2014 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

2014 年 3 月 20 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 40.5 点，午後Ⅱが 32.7 点でした。問題別では，午後Ⅰの問 1 が 22.9 点，問 2 が 19.1 点，問 3 が 17.2 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 29.0 点，問 2 が 36.2 点でした。2013 年秋期の公開模試では，午後Ⅰの平均点が 42.1 点，午後Ⅱの平均点が 32.1 点でしたから，午後Ⅰは若干低下，午後Ⅱはほぼ同程度という結果になりました。

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（Web 販売サイトの認証強化）の選択者が 49.5%，問 2（Web アプリケーションの脆弱性対策）が 10.3%，問 3（インシデント対応）が 40.2%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，午後Ⅰ試験で出題される問題数は 3 問ですから，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（スマートデバイスを用いたシステム開発）の選択者が 47.2%，問 2（ディザスタリカバリシステムの構築）が 52.8%で，ほぼ半々という比率でした。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 Web 販売サイトの認証強化

【採点基準】

[設問1]

（1）解答例どおりに対し 3 点。

（2）解答例どおりに対し 3 点。

[設問2]

（1）解答例どおりに対し 3 点。

（2）アカウントロック，二要素認証とも解答例どおりに対し各 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）解答例と同様の趣旨（メールで通知すること）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。

（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。「失効した証明書の CRL を発行する」などの指摘は 3 点。その他は 0 点。

[設問3]

（1）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。
(3) 解答例と同様の趣旨，あるいは「第三者からの問合せにはパスワードを答えない」旨の指摘に対し 6 点。「当社からパスワードを問い合わせることはない」旨の指摘は 3 点。その他は 0 点。

【講評】

平均点は 22.9 点（平均正答率は 45.9%）であり，パスワードの管理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，及び設問 2 (1)は，想定していたよりも正答率が低かったように思います。設問 1 (1)の User-Agent については，専用用語を知っているかどうかの問題ですが，設問 1 (2)，設問 2 (1)は，クライアント認証を行う上での基本的な知識問題です。クライアントにインストールする必要があるものは，クライアント証明書（クライアントの公開鍵証明書）とクライアントの秘密鍵です。そして，クライアントの秘密鍵を用いて作成されるものはディジタル書名ですが，メッセージダイジェスト（ハッシュ値）などの誤答が目立ちました。クライアントで作成したメッセージダイジェストを秘密鍵によって暗号化することが署名という行為に当たります。こうした基本的な知識はしっかり理解しておきましょう。

設問 2 (2)も，比較的正答率は低かったようです。選択肢の中から該当するものを全て選ぶ問題は，注意深く条件に合致しているかどうかを考察していくようにしましょう。(3)～(5)の記述式の問題は，まずまずの正答率でした。しかしながら，(5)については A 社自身が発行したクライアント証明書の取扱いに関する設問です。このため，クライアント証明書が自己認証局で発行したものか，第三者機関の CA から発行されたものかを区別して考えることが必要でしたが，ユーザ自身が第三者認証局に対して行うべき行為を述べたような答案が多く見られました。

設問 3 は，パスワードの管理に関するものでしたから，正答率は，ほかの設問に比べると高かったようです。

問2 Web アプリケーションの脆弱性対策

【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) COUNTRY，STREET とも，解答例どおりに対し各 4 点。
(2) 解答例どおりに対し 4 点。その他は 0 点。
(3) d，f とも，解答例どおりに対し各 2 点。
(4) 解答例，又は「バインド変数」に対し 3 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 4 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。

【講評】

平均点は 19.1 点（平均正答率は 38.2%）でしたが，セキュアプログラミングの経験者と，そうでない受験者で点数に大きな差があったものと思われます。

設問 1 (1)の穴埋め問題は，用語を正確に覚えていることが必要でしたから，正答率は低かったようです。(2)は比較的，正答率は高かった半面，(3)の正答率は低かったと思います。多くの答案は，下線②だけに着目して解答を作成したものと考えられますが，下線②の後に続く「WAF と合わせて適用する」ことと関連付けて考えれば，Web アプリケーションの脆弱性が修正できない点に気付くことができたのではないでしょうか。

