2012 秋 情報セキュリティスペシャリスト 総合実力診断模試 講評と採点基準

2012 年 8 月 17 日 (株)アイテック 情報技術教育研究部

■ 全体講評

総合実力診断模試は，10 月の情報セキュリティスペシャリスト試験（以下，SC 試験という）で合格するために必要な技術知識が，どれだけ身に付いているか診断することを主な目的としています。今回の採点結果から判断すると，午後Ⅰ試験の正答率は，かなり良かったと思います。ちなみに，問題ごとの平均点は午後Ⅰ（50 点満点）の問 1 が 30.1 点，問 2 が 17.3 点，問 3 が 26.3 点，問 4 が 17.0 点，全体の平均点は 47.5 点でした。一方，午後Ⅱ（100 点満点）は，問 1 が 34.6 点，問 2 が 48.3 点で，問 2 の方がかなり高くなりました。なお，午後Ⅱの平均点は 40.7 点です。問題ごとの選択率は，午後Ⅰの問 1 が 29.1%，問 2 が 21.7%，問 3 が 31.1%，問 4 が 18.1%で，問 3 が多く，問 4 が少ないという状況でした。これに対し，午後Ⅱの問 1 は 53.7%，問 2 が 46.3%で，ほぼ均衡していました。

総合実力診断模試の性格上，午後Ⅰ，午後Ⅱ試験とも，どれだけ得点できたかということよりも，これからどのような姿勢で本番の試験に臨んでいくかということに重点を置いて考えてください。それは，あまり得点できなかった問題については，解説をよく読んだり，弊社刊行のテキストなどを参考にしたりしながら，その技術分野の知識を自分自身のものとして十分に吸収していけばよいからです。

特に，SC 試験では，幅広い情報セキュリティ技術分野から，詳細な知識を問う問題がよく出題されます。総合実力診断模試で取り組んだような問題だけではなく，電子証明書やワンタイムパスワードを用いた認証方式の仕組み，メッセージ認証や時刻認証などの認証技術をはじめ，暗号化技術，Web システムに関するセキュリティ，セキュアプログラミング，SSL や IEEE 802.1X などのセキュリティプロトコル，DNS や電子メールに関するセキュリティ問題，データベースのセキュリティ，ISMS などのマネジメント系についても幅広く，しかも深く掘り下げて理解していくことが必要です。また，試験問題を考える上では，問題文に記述されている内容の範囲内で答案を作成していくことが基本です。つまり，技術知識をしっかり身に付けていなければ，問題で記述された内容を十分に把握することさえ満足にできず，思うように解答を作成することができません。そこで，本番の試験に向け，できるだけ知識レベルを向上させていくことが必要です。本番の試験までには 1 か月半の期間がありますから，しっかり学習計画を立てて，十分に準備をして臨むようにしましょう。

総合実力診断模試の結果については，A 判定から E 判定という評価が行われます。午後Ⅰ，午後Ⅱとも正答率がともに 8 割以上であれば，かなり有望ですが，既に同じような過去問題を解いている場合には，どうしても判定が甘くなります。また，D 又は E 判定であっても，基本技術がしっかり把握できている場合には，それほど心配する必要はありません。解答の作成方法を工夫するだけでも得点はアップします。例えば，今回の採点結果から判断すると，下線に関する理由などを問う設問に対しては，かなりの答案が，下線の部分だけに着目し，全体の関係を考慮しないで解答を作成しているのではないかという印象を受けました。下線だけではなく，その前後に記述された内容を十分に考慮した上で，解答を作成すれば，より的確な答案が作成できると思います。

最終目標は，あくまでも本番の試験で合格することです。このため，本番の試験では，問題の記述内容を十分に考慮し，設問で問われていることを必ず確認した上で，解答を作成するようにしましょう。また，設問では，どのような観点から述べよといった指示がよくあります。こうした場合には，設問の指示に忠実に従って，解答を作成するようにしましょう。そうすれば，点数をアップさせることができます。しかし，こうしたことができるようになるには，情報セキュリティ技術全般に関する理解が一定のレベル以上に達していることが前提となるので，その点については十分に留意してください。

＜午後Ⅰ＞

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，解答例どおりに対し各 2 点。

（2）c は，解答例どおりに対し 2 点。

［設問2］

（1）d 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 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3］

（1）e 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 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 8 点。その他は，基本的に 0 点。

（4）解答例と同様の趣旨（通過したパケットによる攻撃が成功する旨のキーワードが必要）が適切に指摘されているものに対し 8 点。内容が今一歩のものは 4 点。その他は 0 点。

【講評】

午後 I の 4 問の中では，最も正答率が高くなりました。その要因としては，フォールスポジティブ，フォールスネガティブの説明の正答率が高かったことが挙げられます。

