2011 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

2011 年 3 月 18 日 (株)アイテック 商品開発本部

■ 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 45.2 点，午後Ⅱが 34.7 点でした。問題別では，午後Ⅰの問 1 が 25.9 点，問 2 が 13.7 点，問 3 が 28.5 点，問 4 が 14.0 点で，問 1，問 3 の平均点は，問 2，問 4 の 2 倍近くなりました。一方，午後Ⅱは，問 1 が 35.0 点，問 2 が 34.4 点で，問題間の相違はありませんでした。2010 年秋期の公開模試では，午後Ⅰの平均点が 36.9 点，午後Ⅱの平均点が 35.2 点であったことを考慮すると，午後Ⅰの平均点が，大きく向上したといえます。今回は，午後Ⅰの問 1 と問 3 が比較的得点しやすかったことなどが，その理由であると考えられます。

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のではないか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ってほしいと思います。また，記述式の問題において，項目を複数，羅列した答案も見られましたが，こうした解答方法は避ける必要があります。それは，情報セキュリティスペシャリスト試験などの記述式問題では，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ることが多いからです。このため，項目を複数挙げるのではなく，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を解答しても，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（TCP/IP の脆弱性対策）の選択者が 27.5%，問 2（データベースのセキュリティ対策）が 27.7%，問 3（指紋認証によるセキュリティ対策）が 38.3%，問 4（シンクライアントの導入とプログラム開発）が 6.5%であり，少し偏りがありました。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あげることが必要です。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（ネットワークのセキュリティ）の選択者が 48%，問 2（Web アプリケーションの開発と運用）が 52%という比率でした。午後Ⅱ試験では，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 問ともに手をつけて，かえって失敗しまいます。

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に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。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 TCP/IP の脆弱性対策

【採点基準】

［設問1］

（1）a ～ c は，解答例どおりのみ各 2 点。

（2）解答例と同様の趣旨（正常なユーザも接続しにくくなる旨の字句）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 は，解答例どおりのみ 2 点。

（2）SYN クッキーと ACK パケットの確認応答番号－1 が同一という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。
(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。内容が今一歩のもの（パケット数を制限する帯域制御など）は 3 点。その他は 0 点。

［設問3］
(1) e，f は，解答例どおりのみ各 2 点。
(2) g ～ i は，解答例どおりのみ各 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。内容が今一歩のものは 3 点。その他は 0 点。

【講評】

平均点は 25.9 点（平均正答率は 51.7%）であり，想定していたよりも，高くなりました。設問 1 の正答率が良かったことが，その要因と考えられます。

設問 1 の正答率が良かったので，TCP の通信方式については，よく理解されていると思われます。試験で必要となる技術知識については，こうした基本的な知識の積み重ねとなります。本番の試験日まで，できるだけ多くの技術知識の詳細をしっかり身に付けていくようにしましょう。

設問 3 は，ルーティングプロトコルの BGP に関する技術知識が必要ですから，正答率は全体的に低かったように思います。改善すべき点としては，(3)の記述式の問題が挙げられます。答案の中には「不要な経路情報を送信しない」旨を指摘したものがありましたが，これは問題文に記述された内容です。一般に，問題文に記述された内容をそのまま記述した場合には，正解にならないことが多いので，どうしても解答を作成できない場合の最後の手段とするようにしましょう。

問2 データベースのセキュリティ対策

【採点基準】

［設問1］
(1) a は，解答例どおりのみ 2 点。
(2) b は，バックアップというキーワードが指摘されているものに対し 4 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 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各 4 点。その他は，基本的に 0 点。

［設問3］
(1) d は，解答例どおりのみ 2 点。
(2) 選定したツールは，解答例どおりのみ 2 点。理由は，解答例と同様の趣旨（営業所が独自作成した DB も管理できる旨）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。

【講評】

平均点は 13.7 点（平均正答率は 27.3%）と，午後 I の 4 問の中では，最も低い点数でした。本問は，問題の記述内容を十分に把握しながら解答を作成していく必要がある問題でしたから，全体的に正答率が低くなったものと思われます。

設問 1 (2)は，正答率はかなり低かったようです。それは，表 1 の「DB 管理機能を使用」という手口だけに着目し，表 2 の内容を確認しなかったからではないでしょうか。もう少し全体的な関係をよく把握して解答を作成していく必要があると思われます。

設問 2 (1)，(2)は，逆総当たり攻撃を理解していることなどが必要ですから，正答率が低くなることは想定していました。その半面，(3)の正答率は高くなると思っていましたが，必ずしもそうではありませんでした。問題の記述内容を十分に把握することが必要だと思われます。

設問 3 も，問題の記述内容が少し複雑でしたから，全体的に正答率が低くなったと考えられます。

問3 指紋認証によるセキュリティ対策

【採点基準】

［設問1］
(1) a ～ c は，解答例どおりのみ各 2 点。
(2) d，e は，解答例どおりのみ各 3 点。
(3)「他人受入率が高くなり，なりすましのリスクが大きくなる」旨が適切に指摘されているものに対し 6 点。「他人受入率が高くなる」ことだけを指摘したものなどは，基本的に 0 点。

［設問2］
(1) f は，解答例どおりのみ 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) 解答例どおりのみ 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 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 3 点。その他は 0 点。
(2) g は，解答例どおりのみ 2 点。ただし，セキュリティなどの同様の意味をもつ字句でもよい。