設問 2 (1)は，論理的に考えて正解を導いてほしかった問題ですが，正答率は思ったほど高くはなかったようです。また，(4)の空欄 e に入れるプレースホルダの正答率も意外に低かったようです。SQL インジェクション対策として，プレースホルダを用いることはよく知られている方法の一つですから，十分に理解しておいてほしいと思います。

平成 25 年度秋期試験から午後 I 試験の出題数が 4 問から 3 問に減少しました。このため，以前はセキュアプログラミングの問題を選択対象から外してもほとんど影響がありませんでしたが，これからはやむを得ずセキュアプログラミングの問題を選択せざるを得ないことも出てきます。受験対策としては，セキュアプログラミングの分野にもできるだけ注力していかざるを得ないと考えられます。

問3 インシデント対応

【訂正とお詫び】

解答用紙の設問 3 (1)の解答欄において，b，c，d，e とすべきところを，b，c，d，d にしてしまいました。受験者の方々には大変なご迷惑をおかけすることになり，改めてお詫び申し上げます。

【採点基準】

［設問1］

リアルタイムスキャン，フルスキャンとも，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。

［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 4 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。指摘内容が今一歩のもの（IP アドレスが使用されているなど，状況の指摘になっているもの）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。状況の指摘にとどまっているものなどは 3 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。指摘内容が今一歩のもの（IPS に代えて IDS を導入するなどを指摘したものなど）は 3 点。その他は 0 点。

［設問3］

(1) b ～ e は，解答例どおりに対し各 2 点。

(2) 問題，対処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 6 点。その他は，基本的に 0 点。

【講評】

平均点は 17.2 点（平均正答率は 34.5%）にとどまり，午後 I の 3 問の中では，最も低い点数でした。

設問 1 のリアルタイムスキャン，フルスキャンとも正解した答案は，極めて少数だったと思います。これを機にスキャン方法の基本的な知識を身に付けておくとよいでしょう。

設問 2 では，(2)，(3)の正答率が低かったようです。例えば，(3)では「GET メソッドを伴わずに POST メソッドを送信している」などのように，問題文の記述内容をそのまま引用しているような答案が少なからず見受けられました。問題文を単に引用しただけでは正解には至らないことが多いので，もう少し踏み込んで考える習慣を身に付けるようにしましょう。

設問 3 は，技術的な内容の問題でしたから，全体的に正答率は低かったようです。また，(2)は，Z 社がメールを受信するときの問題なのか，Z 社からメールを送信するときの問題なのかの区別ができていなかったような答案が多く見られました。問題をよく読んで，どのような状況の下で，何が問われているかを明確にした上で解答を作成するようにしましょう。

本問もそうですが，一般に技術絡みを中心とした問題の正答率は低いと思われます。技術知識のレベルアップを図って，本番の試験に臨むようにしましょう。

＜午後Ⅱ＞

問1 スマートデバイスを用いたシステム開発

【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) 有効となる手口，入力情報が盗まれる手口とも，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。

(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（端末識別番号によって，両サイトの情報を紐付ける旨）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。

［設問2］

(1) 解答例と同様の趣旨（セキュアコンテナ機能を ON にする旨と，許可するアプリをアプリリストに登録する旨）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 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3］

(1) 下線⑦の理由，下線⑧の理由とも，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 8 点。指摘内容が今一歩のものは 4 点。その他は 0 点。

(2) 解答例どおりに対し 2 点。

(3) 名称は，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。指摘内容が今一歩のものは 3 点。その他は 0 点。

