2010 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

2010 年 2 月 17 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。また，初めて高度試験を受験される方は，午後Ⅰ，午後Ⅱの選択問題の方法を確認しておくことも必要です。午後Ⅰ試験は，4 問の中から 2 問を選択して解答しますが，選択した問題番号を○印で囲んでいなかったり，別の問題番号に○印が付けられたりしています。特に，午後Ⅱは 2 問のうち，1 問を選択しますので，○印で囲まれていないケースが多く見受けられます。本番の試験では，○印で囲んでいないものなどは，採点の対象になりませんので，注意してください。

次に，今回の総合実力診断模試では，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，どれだけ理解できたかということに重点を置くようにしましょう。例えば，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，しっかり吸収していくことが必要です。

その一方，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，セキュアプログラミングやデータベースセキュリティに関する詳細技術をはじめ，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全般，IPsec や SSL，IEEE802.1X などのセキュリティプロトコル，検疫ネットワーク，ファイアウォール，無線 LAN などの情報セキュリティ技術だけではなく，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。特に春期の SC 試験は，秋期とは異なり，技術分野を中心に出題されると考えられます。しかも，試験問題を考えていく上では，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実施している場合には，判定はどうしても甘くなります。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。なお，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，本番の試験で合格点をクリアすることは，それほど難しいというわけではありません。SC 試験をはじめとした高度試験の午後Ⅰ，午後Ⅱでは，問題の記述内容に従って解答を作成していくことが基本です。今回の採点結果を見ると，設問で問われていることに対し忠実に答えるのではなく，自分自身が思いついたことだけを解答しているという答案が，かなり見られました。そこで，本番の試験では，設問で問われていることを必ず確認し，その上で解答を作成するようにすれば，それだけでも点数のアップにつながるはずです。例えば，「理由が問われているのか」，「方法が問われているのか」，「リスクが発生するのは，どのようなケースなのか」など，設問の指示に的確に従った上で，解答を作成するようにしましょう。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 VPN の導入

【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（鍵が危たい化する旨）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。

（3）解答例と同様の趣旨（コネクションを維持しない旨）が適切に指摘されているものに対し 4 点。その他（送達確認ができない，信頼性がないなど）は，基本的に 0 点。

（4）「PC 上でユーザ認証の操作が不要」と「VPN が利用できる」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 4 点。単に「PC 上でユーザ認証の操作が不要」という指摘は 2 点。その他は 0 点。

［設問2］

（1）d ～ f は，解答例どおりのみ各 2 点。

（2）「IP パケットの暗号化」，「メッセージの改ざんを

検出できる」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。IP パケットの暗号化だけを指摘したものは 3 点。その他は 0 点。

(3) 公開鍵証明書 IKE 方式と比較したメリット，手動鍵管理方式と比較したメリットとともに，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 6 点。その他は，基本的に 0 点。

［設問3］

(1) 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 6 点。その他は，基本的に 0 点。

【講評】

穴埋め問題のほか，設問 2，3 の正答率が比較的よかったので，平均点は 24.4 点と想定していた以上によかったと思います。

設問 1 (1)の空欄 b に関連し，情報セキュリティにおける基本用語として，機密性，完全性，可用性，真正性，責任追跡性，否認防止などについては，正確に理解しておきましょう。設問 2 (3)では，相手認証に公開鍵証明書を用いることは，高い安全性が得られる半面，すべての装置に公開鍵証明書をインストールする場合には運用管理が煩雑になるなどの問題があります。また，公開鍵証明書を使用するには，その検証をしなければなりません。公開鍵証明書の検証を行うには，どうすればよいかなどについては十分に理解しておきましょう。

また，鍵の使い方は，メッセージを暗号化する場合のほか，メッセージ認証を行うには，認証鍵を絡ませてハッシュ値を生成する必要があること，あるいは通信相手の認証を行うには，同じ鍵を所有しているかどうかによって判断することもあります。鍵の使い方は，様々な局面で使用されるので，これらの違いについては，問題の記述内容などに従って正確に見極めていく必要があります。こうしたことにも注意しながら，問題文を読んでいくとよいでしょう。

