2012 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

2012 年 3 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 35.8 点，午後Ⅱが 29.8 点でした。問題別では，午後Ⅰの問 1 が 21.4 点，問 2 が 15.9 点，問 3 が 16.7 点，問 4 が 10.6 点で，問 1 の平均点が最も高くなりました。また，午後Ⅱは，問 1 が 25.6 点，問 2 が 34.0 点でした。2011 年秋期の公開模試では，午後Ⅰの平均点が 33.7 点，午後Ⅱの平均点が 28.9 点であったので，午後Ⅰ，午後Ⅱともに，平均点では若干向上しているといえます。なお，採点結果の印象では，十分に準備できている受験者と，そうでない受験者の差が相当大きかったと思われます。

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，「必要最小限の権限を与える」など，問題文に記述されていることをそのまま引用しても，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（情報セキュリティ管理の定期点検と認証の見直し）の選択者が 38.6%，問 2（サイバー攻撃）が 36.1%，問 3（学内 LAN のセキュリティ）が 20.3%，問 4（セキュアプログラミング）が 5.0%であり，問 1 と問 2 の選択者が多くなりました。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（Web システムのセキュリティ）の選択者が 49.5%，問 2（データベースの情報保護）が 50.5%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 情報セキュリティ管理の定期点検と認証の見直し

【採点基準】

[設問1]

項番と検出事例がともに，解答例と同じ内容のものに対し，各 6 点。その他は，基本的に 0 点。

[設問2]

(1) a ～ e は，基本的に解答例どおりのみ各 2 点。

(2) α 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。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 8 点。内容が今一歩と判断されるものは 4 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。

【講評】

設問 1 の正答率は，比較的良かったと思いますが，具体的な検出事例ではなく，対策基準の項番の内容をそのまま指摘したものが散見されました。指摘するものは，検出事例ですから，設問の指示に素直に従って解答を作成するようにしましょう。

TPM を選択する設問 2 (2)の正答率は，想定していたよりも悪かったと思います。基本的な用語の意味は，しっかり把握しておくことが合格への第一歩です。

設問 3 (2)の正答率は低かったようです。ディジタル署名（電子書名）の検証方法については，よく出題されるテーマですから，十分に理解しておくことが必要です。例えば，Y 社が送信する電子メールに添付されたディジタル署名の検証は，次のように行われます。まず，CA（認証局）が発行した Y 社の公開鍵証明書にある公開鍵で Y 社のディジタル署名を復号したものと，ディジタル署名の対象になった電子メールのダイジェスト（ハッシュ値）を求めて両者を比較します。両者が一致すれば，送信された電子メールが改ざんされていないことと，送信者が Y 社であるという真正性が確認されます。更に，CA 自体が信頼できるかどうかを確認するため，ルート CA に至る構築パスが確立されるかどうかのほか，公開鍵証明書の有効期限が切れていないことや公開鍵証明書が失効されていないことを確認する必要があります。このほか，Web サーバでは，サーバのコモンネームと URL で指定された FQDN が一致するかどうかを調べることがあります。また，公開鍵証明書は信頼できる第三者機関のほか，自組織の CA を立ち上げて公開鍵証明書を発行するケースもありますので，公開鍵証明書の検証については，問題の設定によって適切に判断していくことが必要となります。

問2 サイバー攻撃

【採点基準】

［設問1］

a ～ f は，解答例どおりのみ各 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) 解答例どおりのみ 2 点。

［設問3］

(1) ファイアウォールのルールは，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 6 点。内容が今一歩のものは 3 点。その他は 0 点。

［設問4］

(1) 解答例と同様の趣旨（A 部門 LAN の接続ポートをほかのポートにミラーリングすること）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。

(2) 解答例と同様の趣旨（L3SW にログインする旨のキーワード）が適切に指摘されているものに対し 6 点。単に「A 部門の接続ポートをシャットダウンする」旨の解答は 3 点。その他は 0 点。

【講評】

設問 1 の穴埋め問題では，空欄 f の CSIRT の正答率が特に低かったようです。コンピュータセキュリティにかかるインシデントに対応する組織としては CSIRT の存在があるので，こうしたことも含め幅広く把握して試験に臨むようにしましょう。

設問 2 (1)では，未知の脆弱性を適切に指摘した解答は少なかったようです。(2)のゼロデイ攻撃と合わせて考えるようにしてほしかったと思います。

設問 3 (1)のファイアウォールのルールに関する正答率は，想定していたよりも低かったと思います。問題の記述内容から条件がどのように変更されたかを，的確に判断することが必要です。

設問 4 (2)の設問の指示は，「リモートから切り離したい」です。このため，リモートから Telnet などを使って L3SW にログインすることが必要になります。どのような状況を想定すべきかが不明であれば仕方ありませんが，できるだけ設問の指示に従って解答を作成することが点数アップにつながります。本番の試験では，設問の指示を反映させた解答を作成するように心掛けてください。

問3 学内 LAN 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) 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) c，d は，解答例どおりのみ各 3 点。

(2) 解答例と同様の趣旨（異なるサブネットへの通信も含む）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。

(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) e，f 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】

この問題は，ネットワーク技術に関するものですが，ネットワークセキュリティともいわれるように，情報セキュリティスペシャリスト試験（SC 試験）ではネットワークに関連する問題はよく出題されます。このため，ネットワーク系の問題を選択する場合には，情報セキュリティとネットワークの両分野の技術については，十分に理解して試験に臨むことが必要です。

