2013 春 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 3 月 26 日 (株)アイテック 情報技術教育研究部

■ 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 41.9 点，午後Ⅱが 36.6 点でした。問題別では，午後Ⅰの問 1 が 14.1 点，問 2 が 26.2 点，問 3 が 19.6 点，問 4 が 22.4 点で，問 2 の平均点が最も高くなりました。また，午後Ⅱは，問 1 が 30.8 点，問 2 が 41.1 点でした。2012 年秋期の公開模試では，午後Ⅰの平均点が 48.1 点，午後Ⅱの平均点が 34.2 点でしたから，午後Ⅰは低下した半面，午後Ⅱは若干向上するという結果になりました。これは，全体的な受験者のレベルになりますが，今回の模試でも，本番の試験に向けて十分に準備できている受験者と，そうでない受験者の差が相当大きかったことは，間違いないと思われます。

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数多く見られました。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，合格するための絶対条件となります。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，「必要最小限の権限を与える」など，問題文に記述されていることをそのまま引用しても，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試験は，4 問の中から 2 問を選択するので，平均的な選択率は 25%になります。今回は，問 1（スマートデバイスの業務利用）の選択者が 25.6%，問 2（ソフトウェアの脆弱性への対応）が 39.8%，問 3（マルウェアの不正侵入対策）が 30.2%，問 4（セキュアプログラミングの導入検討）が 4.4%であり，問 2 と問 3 の選択者が多くなりました。午後Ⅰ試験では，得意とする分野の問題を早く見極め，その問題で，できるだけ多くの点数を獲得することが必要です。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レベルが，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（Web システムの脆弱性診断と対策）の選択者が 43.0%，問 2（認証システムの再構築の検討）が 57.0%という比率でした。午後Ⅱ試験は，様々なセキュリティ分野から出題される総合的な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ようにしましょう。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。このため，一定の知識レベルに達していれば，問題の記述内容を基にして正解を導き出すことができます。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作成していくための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 スマートデバイスの業務利用

【採点基準】

[設問1]

（1）a ～ f は，解答例どおりのみ各 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 8 点。その他は，基本的に 0 点。

[設問3]

（1）g，h は，解答例どおりのみ各 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。

【講評】

スマートデバイスにおけるセキュリティ問題は，注目度が高いので，平均正答率 35%程度と考えていましたが，結果的には 28.1%（14.1 点）にとどまりました。

設問 1 (2)は，設問で何が問われているかを確認することなく，解答を作成したのではないかと思われます。例えば，スマートデバイスの紛失＝情報漏えい問題と考えてしまい，デバイス内にある情報を消去したり，暗号化したり，あるいはパスワードロックをかけるなどの答案がかなり見られました。しかし，この設問で問われていることは，私物デバイスに残されたログについて，その証拠の保全性を確保するには，従業員との間でどのような取決めが必要になるかということが問われています。問題の記述内容に従って，素直に考えていくことが必要です。設問 1 (3)の正答率は，かなり低かったようです。SSL の通信シーケンスでは，サーバ認証はサーバ証明書の検証によって行われ，クライアント認証は，クライアントのディジタル署名によって行われます。こうした基本的な事項は，一つ一つ積み重ね，よく理解していくようにしましょう。

設問 2，設問 3 は，やや専門的な観点からの出題でしたから，解説などをよく読んで，その内容などを十分に把握するようにしましょう。

問2 ソフトウェアの脆弱性への対応

【採点基準】

［設問1］

（1）受付期間，調整機関は，解答例どおりのみ各 2 点。

（2）a，b は，解答例どおりのみ各 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各 6 点。内容が今一歩のものは 3 点。その他は 0 点。

（2）「重要度の高いものから検証する」，「問題のないことを確認して適用する」という二つのキーワードが適切に指摘されているものに対し 6 点。どちらか一方の指摘のものは 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 8 点。その他は，基本的に 0 点。