問2 ネットワークにおける PC 利用

【採点基準】

［設問1］

a，b は，解答例どおりのみ各 2 点。

［設問2］

(1) c ～ e は，解答例どおりのみ各 2 点。

(2) 解答例どおりのみ各 2 点。ただし，三つ以上，解答したものは，一つにつき 2 点ずつ減点する（四つ以上解答すると，0 点になる）。

(3) APOP とパスワードの暗号化という二つのキーワードが指摘されているものに対し 6 点。指摘された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 8 点。「LAN ケーブルなどから漏れる電磁波を解析する」旨の指摘は 4 点。その他は，基本的に 0 点。

［設問3］

(1) f は，解答例どおりのみ 2 点。

(2)「FW の設定ミス」と「TCP135 番ポートを使用した」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。「FW の設定ミスによってインターネットへの通信が許可されていた」旨は 3 点としたが，「社内セグメントからインターネットへの通信が可能な状態であった」旨の指摘は，問題文の状況を的確に把握していないと判断し 0 点とした。

［設問4］

(1) g は，解答例どおりのみ 2 点。

(2) 機器名，LAN ポート名ともに，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 8 点。内容が今一歩のものは 4 点。その他は 0 点。

【講評】

正答率は，想定していたよりも比較的低かったように思います。その要因としては，VLAN に関する理解が必ずしも十分ではないこと，記述式の問題に的確に解答しきれていなかったことなどが考えられます。

設問 2 (3)では，POP 通信におけるパスワードの盗聴対策を求めましたが，単に POP 通信を暗号化するなどの漠然とした解答が多く見られました。また，設問 3 (2)では，ワーム F が E 社内から FW を通過した理由を，問題の記述内容に沿って考えてもらうことを期待しましたが，TCP ポート 135 番を使って感染したことを指摘した解答は，非常に少なかったようです。また，設問 4 (3)も，検査方法が必ずしも明確に指摘されていないものが多く見受けられました。

記述式の問題は，設問で問われていることに対し，的確に解答していくことが必要です。問題の記述内容のほか，各自が吸収した技術知識などに基づきながら，的を射た解答を作成していくようにしましょう。

問3 Web サイトのセキュリティ

【採点基準】

［設問1］

(1) a ～ e 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) 方式は，解答例どおりのみ 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。
(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2］
(1) f ～ 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 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。

【講評】

午後 I の 4 問の中では，最も選択者数の少ない問題でした。セキュアプログラミングに関する問題は，ある程度の経験が必要になることがあります。本番の試験では，4 問のうち，2 問を選択すればよいので，得意としない受験者は，選択しないことが得策でしょう。

設問 1 は，ほとんどが知識問題ですから，間違えた問題については，再度，確認しておきましょう。また，設問 2 (1)については，問題の条件を考慮しながら考察すれば，空欄 f ～ h については，必ず正解できる問題です。しかし，空欄 i は，4 ビットで 1 文字が構成されていることに注意しないと，正解できないようになっているので，少し難しい問題です。ちなみに，空欄 f ～ i の全問正解者は少数だったと思います。設問 2 (3)では，共通鍵の長さが 128 ビットから 120 ビットになることによって安全性が低くなっている理由を解答として求めました。このため，可変部分が 60 通りしか現れないなどの理由を指摘した解答は，すべて 0 点にしました。

問4 認証システム

【採点基準】

［設問1］
(1) a，b 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各 4 点。その他は，基本的に 0 点。
(3)「所属が変更になると，公開鍵証明書が失効する」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) U 主任が行うべき処置，C 君に対して指示すべき処置ともに，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 6 点。その他は，基本的に 0 点。
(2) 発行申請前，取得後ともに，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 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。

【講評】

午後 I の 4 問の中では，平均点が最も高くなると想定していましたが，結果的には 23.8 点であり，想定よりも低い点数でした。その要因としては，やはり記述式の問題に対して，的確に解答が作成されていないことが挙げられると思います。

