2014 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

2014 年 9 月 26 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 35.4 点，午後Ⅱが 32.8 点でした。問題別では，午後Ⅰの問 1 が 19.7 点，問 2 が 11.4 点，問 3 が 18.5 点で，問 2 の平均点が特に低かったといえます。また，午後Ⅱは，問 1 が 34.9 点，問 2 が 26.5 点でした。2014 年春期の公開模試では，午後Ⅰの平均点が 40.5 点，午後Ⅱの平均点が 32.7 点でしたから，午後Ⅰは低下，午後Ⅱは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，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試験では，問 1（アプリケーションにおけるマルウェア対策）の選択者が 44.3%，問 2（Web アプリケーションのセキュリティ対策）が 18.2%，問 3（ファイアウォールの更新とログ分析）が 37.5%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試験では，問 1（Web サイトのセキュリティ対策）の選択者が 73.5%，問 2（VPN の構築）が 26.5%で，約 3 対 1 という比率で問 1 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察し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 アプリケーションにおけるマルウェア対策

【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。指摘内容が今一歩のものは 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。真正性，あるいは完全性のいずれか一方を指摘したものは 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。指摘内容が今一歩のものは 4 点。その他は 0 点。

（4）解答例どおりに対し 3 点。

（5）解答例どおりに対し 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 6 点。その他は，基本的に 0 点。

(2) 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 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。

【講評】

平均点は 19.7 点（平均正答率は 39.4%）でした。問 1 は，全体的に設問 1 の正答率が低く，設問 2 の正答率が高かったようです。

設問 1 (1)は，exploit コード自体の説明をしたものも少し見られましたが，この設問では，マルウェアによる攻撃がなぜ想定されるのかという視点に立って考えることが必要です。(2)，(3)は，ディジタル署名の基本的な事項ですから，十分に理解しておくことが大切です。署名は，秘密鍵（署名鍵ともいう）を所有している本人だけができる行為です。また，秘密鍵によって暗号化するには，何を暗号化するのかといった対象物が必要です。公開鍵暗号方式では，処理時間の関係からできるだけ短いデータを使用する必要があり，そのデータとしては一般にハッシュ値が使われます。このため，署名を検証することによって確認できることは，本人の真正性と，メッセージの完全性の二つになります。この設問では，更新プログラムのコード署名を検証することによって，顧客が確認できることが問われているので，更新プログラム（ソフトウェア）の配布元が間違いなく C 社であり，しかも更新プログラムに改ざんがない（完全である）旨を答える必要があります。(3)では，署名の検証方法の説明が不十分なものが多く見られました。まず，署名を復号する際には，どの鍵で復号するかを明確に答える必要があります。署名は，署名者の秘密鍵で暗号化するので，復号は署名者の公開鍵で復号しなければなりません。更新プログラムの配布元では，プログラムのハッシュ値を計算し，そのハッシュ値を C 社の秘密鍵で暗号化してコード署名を作成します。そして，顧客は，その署名を C 社の公開鍵で復号し，それと更新プログラムから求めたハッシュ値が一致するかどうかを照合します。また，コード署名証明書とは，コード署名に使用する公開鍵証明書のことですが，使用目的ごとに特有の名称で呼ばれることもあります(S/MIME に使用される公開鍵証明書は，S/MIME 証明書と呼ばれています)。なお，コード署名とコード署名証明書を混同している答案もありましたが，その違いを明確にして考えるようにしましょう。(4)では，ランサムウェアと同じような意味をもつスケアウェア（scareware），クライムウェア（crimeware）という答案もありましたが，今回は不正解にしました。

設問 2 (4)は，アプリインストール時にパスワードを設定する旨の答案がありました。しかし，スマートフォンを不正に使用されないようにするには，端末ロックを行っておくことが基本です。セキュリティ対策の基本的な事項は十分に把握しておきましょう。

問2 Web アプリケーションのセキュリティ対策

【採点基準】

[設問1]

a，b は，解答例どおりに対し各 2 点。

[設問2]

(1) 解答例どおりに対し 6 点。
(2) c，d 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。

[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各 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。その他は，基本的に 0 点。
(3) e は，解答例どおりに対し 3 点。リスクは，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) 解答例どおりに対し 3 点。

【講評】

平均点は 11.4 点（平均正答率は 22.8%）でした。問題選択上，問 2 を選択せざるを得ない受験者も多くいたように感じられ，午後 I の 3 問の中では最も低い点数となりました。

設問 2 (1)は，%エンコードの意味が十分に理解されていなかったようで，正答率は極めて低かったようです。(2)，(3)の正答率も低かったと思われます。

設問 3 も，一部の受験者を除き，全体的に正答率は低かったようです。少なくとも，SQL のほか，HTML などで使用される特殊文字については，正確に覚えておくとよいでしょう。

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かもしれません。

問3 ファイアウォールの更新とログ分析

【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）a は，解答例どおりに対し 3 点。プロトコル名は，解答例どおりに対し 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 4 点。その他は，基本的に 0 点。

（2）項番 1 ～ 4，項番 20 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）項目名は，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。

（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。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。指摘内容が今一歩のものは 3 点。その他は 0 点。