［設問3］

（1）方式は，解答例どおりのみ 2 点。理由は，方式が正しく，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（特に，どのような情報を用いて確認するかということ）が適切に指摘されているものに対し 6 点。内容が今一歩のもの（例えば，パッチの適用状況を確認するだけなどのもの）は 3 点。その他は 0 点。

【講評】

選択者数が最も多く，平均正答率でも 52.4%（26.2 点）と，午後 I の 4 問の中では，最も高くなりました。

点数的にはまずまずといえますが，答案作成上は，もっと工夫する必要があります。設問 2 (1)で問われていることは，「スマートデバイスへのアプリのインストールに関して規定すべきルール」を挙げることですが，アプリケーションを利用する上での対策を述べた答案（例えば，必要以上の権限は許可しないことなど）がかなり見られました。また，設問 2 (3)では「パターンファイルが作成されにくい理由」が問われていますが，標的型攻撃の説明をした答案や，パターンファイルでは検知されにくい理由を述べた答案が，数多く見られました。

問 2 に限らず，どの問題も設問で問われていることを十分に把握することなく，無条件にセキュリティ問題に対する対策などを述べる傾向が見られます。本番の試験では，設問で問われていることを十分に確認した上で，解答を作成するようにしてほしいと思います。

問3 マルウェアの不正侵入対策

【採点基準】

［設問1］

a ～ g は，解答例どおりのみ各 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。単に加害者になるなどの今一歩のものは 3 点。その他は 0 点。

（2）検知方法は，解答例と同等の意味をもつものだけ 2 点。その他は 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 4 点。その他は，基本的に 0 点。

（3）誘導する方法，見分ける方法とも，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 4 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）削除すべきフィルタリングルール，登録すべきフィルタリングルールとも，解答例どおりのみ各 2 点。

（3）プロトコル名，特徴とも，解答例どおりのみ各 3 点。

【講評】

平均正答率は 39.3%（19.6 点）で，ほぼ想定どおりの結果でした。

設問 1 の穴埋め問題の正答率は，それほど高くはありませんでした。日ごろから地道に努力しながら，一つ一つの技術用語を覚えていくようにしましょう。

設問 2 の全体的な正答率は，まずまずでした。さらに，点数をアップさせるには，設問で問われていることを十分に確認した上で，それに対して的確な答案を作成していくことが必要です。例えば，(3)では，興味を引きつけるメールを送信するなどの答案も見られ，HTML メールにおいて不正なサイトに誘導する方法を必ずしも指摘していませんでした。

設問 3 は，全体的に正答率は低かったようです。特に，(2)の登録すべきフィルタリングルールでは，表の注に「プロキシサーバのポートは 80/tcp を使用している」と記載してあるにもかかわらず，80/tcp と 443/tcp の両方を記述し，点数を失っていました。問題の条件を確認し解答を作成しなければ，合格基準点をクリアすることがだんだん難しくなってきます。

問4 セキュアプログラミングの導入検討

【採点基準】

［設問1］

a ～ g は，解答例どおりのみ各 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）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）解答例どおりのみ 4 点。

（3）機能名，攻撃名とも，解答例どおりのみ各 4 点。

【講評】

この問題は，セキュアプログラミングに特化したものですから，選択した受験者は少数でした。

C++では，メモリ境界に関するチェック機構をもたないことや，文字列を終端させるナル文字の扱い方などによって，様々な脆弱性が発生します。例えば，バッファサイズ一杯にデータを書き込んだ際，その最後の文字がナル文字になっていない場合，その文字列を読み出す際には，ナル文字が見つかるまで読み出されてしまい，情報漏えいなどのリスクが発生します。バッファオーバフローだけではなく，こうした基本的な事項は，しっかり把握するようにしましょう。

また，セキュアプログラミングに関しては，IPA から公表されているセキュアプログラミング講座をはじめ，様々な資料を基にして出題されることが多いので，セキュアプログラミングの問題を選択される受験者は，それらの資料を事前に学習しておくとよいでしょう。

＜午後Ⅱ＞

問1 Web システムの脆弱性診断と対策

【採点基準】

［設問1］

（1）解答例どおりのみ 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）解答例どおりのみ 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 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 4 点。その他は，基本的に 0 点。