例えば，設問 1 (3)では，PKI の導入計画として，問題文に「人事異動で失効にならないよう設計に留意する」と明記されています。このため，公開鍵証明書に所属を入れると，人事異動で失効する旨を指摘する必要があります。こうした観点，つまり問題文の記述内容に照らし合わせた答案は，非常に少なかったように思います。また，設問 2 (3)は，解答字数が 80 字と多くなっていますが，ディジタル署名に使用する場合と，クライアント認証に使用する場合の違いに分けて，分かりやすく解答を作成することが必要です。

まずは，問題文の記述内容を的確に反映した答案を作成する力をつけていくようにしましょう。

＜午後Ⅱ＞

問1 大学のキャンパスシステムの再構築

【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 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2］
(1) c ～ f 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。
(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) g ～ i は，解答例どおりのみ各 3 点。
(2) 24 バイト以上と指摘しているものに対し 6 点。24 バイトを超える表現は 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 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。
（3）機能名は，解答例どおりのみ 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。

【講評】
問 1 は，無線 LAN とセキュアプログラミングを組合せた問題であったことから，選択者数が極端に少なく，正答率も全体として低かったようです。
SC 試験で合格をかち取るには，情報セキュリティ技術に関する知識レベルをできるだけ向上させていくことが必要です。例えば，共通鍵暗号方式の暗号化や復号の処理が，公開鍵暗号方式よりも速い理由は，設問 1 (2)の事例でも分かるように，暗号化や復号の処理に排他的論理和（XOR）を用いていることなどにあります。本試験に向け，こうした基本的な事項をよく理解しておくようにしましょう。
設問 2 は，無線 LAN におけるセキュリティ問題が中心となっているので，難易度的には少し難しいと思います。しかし，SC 試験では，様々な角度から問題が出題されますので，模試などで一度，取り組んだことのある問題については，それらに関連する技術知識をできるだけ多く吸収しておくとよいでしょう。
設問 3 (2)では，スタックの積まれ方に注意して解答を考えることが必要です。なぜ 24 バイト以上になるのか（24 バイトを超えるとなぜ正しくないのか）といったことについては，解説をよく読んで，十分に理解しておきましょう。
設問 4 (3)では，メモリリークが多発する（ガーベジコレクションが行われない）と，サーバなどに対する DoS 攻撃に使われることも理解しておきましょう。

問2 システムセンタのバックアップとリモートアクセス

【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 8 点。内容が今一歩のものは 4 点。その他は 0 点。
（3）解答例と同様の趣旨（DNS サーバの冗長化になること）が適切に指摘されているものに対し 8 点。その他（DNS サーバの負荷分散など）は，基本的に 0 点。
（4）d ～ f は，解答例どおりのみ各 3 点。
［設問2］
（1）g ～ k 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。
（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）l ～ o 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。
（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 8 点。その他は，基本的に 0 点。

【講評】
全体の 8 割を超える受験者が問 2 を選択していました。また，平均点では，問 1 が 23.2 点だったのに対し，問 2 は 31.3 点で，結果的には問 2 の方が高くなりました。なお，午後 I の平均点に比較すると，午後Ⅱは技術的な内容が多かったことなどから，全体的に低かったように思います。
午後Ⅱ試験に限らず，午後 I 試験に取り組む際には，必ず設問の指示に従うことを忘れないようにしてください。例えば，設問 1 (1)の空欄 a ～ c は，「ルータ名を答えよ」と指示されているにもかかわらず，ルータ名で答えていない答案がかなりありました。本番の試験では，必ず設問の指示に従って，解答を作成することが重要だと思います。
技術的な観点からは，VPN 技術は重要です。IPsec の鍵交換の仕組みなどは，平成 19 年度春期テクニカルエンジニア（情報セキュリティ）試験の午後Ⅱ問題のほか，IPsec-VPN や SSL-VPN などに関する問題が，平成 20 年度秋期テクニカルエンジニア（ネットワーク）試験の午後Ⅱとして出題されていますので，技術的な仕組みなどは，しっかりと理解しておきましょう。また，IEEE 802.1X／EAP などのセキュリティプロトコルも，よく出題されています。VPN 技術をはじめ，セキュリティプロトコルに関する技術知識は，理解するのに難解な点も多々ありますが，できるだけその本質となっている仕組みを十分に把握し，本番の試験に備えるようにするとよいでしょう。

以上