設問 1 (1)では，すべて（ALL）という答案が見られましたが，字句については表中で使用されているものを使って答えるようにしましょう。

設問 2 (2)では，「パスワードが平文で送信される」というように，設問で問われていることと逆のものを答えた例がありました。設問では何が問われているかを確認することが重要です。本番の試験では問題の条件並びに設問で問われていることは必ず確認するようにしましょう。(3)では，「DMZ のサーバから不正アクセスされる」などの答案がありましたが，この設問ではどこに対する不正アクセスかを指摘することがポイントです。解答者の方は，よく理解されていると思いますが，それが答案用紙にきちんと記述されていなければ得点になりません。あくまでもポイントとなる記述をしっかりと記入することを忘れないようにしましょう。

設問 3 (2)の用語は，基本的なものですから，比較的容易であったといえます。しかし，最近の試験では，用語の意味を問うものはほとんどなく，問題の記述内容などに従って考察していくものが大半を占めています。問題をよく読んで解答を作成することが必要です。また，(4)は FW との連携が前提になっていますので，設問で問われていることに対して素直に応えていくことが必要です。

問2 電子メールのセキュリティ

【採点基準】

[設問1]

a ～ h は，解答例どおりに対し各 2 点。

[設問2]

（1）解答例と同様に，不正中継に利用される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。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3]

（1）比較対象，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 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。

【講評】

電子メールに関するセキュリティのうち，技術的な内容が中心でしたから，正答率は低かったようです。

設問 1 は，電子メールに関する基本的な用語ですから，それらの意味は，できるだけ押さえておきましょう。特に，暗号化メールの S/MIME や PGP のほか，電子署名を付与した場合には，送信者の認証やメッセージの完全性が保証されることのほか，否認防止にもなることなどは十分に把握しておきましょう。

設問 2 (2)は、問題文に直接のヒントのない知識問題ですが，POP before SMTP の仕組みを理解していれば正解できる問題です。このため，技術知識については、できるだけ多くを保有しておくとよいでしょう。(3)は，設問 1 (c)をヒントに考えることがポイントです。

設問 3 (1)では，「メールヘッダ内の IP アドレス」や「ドメインから正引きした IP アドレス」という答案が目立ちました。比較対象は，メールヘッダの情報に基づくものではなく，接続元の IP アドレスです。また「DNS サーバの SPF レコードの IP アドレス」という答案も多く見られました。これは，設問の読み違いと思われますので，注意しましょう。(2)では，DKIM 自体の説明をした答案もありました。この設問では Sender ID にはない，DKIM のセキュリティ機能が問われています。設問で問われていることに対して的確に答えることが得点アップの秘訣です。

問3 認証機能

【採点基準】

[設問1]

（1）a，b 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各 4 点。その他は，基本的に 0 点。

（3）「パスワードを新規作成する」，「電子メールで通知する」という二つのキーワード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。内容が今一歩のものは 4 点。その他は 0 点。

[設問3]

（1）「メールサーバの負荷増大」が適切に指摘されてい

るものに対し 8 点。DoS 攻撃の対象になるなど，内容が今一歩のものは 4 点。その他は 0 点。
(2)「ランダム」と「十分な長さ」の二つの要件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】

平均正答率は 52.5%（平均点は 26.3 点）であり，想定していたよりも，低い結果になりました。問題の記述内容に照らし合わせた解答が作成できていないという印象を受けました。

設問 1 (1)では，パスワードの保存に当たっては，暗号化するよりもハッシュ値を記憶させることが安全であることについては，よく理解しておきましょう。(2)の下線④の対策では，「会員 ID を無効にする」のか，「一時停止（あるいはアカウントロック）にする」のかがポイントです。こうした違いについては，明確に記述するようにしましょう。下線⑤の対策では「注文時にメール通知する」旨の答案もありました。なりすましのログオンを検知するのが目的ですので，注文時だけでは不足です。(3)は，正答率が比較的高かったようです。新しいパスワード（初期パスワード）を新規発行するということと，画面上では通知しないということが必要です。

設問 2 では，「なりすましで不正アクセスする」旨の答案もありました。設問では，「現状の初期パスワードの配布方法では～」と指示されていますので，問題の現状の初期パスワードの配布方法を確認し，解答を作成する必要があります。なお，解答を作成する上では，問題文中のキーワードを適切に引用するとよいでしょう。ただし，問題文そのものの引用は，基本的に正解にならないことが多いので，こうした点は注意しましょう。

設問 3 (1)は，正答率が低かったようです。サーバ負荷といった観点も押さえておきましょう。(2)の照合用文字列では，不正プログラムが判読できない画像文字に着眼した解答がありました。CAPTCHA については，ボットの対策などには必要ですが，この問題では電子メールに記載しますので画像文字は適切ではありません。(3)の正答率は，極めて高かったようです。最後の設問が容易なこともよくありますので，本試験では得点できる設問では，確実に点数を重ねていくようにしましょう。

