2011 春 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

2011 年 2 月 16 日 (株)アイテック 商品開発本部

■ 全体講評

総合実力診断模試は，4 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 試験は，想定していた以上に正答率が高かったと思います。ちなみに，問題ごとの平均点は午後 I（50 点満点）の問 1 が 23.6 点，問 2 が 16.1 点，問 3 が 29.1 点，問 4 が 20.0 点で，平均点は 47.1 点でした。一方，午後Ⅱ（100 点満点）は，問 1 が 31.0 点，問 2 が 44.3 点で，問 1 と問 2 とでは大きな差になりました。なお，午後Ⅱの平均点では，39.1 点です。また，問題ごとの選択率は，午後 I の問 1 が 37.3%，問 2 が 11.4%，問 3 が 29.6%，問 4 が 21.7%，午後Ⅱの問 1 が 36.6%，問 2 が 63.4%という状況でした。

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試験に臨んでいくかということに重点を置いて考えるようにしましょう。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くことの方が大切だからです。

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解いた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，IPsec や SSL，IEEE802.1X 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，できるだけ技術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を解いている場合には，判定は甘くなる傾向があります。最終目標は本番の試験で合格することですから，現状の判定に満足するのではなく，本番の試験まで気を抜かないように注意しましょう。一方，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，今回の採点結果を見ると，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。

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，設問に指示に忠実に従って，解答を考えてみてください。そうすれば，点数のアップにつながってくるはずです。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りますので，その点については十分に留意してください。

＜午後 I ＞

問1 Web 受注システムのセキュリティ対策

【採点基準】

［設問1］

（1）a ～ d は，解答例どおりのみ各 2 点。ただし，a はデータ部でもよい。

（2）e ～ g は，解答例どおりのみ各 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 4 点。その他は 0 点。

（4）「シグネチャの更新」というキーワードが適切に指摘されているものに対し 6 点。その他（パターンファイルの更新など）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（C 社が実施すべき事項）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) 必要な項目，方法ともに，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それぞれ 4 点。その他は，基本的に 0 点。

【講評】

平均点は 23.6 点（正答率 47.1%）で，ほぼ想定通りでした。なお，この問題の選択率は 37.3%であり，4 問の中では最も高いものでした。

設問 1 (4)では，IDS などで照合を行うシグネチャファイルを，ウイルスを検出する際に行われるパターンフィル（ウイルス定義ファイル）と混同しているような答案が幾つかありました。基本的な用語の意味は，しっかりと理解しておきましょう。

設問 2 (1)の正答率は低かったようです。UTM で攻撃を検知するには，〔Web 受注システムの概要〕に「利用者の端末と Web サーバ間のすべての通信は SSL によって暗号化されている」と記述されています。こうした記述をしっかり確認しながら，解答を作成すれば，正解できるはずです。本番の試験では，必ず問題文の記述内容を確認しながら解答を作成するようにしましょう。

問2 プログラム開発のセキュリティ

【採点基準】

[設問1]

a ～ f は，解答例どおりのみ各 2 点。

[設問2]

(1)「ナル文字まで読み出された」というキーワードが適切に指摘されているものに対し 6 点。その他（単に line 3 からオーバフローしたなど）の表現は，基本的に 0 点。
(2) 解答例，又はそれと同等の表現に対し 2 点。
(3)「オーバフローし，9，0，ナル文字が書き込まれた」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) コードは，解答例どおりのみ 4 点。対策は，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。

[設問3]

(1) ファイルパス，パイプ文字とも，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 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 0 点。

【講評】

平均点は 16.1 点（正答率 32.1%），問題の選択率も 11.4%であり，4 問の中では最も低くなりました。本番の試験では，4 問のうち，2 問を選択すればよいので，得意としない分野の問題は，選択しない方が得策です。

この問題では，strcpy と strncpy の違いを，よく把握しておいてほしいと思います。strcpy を実行すると，コピー元の文字列の中から，ナル文字が見つかるまでコピーします。このため，コピー元の文字列長が，コピー先よりも長い場合には，バッファオーバフローを発生させ，コピー先には，ナル文字を含めてコピーされます。一方，strncpy は，コピー元の文字列長のうち，n 文字だけをコピーします。このため，n 文字目がナル文字でない場合には，コピー先のバッファには，ナル文字が書き込まれないことになります。

なお，セキュアプログラミングの問題を選択する場合には，前もって IPA（情報処理推進機構）セキュリティセンターが公表している「セキュアプログラミング講座」を十分に学習されることをお勧めします。それは，情報セキュリティスペシャリスト試験では，「セキュアプログラミング講座」の中の題材を基に出題されることがあるからです。

問3 ISMS 構築時のリスクマネジメント

【採点基準】

[設問1]

a ～ e は，解答例どおりのみ各 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 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 0 点。

[設問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 0 点。

[設問4]

(1) f ～ h は，解答例どおりのみ各 3 点。
(2) i は，解答例どおりのみ 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 8 点。内容が今一歩のものは 4 点。その他は 0 点。

【講評】

平均点 29.1 点（正答率 58.3%）で，午後 I の 4 問の中では最も高く，情報漏えい対策に関する技術知識などについては，十分に把握されているように感じました。

設問 1 は，リスクマネジメントに関する基本的な穴埋

め問題でしたが，全問正解者は比較的少なかったようです。なお，リスク低減については，リスク最適化と呼ばれることもありますが，JIS Q 13335（情報通信技術セキュリティマネジメントの機能及びモデル）などでは，リスク対応として，リスク低減，リスク回避，リスク受容，リスク移転という字句を使用しています。このため，設問 1 の空欄 c に入れる字句としては，低減だけを正解とし，最適化は不正解としました。

