2015 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

2015 年 3 月 18 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 42.0 点，午後Ⅱが 36.5 点でした。問題別では，午後Ⅰの問 1 が 25.4 点，問 2 が 13.2 点，問 3 が 18.1 点で，問題ごとの平均点にかなりの差が見られました。また，午後Ⅱは，問 1 が 32.3 点，問 2 が 38.5 点でした。2014 年秋期の公開模試では，午後Ⅰの平均点が 35.4 点，午後Ⅱの平均点が 32.8 点でしたから，平均点で評価すると，午後Ⅰ，午後Ⅱともにかなり向上したといえます。

採点結果から受けた印象としては，記述式の設問では，下線部にだけ注目しそれに関することを取り上げて解答を作成していたり，設問で指示されていることにあまり従わず，各自がも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たりす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，合格するための基本条件となります。本番の試験では，こうした事項については改善していかなければなりません。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。こうしたケースでは，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，問 1（マルウェア攻撃への対策）の選択者が 47%，問 2（プライベートクラウドの導入とプログラム開発）が 11.4%，問 3（社内ネットワークのセキュリティ）が 41.6%で，多くの受験者が問 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試験は，問 1（Web システムのインシデント対応）の選択者が 40.5%，問 2（電子メールのセキュリティ）が 59.5%で，約 2 対 3 という比率で問 2 の選択者が多くなりました。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，かえって失敗することになってしまいます。

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察していけば正解を導き出すことができます。しかし，受験者によっては問題文の記述内容をそのまま引用して解答を作成している例も多く見られます。単なる引用では正解になることは極めて少ないので，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論理的に考えていくようにしましょう。

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 マルウェア攻撃への対策

【採点基準】

[設問1]

（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。FW で HTTTS 通信を遮断している旨を指摘したものは，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）解答例どおりに対し 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) 解答例どおりに対し 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各 4 点。その他は，基本的に 0 点。
(5) a ～ c は，解答例どおりに対し各 2 点。
(6) 解答例どおりに対し各 3 点

【講評】

平均点は 25.4 点（平均正答率は 50.8%）でした。午後 I の 3 問の中では，平均点が最も高く，選択者数も最も多い問題でした。

設問 1 は，全体的に正答率が高かったようです。URL フィルタリングのブラックリストやホワイトリストによる制御方法については，よく理解されていると感じられました。

設問 2 (1)～(3)の正答率は，かなり低かったと思います。営業秘密の不正な取得や使用などは，不正競争防止法において禁止されています。情報セキュリティに関する基本的な用語については，正確に覚えておくとよいでしょう。SPF については，最近の試験でよく出題されるテーマになっています。どのような仕組みによって送信ドメイン認証が実現されているのかといった点までしっかりと把握しておくとよいでしょう。(3)の RLO 攻撃については，“exe”と“pdf”という文字単位で入れ替えた答案が多く見られましたが，RLO では一文字ずつ左右が入れ替えられていくことに注意することが必要です。

設問 2 (4)は，問題の記述内容を把握しながら解答を作成すれば，比較的やさしい設問であると考えていましたが，問題の記述内容だけを抜き出した答案が，幾つか散見されました。問題の記述内容を基に解答を作成することは重要なことですが，何がポイントになっているかをしっかりと見極めた上で，必要なキーワードを的確に指摘するようにしましょう。(5)は，空欄 c の正答率が少し低かったようです。(6)は，社外メールサーバを指摘したものが見られましたが，ウイルスチェックは，一般に社内メールサーバで実施する方が効果的です。

問2 プライベートクラウド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。

［設問2］

(1) d，e は，解答例どおりに対し各 3 点。
(2) f，g は，解答例どおりに対し各 3 点。
(3) 解答例どおりに対し 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。

［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。

【講評】

平均点は 13.2 点（平均正答率は 26.5%）でした。問題の選択上，問 2 を選択せざるを得ない受験者もいたと感じられました。この結果，午後 I の 3 問の中では最も低い点数となりました。

午後 I 試験の出題数は 3 問ですから，本番の試験でもセキュアプログラミングが含まれる問題を選択せざるを得ないケースが考えられます。その際の準備としては，IPA が公開している「セキュア・プログラミング講座」，「安全なウェブサイトの作り方」，「安全な SQL の呼び出し方」，「セキュアな Web サーバの構築と運用」などの資料を事前に学習しておくことが必要です。しかし，これらの資料を短期間でマスターすることは大変ですから，長期的に取り組んでいく方がよいでしょう。また，プログラミング言語についても，コードで記述された内容を理解できるようにしておくことも必要です。

問3 社内ネットワークのセキュリティ

【採点基準】

［設問1］

a は，解答例どおりに対し 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 4 点。その他は，基本的に 0 点。
(2) アクセスの例，制御方法とも，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 4 点。その他は，基本的に 0 点。
(3) 通信制御は，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。

［設問3］

(1) b は，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。指摘内容が今一歩のものは 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 4 点。その他は，基本的に 0 点。
(5) c は，解答例どおりに対し 2 点。
(6) 方式は，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。

