2013 秋 情報セキュリティスペシャリスト 全国統一公開模試 講評と採点基準

2013 年 9 月 24 日 (株)アイテック 教育研究開発部

■ 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 42.1 点，午後Ⅱが 32.1 点でした。問題別では，午後Ⅰの問 1 が 27.0 点，問 2 が 15.4 点，問 3 が 16.4 点で，問 2，問 3 の平均点が低かったといえます。また，午後Ⅱは，問 1 が 33.5 点，問 2 が 30.9 点でした。2013 年春期の公開模試では，午後Ⅰの平均点が 41.9 点，午後Ⅱの平均点が 36.6 点でしたから，午後Ⅰはほぼ同レベル，午後Ⅱは少し下回る結果となりました。

次に，採点結果から受けた印象としては，問題で記述された内容，あるいは設問で指示されていることにあまり従わず，各自が持ち合わせている知識や先入観などに基づいて解答を作成していると思われる答案が多く見られました。問題の記述内容や設問の指示に従って答案を作成することが，合格するための必須条件となります。本番の試験では，こうした事項については改善していく必要があると思います。特に，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ようにしましょう。また，問題によっては，設問で具体的に述べよと指示されている場合があります。こうしたケースで，例えば，必要最小限の範囲に対してだけ権限を与えるなどと解答しても，それでは具体的と見なされません。権限が与えられるべき範囲を問題の記述から導き出し，それを具体的に表現することが必要です。

次に，問題ごとの選択状況を紹介しておきます。午後Ⅰ試験では，問 1（情報漏えい対策）の選択者が 45.3%，問 2（Web アクセスのセキュリティ）が 13.5%，問 3（社内における脅威）が 41.5%で，大半の受験者が問 1 と問 3 を選択していたことになります。なお，今回の午後Ⅰ試験から，出題される問題数が 4 問から 3 問に減少します。従来と比べて選択の幅が少なくなるので，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ことが必要になると思われます。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。本番の試験日までの期間で，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試験では，問 1（セキュアな Web アプリケーションの開発）の選択者が 43.7%，問 2（標的型攻撃への対策）が 56.3%という比率でした。なお，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になることが多いので，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，試験センターでは「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，かえって失敗してしまいます。

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考えることによって正解を導き出すことができます。更に，設問で問われていることを十分に確認し，問題の記述内容と照らし合わせながら解答を導いていく訓練をしておくとよいでしょう。

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）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 情報漏えい対策

【採点基準】

[設問1]

a，b は，解答例どおりに対し各 3 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。収集した情報を定期的にチェックする，あるいは警告を出す旨の指摘は 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 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。指摘内容が今一歩のものは 3 点。その他は 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。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 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 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 6 点。確認コードによりなりすましが防止できるなど，二要素認証の指摘が明確になっていないものは 3 点。その他は 0 点。

【講評】

平均点は 27.0 点（平均正答率は 54.0%）であり，情報漏えい対策に関する基本的な知識は，しっかり身に付いているものと思われます。

設問 1，設問 2 とも，全体的に正答率は高かったようです。つまり，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。

設問 3 (1)は，ミドルウェアなどについては，利用者の設定に依存しており，修正プログラムが適用されていないことの問題を解決するための方法を問うものです。このため，「ソフトウェアのバージョン情報を確認する」などの指摘では，「PC 上のミドルウェアを更新する」旨のキーワードがないことから，不正解にしました。点数を失わないためには，設問で問われていることに対し，丁寧に解答していくことが大切です。また，(2)は，不正アプリをリストに登録しているかどうかが採点上のポイントです。例えば，未知の不正アプリがインストールされるなどの表現は，未知のものを検知した際に，それをリストに登録すれば，インストールを避けることができるので，こうした指摘内容は不正解にしました。

設問 4 (1)は，想定していた以上に正答率は良かったと思います。しかし，解答字数が 60 字でしたから，適切に表現しきれていない答案も見受けられました。採点者は，解答用紙に記述された内容だけで判断しますので，分かりやすく記述することが必要です。(2)も，問題で記述された状況をうまく整理できず，認証を強化できる理由だけを解答していたものが見受けられました。認証を強化するには，二要素認証を採用することもその一つの方法です。こうしたセキュリティの基本的な知識は，しっかりとインプットしておきましょう。

