2012 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

2012 年 9 月 21 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 48.1 点，午後Ⅱが 34.2 点でした。問題別では，午後Ⅰの問 1 が 25.7 点，問 2 が 17.5 点，問 3 が 25.4 点，問 4 が 24.0 点で，問 2 の平均点が最も低くなりました。また，午後Ⅱは，問 1 が 33.9 点，問 2 が 35.9 点でした。2012 年春期の公開模試では，午後Ⅰの平均点が 35.8 点，午後Ⅱの平均点が 29.8 点であったことを考慮すると，午後Ⅰ，午後Ⅱともかなり上回っていますが，特に午後Ⅰの平均点の向上が顕著で，想定していたよりもよい結果だったと思います。

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（ログ管理）の選択者が 32.4%，問 2（シングルサインオンと認証強化の検討）が 16.3%，問 3（人的要因による情報漏えい対策）が 42.6%，問 4（セキュアプログラミング）が 8.7%であり，大半の受験者が問 3 を選択していたことになります。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技術力が，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（情報セキュリティ監査）の選択者が 80.7%，問 2（モバイル環境のセキュリティ）が 19.3%という比率でした。なお，午後Ⅱ試験は，様々な分野から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 ログ管理

【採点基準】

[設問1]

（1）a 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各 6 点。その他は，基本的に 0 点。

[設問3]

（1）b 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 8 点。要因が適切に指摘されていないものなどは 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 6 点。その他は，基本的に 0 点。

【講評】

平均点は 25.7 点（平均正答率は 51.4%）であり，ログ管理における基本的な知識は，しっかり身に付いているものと思われます。

設問 1 (2)の正答率は，必ずしも高くはありませんでした。ログの時刻同期を行っておくことは，ログ分析における基本事項です。しかし，「ログを時系列で追うことが可能」など，指摘内容が不十分なものが幾つか散見されました。

設問 2 は，比較的正答率が高かったので，これ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 (2)の設問の指示は，「ログの調査ができなかった要因も含めて」です。このため，問題文の記述内容に基づいて，「仮想サーバを再起動するとログデータが消失する」という要因を指摘することが必要です。

問2 シングルサインオンと認証強化の検討

【採点基準】

[設問1]

(1) a，b は，解答例どおりに対し各 2 点。

(2) c 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各 4 点。その他は，基本的に 0 点。

(4) 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。ドメイン名は，解答例どおりに対し 2 点。

(5) 方式名は，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 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) d，e は，解答例どおりに対し各 1 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 17.5 点（平均正答率は 35.1%）と，午後 I の 4 問の中では，最も低い点数でした。クッキーに関する技術知識や，リスクベース認証の考え方など，技術内容を問うものが多かったことが，その要因でしょう。

設問 1 (1)の空欄 b や(2)の正答率はあまり高くなかったようです。利用者の権限に基づいてシステムを利用できる範囲を制御することを Authorization（認可又は許可）といいます。これに関連し，3A や 4A についても理解しておくとよいでしょう。(4)では，クッキーが送信される条件について，もう一度，よく整理しておきましょう。(5)は，問題の記述内容に基づいて，理由が述べられていたので，正答率は高かったと思います。その半面，(6)は，可用性の意味がよく理解されていないようであり，「処理が集中した場合，レスポンスが悪化する」などの答案が幾つか見られました。可用性とは「認可されたエンティティが要求したときに，アクセス及び使用が可能である特性」ですから，SSO サーバが故障すると，Web アプリが使用できなくなることを指摘することが必要です。

設問 2 は，解説などをよく読んで，リスクベース認証についての理解を深めておくとよいでしょう。

問3 人的要因による情報漏えい対策

【採点基準】

[設問1]

(1) 人的ミスは，解答例どおりに対し 2 点。損失金額は，解答例どおりに対し 5 点。

(2) a は，「ファイルを誤って添付する」旨が適切に指摘されているものに対し 6 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) b ～ d は，解答例どおりに対し各 3 点。

(2) 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 6 点。その他は，基本的に 0 点。

(3) OS，アプリとも，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】

平均点は 25.4 点（平均正答率は 50.7%）であり，問 1 とともに，高い正答率でした。

設問 1 の(1)，(2)は，比較的正答率が高かったといえますが，損失金額の計算ミスも見られました。確実に得点できる設問では，点数を失わないことが重要です。

設問 2 は，解答を導くためのヒントが問題文に記述されているわけではないので，正答率が低くなると想定していました。しかし，(1)は「情報端末の棚卸（存在確認）

を定期的に行う」こと，(2)では「作業を 2 人で行う」ことなど，基本的な確認作業の方法について，うまく指摘されていたと思います。

設問 3 (1)では，空欄 b の正答率が低かったようです。「NPC 内の情報を収集して攻撃者に送信する」という修飾語からスパイウェアを選択したのではないでしょうか。しかし，この修飾語の前には「リモートから受けた指令に従って」という条件がありますので，もっと全体的な関係を把握しながら，選択する字句を考えることが必要です。これに関連し，下線部分に関する記述式の問題に取り組む際にも，同様な注意が必要です。例えば，下線の部分だけに着目して解答を作成しようとする傾向が多いので，下線の前後に記述されている文章，あるいは全体的な記述内容から考察していけば，より適切な解答を導くことができるはずです。本番の試験では，もう少し全体的な関係を念頭に置きながら解答を作成していくようにしましょう。

