2012 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

2012 年 2 月 15 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，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，想定していたよりも正答率が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 22.0 点，問 2 が 19.7 点，問 3 が 29.0 点，問 4 が 21.6 点，全体の平均点は 45.5 点でした。一方，午後Ⅱ（100 点満点）は，問 1 が 26.3 点，問 2 が 31.0 点で，問 2 の方が少し高くなりました。なお，午後Ⅱの平均点では，29.9 点です。問題ごとの選択率は，午後 I の問 1 が 25.7%，問 2 が 25.7%，問 3 が 21.0%，問 4 が 27.6%でほぼ均衡していました。これに対し，午後Ⅱの問 1 は 22.1%，問 2 が 77.9%という状況で，かなり偏っていました。

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，解答を考えるようにしましょう。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 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】

平均正答率は 43.9%（平均点は 22.0 点）であり，ほぼ想定どおりでした。

設問 1 (1)の空欄 b は，情報セキュリティにおける基本用語（機密性，完全性，可用性，真正性，責任追跡性，否認防止など）の中から，適切なものを答えるものです。これらの用語は，基本中の基本ですから，正確に覚えておきましょう。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。その検証方法については，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（鍵付きハッシュ）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ようにしましょう。

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 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】

平均正答率は 39.4%（平均点は 19.7 点）であり，想定していたよりも若干，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 ソフトウェアの脆弱性への対応

【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 6 点。ただし，「Exploit コードが公開されている」という答案は，単に図 3 の脆弱性情報の引用にすぎないことから 3 点。その他は 0 点。

［設問2］

(1) a は，解答例どおりのみ 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 6 点。その他は，基本的に 0 点。

(4) 記号は，解答例どおりのみ 2 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。「限定された権限」と指摘したものは 3 点。その他は 0 点。

［設問3］

(1) 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 3 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】

平均正答率 58.0%（平均点は 29.0 点）であり，想定していたよりも，よく出来ていたと思います。

設問 1 (2)の解答については，その多くが「Exploit コードが公開されている」というものでした。この設問では，図 3 の脆弱性情報そのものではなく，なぜ攻撃を行うことができるのかという視点に立った解答を作成することが必要です。例えば，Exploit コードは何のために作成されているかを知らなくても，解答が作成できるようなケースでは，その本質はどこにあるかといった視点に立って解答を作成するようにするとよいでしょう。問題文の記述に着目して解答を作成することは，極めて重要なことですが，設問で問われていることをよく考慮しながら解答を考えていくことが必要になるケースもあります。

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】

平均正答率は 43.2%（平均点では 21.6 点）であり，想定よりも低くなりました。その要因としては，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などが挙げられると思います。

例えば，設問 1 (2)は，パスワードが利用者にとって負担になる問題を求めていましたが，単にパスワードを扱う際の問題点などを指摘しているものが見られました。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」と記述されています。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が，こうした観点の答案は，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とよいでしょう。

＜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み合わ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おくことが必要です。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とよいでしょう。

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。

(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) 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 割近くの受験者が問 2 を選択していました。また，平均点では，問 2 は 31.0 点で，問 1 の 26.3 点を少し上回りました。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 I 試験に限らず，午後Ⅱ試験に取り組む際には，必ず設問の指示に従うことが必要です。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大切です。

VPN 技術については，これまでのテクニカルエンジニア（情報セキュリティ）試験や，テクニカルエンジニア（ネットワーク）試験の午後問題などとして頻出されるテーマでしたから，IPsec-VPN，SSL-VPN，PPTP，PacketiX などの基本的な仕組みはよく把握しておきましょう。また，無線 LAN のセキュリティ問題や IEEE 802.1X／EAP などのセキュリティプロトコルも，出題されることもあります。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するように努めましょう。

以上