設問 2，設問 3，設問 4 (1)の正答率は高かったようです。しかし，設問 4 (3)では，ソルトとパスワードの関係が必ずしも十分に理解されていないように見受けられましたので，よく理解しておいてほしいと思います。

問4 DNS のセキュリティ

【採点基準】

［設問1］

a ～ g は，解答例どおりのみ各 2 点。ただし，a はドメイン名でもよい。

［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。

［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。その他は，基本的に 0 点。

［設問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て 6 点。その他は 0 点。

【講評】

DNS に関する詳細な技術知識が要求されることから，平均点は 20.0 点（正答率 40.0%）であり，ほぼ想定通りの結果でした。午後 I 試験では，得意分野の問題を選択していくことがポイントになりますので，本番の試験までに，できるだけ得意分野を増やし，選択できる問題の幅を増やしていくことも必要となります。

記述式の問題では，問題に記述された内容をよく理解しながら解答を作成していくことが基本です。例えば，設問 2 (1)は，想定以上に正答率が良かったと思います。それは，図 2 の「キャッシュ汚染の手法（例）」を見ながら，コンテンツサーバの正規の応答よりも，攻撃者の送り込んだ応答パケットの方が早く到着する必要があることに気付き，その旨を解答したからではないでしょうか。

その半面，設問 1 の空欄 d の正答率は，期待ほど高くありませんでした。A 君の「IP アドレスのほか，ポート番号が一致すれば，……」という発言から，ポート番号にすべて“53”が使用されているキャプチャ番号の I が汚染される可能性が高いことが分かります。しかし，空欄 d を考える際には，図 3 の「キャプチャ結果」だけから考え，番号を選択したのではないでしょうか。問題の記述内容を十分に確認しながら考えていくことが必要です。本番の試験では，問題文に基づいて考えていくことを基本にしましょう。

＜午後Ⅱ＞

問2 Web システムのセキュリティ

【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) 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2］

(1)「顧客の個人情報の漏えい」,「システムの脆弱性情報の漏えい」というキーワードが適切に指摘されているものに対し各 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 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 6 点。その他は，基本的に 0 点。

［設問3］

(1) a ～ d 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 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。

［設問4］

(1) e，f は，解答例どおりのみ各 2 点。

(2) 属性名は，解答例どおりのみ 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 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】

正答率は 31.0%で，想定していたものよりも，低い結果でした。午後Ⅱ試験では，まず問題の記述内容を十分に把握しながら解答を作成することが必要です。

設問 1 については，セキュリティ事故に遭遇した際，担当者独自が判断するのではなく，責任者に報告の上，その指示を仰ぐという視点は重要なことです。しかし，この問題では，下線の前後にある記述を読めば，エラーメッセージの表示に関するものであることが判断できます。このため，エラーメッセージの表示に関することを指摘したものだけを正解にしました。

セキュアプログラミングの問題については，ある一定の知識が要求されますが，問題の記述内容を基にしながら設問 3 のような問題には，正解できるように技術レベルを向上させておくとよいでしょう。そうすれば，幅広い分野の午後Ⅱ問題に対しても対応することが可能となります。なお，設問 3 の正答率は，全体的に低かったようです。

また，クッキー情報に関するセキュリティ問題も重要です。セッション管理の方法だけではなく，セキュアな通信を行うための属性などを含め，幅広く理解するようにしましょう。

問2　社内システムのセキュリティ対策

【採点基準】

［設問1］

(1) a ～ c 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。

(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) d ～ f は，解答例どおりのみ各 2 点。

(2)「通信相手の認証」というキーワードが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) 採用すべきモードは，解答例どおりのみ 2 点。理由は，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) g ～ i 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。

(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4］

(1) i は，解答例どおりのみ 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)「ハードディスクを暗号化する」,「復号鍵を認証デバイスに格納する」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 8 点。内容が今一歩のものは 4 点。その他は 0 点。

［設問5］

(1)「送信元アドレスが FW のアドレスに書き換わる」旨のキーワードが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) 原因，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，それぞれ 6 点。内容が今一歩のものは 3 点。その他は 0 点。

【講評】

正答率は 44.3%であり，ほぼ想定通りでした。なお，正答率が低かった個別の設問としては，設問 1 (3)，設問 2 (2)，設問 4 の(2)，(3)，設問 5 (1)のほか，(2)の検知できなかった理由などがあります。

例えば，設問 1 (3)では，「利用者 ID が分かれば，なりすまされる」などの問題点だけに着目した答案が，かなり見られました。しかし，この設問では，下線②の対応の問題点を述べることが求められていますので，対応上に関する事項を述べることが必要です。この例は，設問の指示に従っていないことになりますので，本番の試験では注意するようにしましょう。

設問 2 (2)では，ハッシュ値が一致するということは，改ざんがないことですが，図 3 や図 4 のほか，本文中の記述に基づいて，同じ事前共有鍵をもった相手であることを確認していることに気付いてほしかった問題です。

設問 5 のプロキシモードによるメールの転送に関する記述は，少し複雑になっています。しかし，SMTP やアドレス変換の知識がしっかり身に付いていれば，どのような状況になっているかが理解できたはずです。そうすれば，的確な解答を作成することができます。

記述式の問題に対しては，情報セキュリティ技術の本質をよく理解し，的を射た解答を作成していくことが重要です。また，試験での合格を目指すには，事前によく学習し，詳細な技術に至るまでしっかりと理解しておくことが必要です。問題の記述内容に沿った解答の作成方法とともに，技術知識に関してもできるだけ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。

以上