［設問4］

(1) 解答例どおりに対し 4 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】

問 1 の平均点は 29.0 点で，問 2 よりも少し低い点数でした。これは，問 2 と共通する事項ですが，問題文を表面的にしか読み取っていない，問題の条件設定がどのようになっているかなどの把握が十分になされていない，自身の知識だけから解答を作成しようとする傾向が強いなどといった事項が大きく影響しているものと考えられます。

設問 1 (2)のクッキー情報を窃取する手口については典型的な例を覚えておくとよいでしょう。(3)は，データを暗号化する，あるいはハッシュ化するなどの答案も見られましたが，問題の条件設定はどのようになっているかをよく考えるようにしましょう。(4)は，想定以上に正答率は良かったと思います。

設問 2 (1)では，設定や登録する内容を問うていましたが，制限する方法を答えていたものが多く見られました。本番の試験では，設問で何が問われているかを必ず確認するようにしましょう。(2)は，留意すべき事項が指摘されず，状況を単に説明したものが多く見られましたので，こうした点も改善するようにしましょう。

設問 3 は，技術絡みの問題でしたから，全体的に正答率は低かったようです。特にソルトについては，まだ十分に理解されていなかったようですから，解説をよく読んで理解を深めておくとよいでしょう。

設問 4 の(1)は，レビュー報告書という字句が思い浮かばなかったようで，正答率は低かったと思います。

問2 ディザスタリカバリシステムの構築

【採点基準】

[設問1]

(1) 要件は，解答例どおりに対し 3 点。理由は，解答例と同様の趣旨（RPO の 60 分を実現できない旨のキーワードが必要）が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) 解答例と同様の趣旨（通信データの暗号化）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 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。「通信帯域を圧迫し，レスポンスが遅くなること」などを指摘したものは 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。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。「両方とも被災する」，「両方ともダウンする」などを指摘したものは 3 点。「両方とも都内にある」など，状況だけを指摘したものは 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) メリット，利用方法とも，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各 6 点。その他は，基本的に 0 点。

(4) ファイアウォールのルールは，送信元，宛先，ポート番号，動作の四つとも正しい場合に限り，各 4 点。ポート番号を二つ答える必要があるものについて，一つしか答えられていない場合には 2 点。逆にポート番号が一つのところに対し，二つ以上答えている場合には 0 点。

[設問4]

(1) 問題，変更内容とも，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 6 点。その他は，基本的に 0 点。

(3) 不十分な点，追加した手順とも，解答例と同様の趣旨が適切に指摘されているものに対し各 6 点。その他は，基本的に 0 点。

【講評】

問 2 の平均点は 36.2 点となり，問 1 よりも高い点数でした。しかし，記述式の問題では，問題の記述内容をそのまま引用し，状況説明にとどまっているものも多く見られ，問 1 と同様，点数を失っていました。

設問 1，設問 2 は，全体的にまずまずの正答率だったと思われます。

設問 3 の(1)では，プライマリとセカンダリの両方とも都内にあるなどの状況を説明したものも見られました。ここでは，広域災害が発生したときの具体的な問題とは何かを，もう少し考察してほしかったと思います。(2)は DNSSEC の技術的な仕組みを問うものでしたが，正答率は低く，技術の具体的な仕組みに関する理解をもっと深めていく必要があると思われます。(3)も正答率は低くかったようで，メリットについては，メールが PC に保存されないので，情報漏えいにつながりにくいということに気付いてほしかったと思います。(4)のルールについては，問題の条件を考慮しながら，解答が作成されていると見受けられました。記述式の問題に対しても，同じように条件などを加味しながら解答を作成する習慣を身に付けてほしいと思います。

設問 4 も，全体的に正答率は良くなかったです。(1)の変更内容は，Web-2 サーバではなく，DNS-2 サーバへの接続を拒否することがポイントです。

なお，本番の試験で合格基準点をクリアするには，問題の記述内容をベースにしながら，しっかり考え，正解を導いていくことが必要です。技術知識に加え，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