4］

（1）m 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 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各 4 点。その他は，基本的に 0 点。

（4）n 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各 4 点。その他は，基本的に 0 点

（6）o 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 6 点。その他は，基本的に 0 点。

【講評】

問 1 の選択者数は約 28%であり，平均点は 34.1 点と，問 2 よりも約 10 点低いという結果になりました。

設問 1 は，全体的にやや正答率が低かったです。(1)の異なる利用者の情報を参照する方法として，どのようなリクエストを送信する必要があるかという形式の問題はよく出題されるので，十分に理解しておきましょう。(2)は，Web API の診断時に A サイト上のファイルが削除されたという事象に着目すれば，解答を作成できると思っていましたが，採点結果はそうではありませんでした。(3)の正答率も，低かったと思います。

設問 2 の(1)，(2)の正答率は平均的でしたが，(3)の正答率は低かったです。認証情報や認可情報の連携については，基本的な考え方を把握するようにしましょう。

設問 3 は，全体的に正答率は低かったようです。(1)のように，完答が求められる設問は，選択肢を一つ一つ

丁寧に確認していくようにしましょう。(2)の空欄 k の正答率は平均的でしたが，空欄 l の正答率は，少し低かったと思います。(3)の DMARC は，最近注目されていますから，DMARC を導入することによる効果をよく理解しておくとよいでしょう。

設問 4 の(1)，(4)，(6)の穴埋め問題の正答率は平均的でした。(2)は，不正な ST を業務サーバにおいてログを取得する必要性について尋ねましたが，正答率は低かったです。(3)は，root アカウントを無効化することによって期待できる効果を問う問題でしたが，正答率は低かったようです。(5)は，(3)と同様に正答率は低かったと思います。(7)は，問題の条件がうまく反映できていなかったようで，正答率は思っていたよりも，低かったと思います。

問2 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) b は，解答例どおりに対し 3 点。

(3) c，d は，解答例どおりに対し各 3 点。

［設問2］

(1) 解答例（又は，同様の意味合いをもつ字句）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3］

(1) e は，解答例どおりに対し 3 点。

(2) f は，解答例，又はそれと同様の意味をもつ字句を指摘したものに対し 4 点。

(3) g 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 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 8 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。

(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 6 点。その他は，基本的に 0 点。

(8) h ～ j は，解答例どおりに対し各 3 点。

［設問4］

(1) k 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（対象が誰かと，どのような訓練かという 2 点）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) 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（TLS インスペクション機能と IPS 機能の二つ）に対し 8 点。二つの機能のうち，いずれか一方だけを指摘したものは 4 点。その他は 0 点。

(5) l 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。

【講評】

問 2 の選択者数は，7 割強でしたから，受験者が取り組みやすいと判断した結果と思われます。また，平均点でも 43.9 点で，問 1 よりも約 10 点高い点数でした。

設問 1 は，全体的に正答率が高かったですが，(3)の空欄 d の正答率は低かったと思います。

設問 2 (1)の正答率は，比較的高かったです。(2)は，独自のルールの特徴を答えるものですが，ホワイトリストに登録する内容や理由を解答したものなどが散見され，正答率は低かったと思います。

設問 3 (1)～(3)の穴埋め問題の正答率は，平均的でした。(4)は，技術的な内容を答える設問でしたが，まずまずの正答率だったと思います。一部，DNS リフレクション攻撃や DNS キャッシュポイズニング攻撃を想定した答案も散見されました。(5)，(6)の正答率は低かったと思います。(7)は，問題の図 2 中の(i)のシグネチャ検知の記述内容を見極めて解答を作成されており，正答率は比較的高かったようです。

設問 4 (1)の正答率は高かったです。(2)～(4)の正答率も，問題の記述内容などをうまく引用するなどして，答案が作成されていたようで，比較的高かったと思います。(5)は，アクセス制御を行う対象は，業務サーバ D です。このため，ファイアウォールではなく，業務サーバ D において，どのような通信を許可すればよいかという観点から答案を作成すると，正答率はもっと上がると思います。

午後Ⅰ，午後Ⅱという二つの試験が行われるのは，今回の試験で最後になります。来たる 4 月 16 日に行われる本試験の実施日に向けて，より多くの知識を吸収するなどして，さらなるレベルアップを図るようにしましょう。試験当日においては，冷静に問題と向き合い，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た上で，的確で理解しやすい内容の答案を作成することを心掛けてください。そして，必ず合格するという強い気持ちで臨むようにしましょう。

以上