(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，基本的に 0 点。

【講評】

平均点は 28.5 点（平均正答率は 56.9%）と，午後 I の 4 問の中では，最も高くなりました。問題の記述内容が比較的分かりやすかったことなどから，解答を作成しやすかったのではないでしょうか。

問 2 と問 3 を比較して評価すると，問題の記述内容が複雑かどうかの違いが，そのまま正答率が高いか低いかの違いになっているといえます。そこで，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ことが必要です。そのためには，技術力のほか，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ことが必要であると考えられます。

問4 シンクライアントの導入とプログラム開発

【採点基準】

[設問1]
(1) a ～ c 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) d は，解答例どおりのみ 2 点。発生するエラーは，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) 解答例どおりのみ 4 点。その他は 0 点。
(3) 解答例どおりのみ 6 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 6 点。その他は，基本的に 0 点。

[設問3]
(1) f，g 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。

【講評】

平均点は 14.0 点（平均正答率は 28.1%）であり，問 2 に続いて低い点数になりました。なお，選択者数は，4 問の中で最も低い問題でした。問題の後半部分が，セキュアプログラミングの問題であったことから，選択する受験者が少なかったものと思われます。

設問 1 (1)の正答率は高かったものの，(2)，(3)の記述式の問題の正答率は，低かったように思われます。

設問 2，3 も，全体的に正答率は低かったように思います。こうしたことからも分かるように，セキュアプログラミングに精通していない場合には，選択する問題から外すことが必要になります。このため，選択する問題の範囲を 4 問ではなく，あらかじめ 3 問に絞った上で，2 問を選択する方法も考えておくとよいでしょう。

＜午後Ⅱ＞

問1 ネットワークのセキュリティ

【採点基準】

[設問1]
(1) a，b は，解答例どおりのみ各 3 点。
(2) c，d は，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2]
(1) e は，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3]
(1) f ～ 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 10 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 10 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) 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5]
(1) i は，解答例どおりのみ 2 点。
(2) c，d は，解答例どおりのみ各 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 10 点。内容が今一歩のもの（ロードバランサで SSL の処理を行うことだけで，IPS の機能などを指摘していないもの）は 5 点。その他は 0 点。

【講評】

技術的に難度の高い設問が一部あったことなどから，全体的に正答率は低く，平均点は 35.0 点でした。なお，問題の選択率は，問 1 と問 2 との間には大きな差異はありませんでした。

設問 1 (1)，(2)の正答率は低かったようですが，(3)の正答率は高かったようです。なお，公開鍵暗号方式を利用した暗号化メールの方式には，S/MIME と PGP の二つがあること，並びにそれらの仕組みについては十分に理解しておいてほしいと思います。

設問 3 (1)は，専門知識が必要な字句でしたが，正答率は，比較的高かったように思います。その半面，(2)の正答率は，低かったようです。キャッシュサーバに古い ZSK の DNSSEY レコードがキャッシュされていることが基本の問題ですから，この点に気付いてほしかったと思います。

設問 4 は，全体的に正答率が低かったようです。メールの本質的な仕組みは，十分に理解しておく必要があると考えられます。

問2 Web アプリケーションの開発と運用

【採点基準】

［設問1］

(1) a，b は，解答例どおりのみ各 3 点。

(2)「他人の通信を盗聴し，そのセッション ID を再利用すること」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) c 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。

(4) 変更する画面は，解答例どおりのみ 2 点。d 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。

［設問2］

(1) e は，解答例どおりのみ 2 点。

(2) 方法，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 6 点。その他は，基本的に 0 点。

(3) 方法は，解答例どおりのみ 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。

［設問3］

(1) 解答例どおりのみ各 2 点。ただし，問合せ用，確認用，情報提供用の三つを解答した場合は減点対象なので，全体で 2 点としました。

(2) 解答例と同様の趣旨（少なくともディジタル署名を添付する旨）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) f，g は，解答例どおりのみ各 2 点。

(2) h は，解答例どおりのみ 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。

(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。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各 6 点。その他は，基本的に 0 点。

【講評】

平均点は 34.4 点であり，問 1 よりも若干，低くなりました。

設問 1 (1)，(3)，(4)の正答率は，比較的高かったように思いますが，(2)の正答率は，低かったようです。(2)は，問題文を読めば，社内は HTTPS による暗号化が行われていないことが分かるので，セッション ID が盗聴される点に着目し，解答を作成してほしかったと思います。下線部だけに着目するのではなく，全体的な関係を考慮しながら解答を考えることが必要です。

設問 2 は，全体的に正答率が低かったようです。このうち，(2)は，問題の記述内容から解答を導いていくことが難しいので，正解を得ようと考えるならば，日ごろから情報セキュリティに関する知識レベルを高めておくことが必要です。

設問 3 も，全体的に正答率が低かったようです。中でも，(2)の正答率は少し高くなると想定していましたが，記述内容の関係を十分に把握できなかったためか，S/MIME で行われるディジタル署名の検証を指摘した解答が少なく，C 社の公開鍵証明書を送付する旨の解答が多かったように思います。公開鍵証明書を送付するだけでは，送信元の真正性を確認することになりません。ディジタル署名の検証については，十分に理解されていると思います。このため，問題の記述内容が少し複雑になったとしても，本質をしっかり捉え，的確な解答を作成していくようにしてほしいと思います。

設問 4 は，ほかの設問に比較すると，正答率が少し高かったように思いますが，(5)については，問題の条件を十分に考慮すれば，もっと正答率が良くなったと思われます。

いずれにしても，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ように心掛けましょう。

以上