【講評】

平均点は 18.5 点（平均正答率は 37.0%）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印象です。

設問 1 (1)，(2)は，まずまずの正答率だったと思われますが，(2)はもう少し高い正答率を期待していました。

設問 2 (2)～(4)の正答率は低かったようです。(2)については，DNS の MX レコードや TXT レコードの意味をしっかり把握している必要があると思われます。(3)は，問題の条件から，内部の PC がインターネットへアクセスする経路はプロキシサーバ経由しか存在しないことに気付いてほしかったと思います。(4)は，不正なサイトへの接続を禁止するには URL フィルタリングを行うことが基本ですが，この設問では不正なアプリケーションの通信を禁止する必要があることから，アプリケーションリストを用いた制御を行うことが必要です。問題の条件をよく考慮しながら解答を作成するようにしましょう。(5)は，トラップアカウントの意味がよく理解されており，正答率は高かったようです。その半面，(6)は具体的にと指示されているので，FW ログのどのような情報と，システムログのどのサーバのどのログを用いることなどを明確にして解答を作成しなければなりません。単に FW ログとシステムログを時系列的に突合させるなどの答案が多く見られましたが，例えば，表 1 には 6 種類のサーバがあるので，そのうち，どのサーバのどのようなログを対象にするかなどのキーワードを明確にして解答を作成するようにしましょう。

＜午後Ⅱ＞

問1 Web サイトのセキュリティ対策

【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）理由，確認内容とも，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。

［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）a は，解答例どおりに対し 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。

（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。その他は，基本的に 0 点。

［設問3］

（1）解答例どおりに対し 5 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）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。ハートビート機能を無効にするだけを指摘したものは 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各 4 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（認証情報が平文で流れるなど，デコードによって解読できる旨が指摘されていないもの）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 8 点。その他は，基本的に 0 点。

【講評】

問 1 の平均点は 34.9 点で，平均点では問 2 よりも高い結果でした。なお，問 2 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ていってほしいと思います。

設問 1 (2)の理由では，利用者が偽サイトに誘導される旨の答案が見られましたが，問題の背景がどのようになっているかを見極めるようにしましょう。また，確認内容では，コードの完全性を確認することに気付いた答案は，少なかったようです。

設問 2 の正答率は，全体的にまずまずでしたが，(3)の空欄 a に入れるプレースホルダの正答率は，それほど高くありませんでした。また，(5)も，改善すべき事項が問われているにもかかわらず，問題点を指摘したものや，現状のアクセス方法の状況を説明したものも見受けられ，的確な解答が作成できていませんでした。

設問 3 の正答率は，全体的にかなり低かったようです。(2)では，URL が異なっているなどの答案がありました。どこがどのように異なっているかを指摘することが重要ですから，単に URL が異なっているという指摘は，不正解にしました。(3)も，CSRF 攻撃の本質を突いた答案も少なかったように思われます。

設問 4 (2)は，秘密鍵の証明書などのように，公開鍵証明書が明確に読み取れない答案が散見されました。証明書が存在するのは，あくまでも公開鍵だけですから，よく理解しておきましょう。

設問 5 (1)は，問題の前方にある表 2 の内容に気付かなかった答案が多く見られました。

問2 VPN の構築

【訂正とお詫び】

図 2（受信側が管理するリプレイ防御ウィンドウ（32 ビット）の例）の上の図において，シーケンス番号の表示に誤りがありました。右端の値を“2”と表示していますが，正しくは“N”です。お詫びして訂正させていただきます。受験者の方々には，混乱を与えることになってしまい，改めて深くお詫び申し上げます。

【採点基準】

［設問1］

a ～ g 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 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各 6 点。その他は，基本的に 0 点。

［設問3］

（1）解答例どおりに対し各 2 点。

（2）管理上の注意点，改善点とも，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。

［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 4 点。その他は，基本的に 0 点。

（2）名称は，解答例どおりに対し 2 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 6 点。その他は，基本的に 0 点。

（3）解答例どおりに対し 4 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。

（2）解答例どおりに対し 3 点。

【講評】

問 2 の平均点は 26.5 点にとどまり，問 1 よりもかなり低い結果でした。本問は，ネットワークセキュリティに特化した問題であったため，ごく一部の受験者を除き，全体的に得点することが難しかったと思われます。

設問 1 の空欄 a ～ d の正答率は高く，空欄 e ～ g の正答率は低かったと思われます。

設問 2 の正答率は，全体的に低かったようです。特に，(3)は，AH と ESP の違いを説明したものも見受けられ，メッセージ認証の範囲を明確に指摘できていなかったようです。(4)も，ディジタル署名を検証するためには，自分自身の鍵ペアと，自身の公開鍵証明書を発行した CA のルート証明書が必要となります。こうした観点に立ち，CA とインストールするという字句を使う場合に必要となる作業をしっかり見極めるようにしましょう。

設問 3 ～設問 5 についても，全体的に正答率は低かったようです。例えば，設問 3 (2)では，管理上の注意点が問われているにもかかわらず，PSK を利用したときの問題点などを指摘した答案も見られました。設問に素直に答えていくことを忘れないようにしましょう。

以上