設問 1 (1)では，空欄 b に入れるミラーポートの正答率は低かった半面，(2)の記述式問題の正答率は高かったと思います。しかし，リピータハブに接続するだけで LAN を利用できるなど，盗聴リスクに触れていないものも若干みられましたので，設問で問われていることに適切に答えることが必要であると思われます。

設問 2 (4)の正答率が低かったのは，残念な結果でした。EAP-TLS を採用するメリットは，接続できるクライアントを，電子証明書をインストールした無線端末に限定できることです。しかし，機器認証はできても，利用するユーザの本人認証にはならないので，こうしたことも含め，十分に理解しておきましょう。

問4 セキュアプログラミング

【採点基準】

［設問1］
a ～ d は，解答例どおりのみ各 3 点。

［設問2］
(1) e ～ f は，解答例どおりのみ各 2 点。
(2) 解答例どおりのみ 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。

［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。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。

【講評】

この問題は，セキュアプログラミングに特化したものですから，選択した受験者は少数でした。なお，平成 24 年度春期試験から SC 試験で出題の対象となるプログラミング言語は C++，Java，ECMAScript になり，Perl は対象外になりましたので，注意しましょう。

設問の穴埋め問題は，専門的な技術用語を答える必要があるので，正答率が低くても仕方ありません。しかし，記述式の問題は，想定していたよりも正答率がかなり低かったようです。Web システムへの攻撃とその対策方法については，それらの仕組みを十分に把握しておくことが必要です。また，IPA から公表されているセキュアプログラミング講座の内容は膨大な量がありますが，よく出題されます。セキュアプログラミングの問題を選択する際には，事前にその内容を理解しておくとよいでしょう。

＜午後Ⅱ＞

問1 Web システムのセキュリティ

【採点基準】

［設問1］
a ～ j は，解答例どおりのみ各 3 点。

［設問2］
(1) 文字は，解答例のみ 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。
(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 8 点。その他は，基本的に 0 点。

［設問3］
(1) 方法，理由ともに，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 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。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 8 点。その他は，基本的に 0 点。

［設問5］
解答例と同様の趣旨（SSL の暗号化を復号するというキーワードが必要）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】

設問 1 の穴埋め問題の正答率は，全体的に低かったようです。穴埋め問題については，穴埋めの箇所だけに着目するのではなく，文章の全体的な流れを考慮しながら適切な字句を考えていくようにしましょう。そうすれば，正答率もアップすると思われます。

設問 2 ～ 5 の記述式問題も，全体的に正答率が低かったようです。設問 2 は，Web アプリなどのセキュリティ対策ですから，基本的な事項については，しっかり把握しておきましょう。設問 3 (1)は，パスワードの保存に関する基本的な問題です。ハッシュ値を保存するという解答は比較的少なく，データベースへのアクセス権を設定する，あるいは現在と過去のパスワードを異なるデータベースに保存するなどの答案が見られました。なお，ハッシュ値を保存するとした答案でも，その理由であるハッシュ関数の一方向性を指摘できていないものも少しありましたので，基本的な知識はしっかり身に付けておくことが必要です。設問 4 では，(3)の正答率がかなり低かったと思います。席をはずした際に，その端末を悪用されるなどの問題点を指摘しているものが多くありました。また，セッションハイジャック攻撃が行われる旨の答案もありましたが，ほかのユーザが利用しているセッションに入り込むためには，攻撃者はそのセッション ID を推測することが必要であることに気付いてほしかったと思います。設問 5 は，SSL の暗号化を解くことがこの設問のポイントになっています。何がポイントになっているかを見極めながら解答を作成するとよいでしょう。

問2 データベースの情報保護

【訂正とお詫び】

P15 の表 3 の中に，パスワード履歴の項目が二つ存在しており，正しくは一つだけです。最初のパスワード履歴の行を削除しますので，この場を借りて訂正させていただきます。受験者の方々には無用の混乱を与えてしまうことになり，深くお詫び申し上げます。

【採点基準】

［設問1］

(1) a は，解答例どおりのみ 3 点。

(2) 解答例と同様の趣旨（DBMS 側でセキュリティ機能を実装すること）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) 検索処理，理由ともに，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) 機密性の観点，可用性の観点ともに，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各 6 点。その他は，基本的に 0 点。

(3) 解答例どおりのみ 5 点。

(4) b，c は，解答例どおりのみ各 3 点。

［設問4］

(1) 解答例と同様の趣旨（操作ログを取得すること，別の管理者が定期的に確認することの 2 点）が適切に指摘されているものに対し 8 点。単に操作ログを取得するだけでは 4 点。その他は 0 点。

(2) 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。

(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。

【講評】

設問 1 (1)の正答率は，高くありませんでした。バインド機構は基本的な用語です。基本的なものについては確実に正解することが合格への第一歩となります。

設問 2 (2)の正答率はまずまずでしたが，(1)，(3)ともにかなり低かったようです。特に，(1)は，問題の記述内容を十分に把握した上で，解答を作成すれば正解を導くことができます。こうした設問では取りこぼしをしないようにすることが必要です。

設問 3 では，(1)，(2)の正答率は良い半面，(3)，(4)は想定よりも低かったと思います。なお，(2)では，図 2 におけるセキュリティ運用規定をそのまま指摘したものが散見されましたが，解答を作成するに当たっては，具体的な違反事例を指摘することが必要です。本番の試験では，問題文の単なる引用ではなく，できるだけ具体的な事例を指摘するようにしましょう。

設問 4 は，全体的に正答率は高くなかったようです。記述式の問題では，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。また，SC 試験で合格を目指すには，一つ一つの知識を積み重ねていくことが重要ですから，本番の試験に向けて努力を惜しまないようにしましょう。

以上