［設問3］

（1）解答例どおりのみ 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 8 点。その他は，基本的に 0 点。

［設問4］

（1）解答例どおりのみ各 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。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 8 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 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 8 点。内容が今一歩のものは 4 点。その他は 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 8 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 8 点。その他は，基本的に 0 点。

（2）管理体制，理由とも，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。

【講評】

平均正答率は 30.8%で,想定していたものよりも低い結果になりました。

設問 1 の正答率は，全体的に低かったと思います。特に，(2)では，パラメタ偽装を行う目的を問うようにしていましたが，エスケープ処理を逃れるためなどの答案が目立ちました。何が問題となっているかをしっかりと見極めることが必要です。また，(3)では，DNS キャッシュポイズニングの仕組みに対する理解が，まだ十分ではないように思いました。

設問 2 (2)は，一部の受験者を除き，CSRF 脆弱性の対策の理解が不足しているように感じられました。また，(3)は，日ごろからログアウト処理に気を付けていれば，簡単に答えられると思っていましたが，それほど正答率は高くなかったようです。情報セキュリティスペシャリスト試験では，私たちが日常，出くわすような場面を想定した事項を対象として出題されることがあります。日常のセキュリティ問題に対しても，常に意識を高くもつようにしておきましょう。

設問 3 は，プレースホルダの正答率が高くなかったようです。本番の試験でも既に出題されており，基本的な用語となっていますので，覚えておきましょう。

設問 4 は，全体的に正答率が低かったようです。(1)の空欄 h に入れる字句は，難しい用語でしたが，一部の受験者は正解していました。(2)，(5)の正答率は，まずまずだったと思いますが，(6)の正答率は，かなり低かったようです。WAF は，SSL の暗号化を解いた後でなければ，通信内容の検査ができず，フィルタリングできるかどうかの判断ができません。こうした基本的な事項は，問題文の中からしっかりくみ取ってほしいと思います。

設問 5 は，比較的正答率が高かったようです。しかし，(2)の理由は，問題の記述内容から「営業部はセキュリティ意識が弱い」旨を指摘してほしかったと思います。

問2 認証システムの再構築の検討

【採点基準】

[設問1]

(1) 利用者の視点，管理者の視点とも，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。

(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2]

(1) 解答例どおりのみ 3 点。

(2) 権限管理の方法，人事部との役割分担とも，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 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 8 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 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に対し 8 点。その他は，基本的に 0 点。

(2) 解答例どおりのみ各 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 8 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 6 点。その他は，基本的に 0 点。

(2) 登録する情報は，解答例と同等の意味をもつものだけ 5 点。その他は 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。

【講評】

平均正答率は 41.1%で，問 1 よりも高く，選択者数も問 1 よりも多くなりました。

設問 1 の正答率は，まずまずでした。(1)の利用者の視点は，日ごろ行っているアカウント管理の煩わしさを思い浮かべ，素直に解答を作成すればよいのです。本番の試験でも日常の例と同じようなケースが当てはまれば，それを素直に解答するとよいでしょう。

設問 2 の正答率もまずまずだったと思います。しかし，(2)は,解答すべき内容をもっと分かりやすい表現で記述するように改善していきましょう。また，(3)は，「統合 ID システムがアカウント情報を配信する」という指摘にとどまり，それがどのような効果をもたらすかを指摘していなかったり，「マスタ DB で認証を行っている」と誤解していたりするようなものも見られました。本番の試験では，全体の関係をよく整理した上で，解答を作成していくことがポイントになります。

設問 3 は，全体的に正答率が低かったようです。(2)のクッキーの属性については，二つとも正解している答案は少なかったと思います。合格を目指すには，技術的な仕組みも，しっかり把握していくことが必要です。

設問 4 (1)の正答率は高かった半面，(2)は低かったようです。ディジタル署名の検証を行うには，何が必要になるかについて，十分に把握しておきましょう。

以上