問2 Web アクセスのセキュリティ

【採点基準】

［設問1］

（1）a ～ e 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。指摘内容が今一歩のものは 3 点。その他は 0 点。

［設問2］

（1）要件は，解答例どおりに対し各 2 点（ただし，三つ以上，解答したものについては，一つにつき 2 点ずつの減点を行う）。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。FW は認証機能をもっていないなど，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（更新頻度の高い在庫情報）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 15.4 点（平均正答率は 30.8%）と，午後 I の 3 問の中では，最も低い点数でした。

設問 1 (1)の正答率は，空欄 b を除き，高かったと思います。その半面，(2)～(5)の正答率は，全体的に低かったようです。サーバ証明書の検証方法は，よく理解されていると思いますが，(3)のように，表で示された項目名を用いた説明が求められると，極端に正答率が低くなってしまいます。誤答の例として，署名をサブジェクトの公開鍵を用いて検証するという答案などが，少なからず見受けられました。署名は，発行者（CA）が行うものであり，サブジェクト（公開鍵の所有者）ではありません。このほか，クライアント証明書を不特定の利用者がもつことを前提にできないことなども基本的な知識といえます。なお，(5)は，難度の高い設問でしたから，必然的に正答率も低くなったようです。

設問 2 (1)は，要件 1 から 5 の内容が十分に把握できていなかったようで，全体的に正答率は低かったと思います。(2)は，正答率は良かったものの，一般的なキャッシュの説明をしていたり，DNS キャッシュポイズニングと読み間違えたりしたような答案も見受けられました。問題の記述内容をよく確認した上で，解答を作成するようにしましょう。

問3 社内における脅威

【採点基準】

［設問1］

（1）a，b とも，解答例どおりに対し各 3 点。

（2）解答例と同様の趣旨，例えば，特権操作は不正なアクセスかどうかを判断しにくい旨などが適切に

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（特権操作の内容が具体的に示されているもの）に対し 6 点。単に管理者 ID では特権操作ができる旨の指摘は 3 点。その他は 0 点。

［設問2］

(1) 項番は，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。対策は，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（電子すかしというキーワードが必要）に対し 8 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（セキュリティ規定を順守すること）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 16.4 点（平均正答率は 32.7%）にとどまり，想定していたよりも，低い正答率になりました。

設問 1 は，全体的に正答率が低かったようです。例えば，(1)の空欄 a は 27001，空欄 b は可用性，保守性，安全性などの誤答が目立ちました。基本的な用語については，正確に覚えておくことが必要です。(2)では，問題文に「取得されたログについては，管理者用 ID の特権操作によっても，改変できないように管理されている」と記述されているにもかかわらず，ログを操作するなどの答案も見られました。解答作成に当たっては，問題の条件を必ずチェックするようにしましょう。

設問 2 (1)の理由では，「1 名で作業を行っている」という表現にとどまり，セキュリティ上の理由を指摘していないものが目立ちました。セキュリティの問題ですから，1 名で作業を行うことで相互けん制が働かなくなるという点を明確に解答するようにしましょう。また，対策としては，「要員計画の点から，現在の作業体制は変更できないという制約条件がある」と記述されているにもかかわらず，2 名体制にするなどといった安易な解答が目立ち，点数を失っていました。本番の試験では，同じ間違いを繰り返さないようにしましょう。

設問 3 (1)では，「セキュリティ規定を順守する」旨のキーワードをしっかり指摘してほしかったと思います。(2)の正答率は良く，特に問題はありませんが，強いて言えば，分かりやすい文章で記述していくことを常に心掛けるようにしましょう。

＜午後Ⅱ＞

問1 セキュアな Web アプリケーションの開発

【採点基準】

［設問1］

a ～ e は，解答例どおりに対し各 3 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 8 点。その他は，基本的に 0 点。

［設問3］

(1)「十分な長さがある」,「ランダムである」旨が適切に指摘されているものに対し各 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 6 点。その他は，基本的に 0 点。

(3) 読み取ること，メッセージとも，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 3 点。その他（利用者 ID とパスワードの admin が正しい旨の指摘など）は 0 点。