問4 セキュアプログラミング

【採点基準】

[設問1]

(1) 攻撃名は，解答例どおりに対し 4 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 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。その他は，基本的に 0 点。

[設問2]

(1) 解答例と同じ意味をもつものに対し 4 点。

(2) a は，解答例又は「prepareStatement」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 6 点。その他は，基本的に 0 点。

(4) 解答例どおりに対し 4 点。

(5) 対策，効果とも，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 24.0 点（平均正答率は 48.1%）でした。基本的な問題が多いこともあって，まずまずの出来であったといえます。

設問 1 (1)が正解にもかかわらず，設問 2 (1)が正解できていないケースが，かなりありました。プレースホルダ（バインド機構）は，SQL インジェクション対策の基本ですから，十分に理解しておいてほしいと思います。また，セキュアプログラミングの問題を選択される受験者は，実務でもそれらに携わっている方が多いと思いますので，IPA セキュリティセンタから公表されているセキュアプログラミング講座などの資料は，実務でも役立つはずです。よく学習されることをお勧めします。

＜午後Ⅱ＞

問1 情報セキュリティ監査

【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 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。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3]

「情報区分のラベルが付与されていない」，「情報セキュリティ教育の効果が不十分である」旨が指摘されているものに対し各 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 8 点。その他は，基本的に 0 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 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 6 点。その他は，基本的に 0 点。

[設問5]

(1) 解答例どおりに対し各 3 点。

(2) d 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。

(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 0 点。

(5) 解答例どおりに対し 2 点。

[設問5]

「マネジメントレビューを実施する」，「改善措置の実施を決定する」旨が適切に指摘されているものに対し 8 点。いずれか一方の指摘にとどまっているものは 4 点。その他は 0 点。

【講評】

前半は ISMS 関連，後半は技術的な内容に重点を置いた問題でしたから，平均点は 33.9 点と，問 2 よりも少し低い点数にとどまりました。

情報セキュリティ監査をはじめ，監査では決められた

ルールに則り，様々な手続きが実施されているかどうかを中心にチェックしていくことになります。このため，設問 2 (1)では，入退館カードが決められたとおりに使用されているか，あるいはその保管が問題なく行われているかなどを含めて実施すべきです。こうした点を分かりやすく指摘してほしかったと思います。

設問 3 では，Y 社の情報セキュリティ上の問題点を指摘した答案が散見されましたが，ここでは監査の立場からの指摘事項を答えることが必要です。本試験では，設問で何が問われているのかを必ず確認し，問題点を指摘すればよいのか，あるいは問題の対策を答える必要があるのかなど，設問で問われていることに素直に解答していくことが必要です。

設問 4 (1)の正答率は，高かったものの，(2)～(4)の正答率は低かったようです。(2)の空欄 c のように適切な字句を入れるものは，基本的に一つの用語を答えることが基本ですから，「公開鍵と秘密鍵」というように二つの用語を答えないようにしましょう。(3), (4)についても，解説をよく読んで，こうした内容も考慮する必要があるということを理解しておけばよいでしょう。

設問 5 は，ネットワークセキュリティの問題でしたから，全体的に正答率は良くなかった半面，設問 6 は，比較的良かったと思います。

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。

問2 モバイル環境のセキュリティ

【採点基準】

[設問1]

(1) a ～ h 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。

[設問2]

(1) 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) 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) j，k 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 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。

[設問4]

(1) l ～ n は，解答例どおりに対し各 2 点。
(2)「プローブ要求フレームを盗聴すれば SSID が分かる」などを指摘したものに対し 6 点。その他は，基本的に 0 点。
(3)「DMZ の DNS サーバ」と「インターネット側への通信」の 2 点が適切に指摘されているものに対し 8 点。「インターネット側への通信」だけを指摘したものは 4 点。その他は 0 点。
(4) 機密性，完全性とも，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 35.9 点と，問 1 よりも若干，高くなりましたが，決して満足できるような点数ではありません。

設問 1 (1)は，無線 LAN のセキュリティにおける基本的な用語ですから，多くの設問に正解できるようにしておくとよいでしょう。(2)は，暗号文とキーストリームの XOR をとれば，元の平文に戻るというものです。こうした事例を見れば，共通鍵暗号方式の処理速度が極めて速いことが理解できるでしょう。

設問 2 (1)は，1,024 ビットの RSA を使用した場合，通信データの暗号に使用するアルゴリズムの強度が幾ら高くても解読されるリスクがあるのはなぜかという問題です。SSL では，暗号化に使用する共通鍵の情報が 1,024 ビットの RSA で送信されるので，これが脆弱性の原因となります。記述式の問題では，設問で問われていることの本質を考えて解答を作成しましょう。

設問 3 は，ほかの設問に比べると，正答率は若干，高かったようです。これからは，モバイル環境のセキュリティが重要になってくるので，できるだけ多くの事例を会得しておくとよいでしょう。

設問 4 (4)ので解答内容を見ると，機密性と完全性の意味がよく理解されていないのではないかと思われます。この際，基本的な用語の意味は十分に把握するようにしましょう。

なお，午後Ⅱ試験では，問題の記述内容を理解し，設問で問われていることに的確に対応していくことが必要です。本試験では問題の条件などを十分に考慮しながら解答を作成することを忘れないようにしましょう。

以上