問4 検疫システム

【採点基準】

[設問1]

a，b は，解答例どおりに対し各 4 点。

[設問2]

解答例どおりに対し 4 点。

[設問3]

(1) タイミングは，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。内容が今一歩のものは 3 点。その他は 0 点。範囲は，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。
(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。内容が今一歩のものは 4 点。その他は 0 点。

[設問4]

接続方法は，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。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 10 点。その他は，基本的に 0 点。

【講評】

ネットワークセキュリティのうち，検疫システムに特化した問題でしたから，平均正答率は問 2 とともに低くなりました。

TCP/IP ネットワークでは，ネットワーク内の各ホストが IP 通信を始めるには，それぞれのホストは IP アドレスを取得していることが必要です。こうした基礎知識を十分に身に付けていない場合には，正答率を高めることは難しいと思われます。

SC の午後 I 試験は，4 問の中から 2 問の選択ですから，各自が得意とする分野の問題をうまく選択することが必要です。今回の総合模試の午後 I では，セキュアプログラミング関連の問題を出題していませんでしたが，セキュアプログラミング関連の問題を選択するかどうかも，あらかじめ決めておくとよいでしょう。

＜午後Ⅱ＞

問1 情報セキュリティ対策と無線 LAN のセキュリティ

【採点基準】

[設問1]

(1) ア～ウは，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。

[設問2]

(1) a ～ g 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。
(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（機密情報が漏えいするなど）

は，基本的に 0 点。

［設問3］

（1）h ～ j 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。

（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 8 点。その他は，基本的に 0 点。

［設問4］

（1）k，l 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 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 8 点。その他は，基本的に 0 点。

【講評】

設問 3，設問 4 が無線 LAN のセキュリティに関する問題であったことから，平均正答率は問 2 に比べると，かなり低くなりました。

設問 1 の正答率は高く，基本的なセキュリティ対策は十分に理解できていると判断されます。

設問 2 (1)の空欄 g の後ろに「特殊文字」とありますので，「バインド変数」や「プリペアドステートメント」などは除外しました。(2)は，設問のキーワード「可用性」からストレートに考えるとよいでしょう。なお，「可用性の問題」が問われているにもかかわらず，解決策を指摘した答案も見られました。(3)は，エラーメッセージの内容に起因するリスクが論点ですが，ユーザの視点での使いやすさなどに着眼した答案もありました。常にセキュリティの観点で考察することに留意してください。

設問 3 や設問 4 については，解説などをよく読んで理解を深めるようにするとよいでしょう。なお，設問 4 (2)では，CRC-32 を暗号化方式と理解している答案が目立ちました。CRC-32 は，もともと伝送誤りを検出するために用いられたもの（暗号化とは無関係です）で，それを WEP では，メッセージの完全性のために利用したことから，WEP の脆弱性の一つとして指摘されるようになったものです。

問2 Web アプリケーションシステムの脆弱性対策

【採点基準】

［設問1］

（1）a，c は，解答例どおりに対し各 3 点。

（2）解答例どおりに対し 8 点。

（3）攻撃，問題点とも，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 8 点。その他は，基本的に 0 点。

［設問2］

（1）解答例どおりに対し 4 点。

（2）d は，解答例どおりに対し 4 点。

（3）解答例どおりに対し 4 点。

（4）b 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 10 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 8 点。その他は，基本的に 0 点。

（2）不足している情報は，正解につき各 2 点。ただし解答数が多い場合には，それぞれ減点。改修内容については，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 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各 8 点。その他は，基本的に 0 点。

【講評】

全体的には，まずまずの正答率であったと思います。

設問 1 (1)の c では，認証と認可の違いを明確に把握しておきましょう。(2)は，最後のパイプ文字が不足している答案が多く見られました。(3)の正答率は，比較的高かったようです。SQL インジェクションを指摘したものもありましたが，セキュアプログラミングにおけるどのテーマが論点かを意識するとよいでしょう。

設問 2 (1)のログを考察する問題は，よく出題されますので，読み方を把握するようにしましょう。(4)では，DB アカウントに付与するアクセス権限を最小化することは，DB アクセスにおける定石になっている事項です。

設問 3 (1)の正答率は高かった半面，(2)の正答率は低かったようです。(2)では，TRN ログ単独と DB ログ単独で不足している情報は何かを考えさせています。つまり，共通に不足している情報として，利用者 ID を答えさせた上で，それをどのように改修したらよいかが問われています。設問で設定されている状況にうまく誘導されながら解答を考えることも重要です。解答作成における留意事項として覚えておくとよいでしょう。(3)では，「インシデント対応手順とその訓練」というように，一つの項目で二つの事項を記述した例も見られました。解答の作成に当たっては，一つ項目に対し，一つの事項を答えることが原則になっています。穴埋め問題でも同様で，二つの字句を入れることはありません。こうしたことにも留意しながら，解答を作成するようにしましょう。

以上