【講評】

平均点は 18.1 点（平均正答率は 36.3%）でした。想定していた平均点よりは，低い点数にとどまったという感じがしました。

設問 1 の正答率は，高くありませんでした。ネットワークセキュリティに関する技術用語などについては，正確に覚えておくことが必要です。

設問 2 (1)，(2)の正答率も高くなかったと思います。(2)については，表 1 のアクセス元とアクセス先を明確にしながら考えていけば，正解を導いていくことができるはずです。問題の条件に従って考察していく設問については，受験者の多くが弱点をもっているように感じられます。これらの設問については，できるだけ正答率を高めていくことが必要ですから，4 月の本試験に向けて強化していってほしいと思います。その半面，(3)は，各部のネットワーク機器からシステム部の PC へ trap 情報が送られることについては，比較的正答率が高かったようです。少しでも考える要素が要求される設問については，正答率が低く，問題の記述内容をそのまま引用すれば正解が得られるような設問は，正答率が高くなる傾向が見られます。いずれにしても，問題文の説明をそのまま引用して正解になるケースは，本試験の出題においても限られています。設問で問われていることを精査しながら，的確に答案を作成していくことを心掛けるようにしましょう。

設問 3 (1)～(3)は，問題の難度を考慮すれば，ほぼ想定どおりの低い正答率にとどまったと思われます。(4)の正答率は高かったようです。(5)は，問題の記述内容から，どのような攻撃が行われているのかをよく確認することなく，DNS キャッシュポイズニング攻撃と判断されたためか，キャッシュ DNS サーバという答案が幾つか散見されました。(6)は，個人所有の PC の接続を排除するため，表 2 の認証方式のうち，どの方式を採用すべきかを問うものでした。EAP-TLS を選択できても，その理由については，表 2 の EAP-TLS の説明をそのまま引用しているような答案もありました。何が決め手になっているかを明確に指摘することが必要です。

＜午後Ⅱ＞

問1　Web システムのインシデント対応

【採点基準】

[設問1]

(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) a，b は，解答例どおりに対し各 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各 4 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。指摘内容が今一歩のものは 3 点。その他は 0 点。
(5) 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 3 点。その他は 0 点。方法は，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。指摘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 4 点。その他は，基本的に 0 点。
(7) 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 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各 4 点。その他は，基本的に 0 点。
(4) d は，解答例どおりに対し 2 点。連携内容は，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3]

理由，施策とも，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。指摘内容が今一歩のものは 3 点。その他は 0 点。

【講評】

問 1 の平均点は 32.3 点で，問 2 よりも 6.2 点低い結果でした。このため，問 1 を選択した受験者の評価は，全体的に厳しいものとなっていますので，たとえ評価が低くても，あまり気にしないようにしましょう。

設問 1 は，全体的に正答率が低かったようです。例えば，(2)の空欄 b の Smurf 攻撃は，本試験の午前Ⅱ問題でも出題されたことがあるものでしたから，もっと正答率が高くなると考えていました。こうした点を見ても，本試験の過去問題の学習が十分に行き届いていないように感じられます。また，(5)の設問では，文脈から該当する利用者に連絡を取る方法が問われているにもかかわらず，「Web サーバのアクセスログから影響範囲を特定する」などのように，何を特定するかが具体的に指摘されていないものが幾つか散見されました。下線部に関する設問では，下線の前後にある記述内容をよく確認し

ながら，問われていることを明確にした上で解答を作成することが大切です。

設問 2 の正答率は，全体的にまずまずでした。なお，(3)では，TLS に完全移行することなどを指摘した答案も見られましたが，TLS に移行するに当たっては，取引先にお願いするべき事項があるはずです。こうした観点から解答を作成するようにしてください。取引先に対して案内する内容が，的確に指摘されていないものが多く見られました。

設問 3 の正答率は，まずまずでしたが，具体性に欠けるものが多かったように思います。例えば，ログ管理については，リストアに時間がかかるので，ログを迅速に分析できないということに気付いてほしかったと思います。

なお，問 1 と共通する事項ですが，全体的に，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ことが感じられました。本番の試験では，問題文をよく読んで設問で問われていることに対し素直に答えていくことを心掛けるようにしましょう。

問2 電子メールのセキュリティ

【採点基準】

［設問1］

a ～ i は，解答例どおりに対し各 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。

(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。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 3 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 5 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 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) 解答例どおりに対し各 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。

【講評】

問 2 の平均点は 38.5 点で，問 1 よりも 6.2 点高くなりました。電子メールのセキュリティに関する関心は高く，しかも理解もかなり進んでいるように思われます。

設問 1 は，全体的に正答率は高かったようですが，空欄 h，i の正答率は低かったと思います。迷惑メールの判定方法のベイジアンフィルタリングについては，本試験の午前Ⅱ問題としても出題されているものです。本試験問題については，午後問題に限らず，午前Ⅱ試験で出題された内容を含め，十分に把握しておくようにしましょう。

設問 2 (1)，(2)は，全体的に正答率が高かったようです。その半面，(3)，(4)の正答率は，かなり低かったと思います。特に，POP before SMTP については，本試験で既に出題されていますので，過去問題の学習が十分に行われていれば，難なく正解が得られるレベルの問題です。

設問 3 の正答率は，想定していたものよりも低い正答率だったと思います。(2)の署名の検証方法については，以前に比べて正しく理解されるようになってきましたが，復号する際には，対象物が何で，どの鍵を用いるのかといった事項を明確に答えるようにしましょう。

設問 4 は，全体的に正答率は高かったようで，特に問題はありません。

設問 5 は，SPF と DKIM の技術的な問題を出題しました。(1)は，TCP/IP 通信の基本ですから，よく理解しておくとよいでしょう。(2)は，既に本試験でも出題されている内容でしたから，正答率はまずまずでした。(4)は，署名対象データが転送途中で変更されると，受信側では，改ざんありと判断され，署名の検証に失敗するという基本的な知識です。こうした知識を一つ一つ積み重ね，ぜひ合格するように努力していきましょう。

以上