［設問4］

(1) 項番 1 ～ 3 は，解答例どおりに対し各 3 点。

(2) f は，解答例どおりに対し 4 点。

［設問5］

(1) 体制，対応手順とも，解答例と同様の趣旨が適切に指摘されているもの（問題点と改善すべき事項が示されているもの）に対し各 6 点。問題点の指摘，ないしは改善点の指摘だけにとどまっているものなどは 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 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のほか，CMS サーバから Web サーバへの通信は正常なものなので，NIDS では検知できない旨を指摘したものなどは 8 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) 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（DNS サーバに関する調査方法など）は 4 点。その他は 0 点。

【講評】

問 1 の平均点は 33.5 点で，問 2 よりも少し高い点数でしたが，基本的な問題と考えて出題した設問の正答率

は，期待していたような結果とは異なりました。

設問 1 は，基本的な用語が多いと考えていましたが，全体的に正答率は低かったと思われます。

設問 2 (1)の正答率はまずまずでしたが，(2)の正答率は，耐タンパ性という特性が必ずしも理解されていないようで，かなり低かったようです。

設問 3 (1)は，基礎的なものですから，正答率は高いと考えていました。しかし，セッション ID ではなく，パスワードの要件を答えていたようなものも見られました。(2)もそうですが，設問で問われていることは何かを考慮し，素直に解答を作成していくことが必要です。

設問 4 も，正答率は決して高くはありませんでした。基本的な攻撃の内容については，よく理解しておきましょう。

設問 5 (1)は，図 3 の中からインシデント対応における問題点を的確に抽出し，その上で改善すべき内容を述べることが求められています。しかし，設問で問われていることとは関係なく，インシデント発生時における対応策を記述したものが多く見られました。また，ウイルスの感染を防ぐにはどうすべきかといった観点の答案も見られました。本番の試験では，設問で問われていることに忠実に従って解答を作成することが基本ですから，こうした姿勢を身に付けていきましょう。

設問 6 (1)の正答率は，比較的良かったと思います。(2)は，共用サーバは DNS サーバしかないことまでは攻めきれていましたが，その確認内容になると今一歩の答案が多かったように思われます。

問2 標的型攻撃への対策

【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 ～ g は，解答例どおりに対し各 3 点。

(2) 情報は，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。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。

(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。指摘内容が今一歩のもの（メッセージの改ざんを検出できることだけを指摘したものなど）は 4 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 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 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 8 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 8 点。指摘内容が今一歩のもの（送信元メールサーバの名前解決に失敗したことなど）は 4 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 4 点。その他は，基本的に 0 点。

[設問4]

(1) h，i は，解答例どおりに対し各 3 点。

(2) 解答例どおりに対し 4 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 5 点。その他は 0 点。

【講評】

平均点は 30.9 点にとどまり，問 1 よりも若干，低くなりました。

設問 1 (1)では，空欄 a の APT の正答率が低かったと思います。(2)の正答率は良かった半面，(3)では，会話文で K 君が「社員がメールに添付されたウイルスを実行しないようにする教育が必要です」と発言しているので，「メールの添付ファイルを安易に開かない」旨の指摘が正解になることは，まずありません。ウイルス対策としては，ウイルス定義ファイルを最新にすることと，最新のセキュリティパッチを充てることが基本です。こうした基本的なことは忘れないようにしましょう。

設問 2 は，(5)を除き，全体的に正答率は低かったようです。SPF／Sender ID，DKIM などの仕組みは，少し複雑ですが，十分に把握しておくとよいでしょう。

設問 3 の(1)，(3)の正答率は高かった半面，(2)の正答率は低かったように思います。DNS の仕組みは，セキュリティ技術者にとっても，重要になってきています。できるだけ技術の詳細を理解するように努めましょう。

設問 4 は，全体的に正答率が高くなかったようです。APT 対策については，URL フィルタ，プロキシサーバにおけるユーザ認証などが必要となります。

なお，本番の試験で合格基準点をクリアするには，問題の記述内容が複雑になったり，高度になったりしても，正解を導いていくことができるようにする必要があります。基本的な知識のほか，問題の読解力，全体の関係を相互に整理しながら考える洞察力などを，できるだけ磨いていくようにしましょう。

以上