2009 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

2009 年 3 月 18 日 (株)アイテック 情報技術教育研究部

■ 全体講評

情報セキュリティスペシャリスト試験は，試験制度の改正に伴い，4 月の試験が最初の試験となります。従来のテクニカルエンジニア（情報セキュリティ）試験と，ほぼ同等の位置付けの試験とされていますので，午後試験では，主に技術的な問題が出題されると考えられます。ただし，試験センターは，情報セキュリティアドミニストレータ試験の内容を内包したものになると発表していますので，情報セキュリティマネジメント系の問題も出題されると想定されます。そこで，今回の模試では，午後Ⅰ試験の問題の 4 問のうち，1 問をマネジメント系中心の問題にしました。

午後Ⅰ試験は，4 問の中から 2 問を選択すればよいので，得意分野の問題を選ぶことができます。このため，午後Ⅰ試験の正答率は，全体的に上がると考えていました。しかし，採点結果から判断すると，午後Ⅰ試験の正答率は少し低めという印象を受けました。これに対し，午後Ⅱ試験は，そのほとんどが技術的な問題であったにもかかわらず，午後Ⅰ試験に比較すると，正答率はよかったと思われます。中には，高得点の方も見受けられ，本番の試験に向けて準備がよくなされているという印象を受けました。

一方，自分が得意としない分野の問題であったり，準備が十分にできないまま受験されたりした方もいらっしゃると思います。このような場合には，模試の判定にこだわることなく，4 月 19 日の本試験に向け，十分にレベルアップを図っていくことが大切です。例えば，試験日までの残された 3 週間程度を有効に使い，模試の解答・解説などをよく読んだりして，自分自身で関連する技術内容を含め，しっかり把握できるようにしておいてください。

次に，午後Ⅰ試験と午後Ⅱ試験の状況を簡単に紹介しておきます。午後Ⅰ試験は，問 4 の選択者の割合が 75%強と最も多く，次いで問 3，問 2，問 1（25%弱）という順でした。問 1 は C/C++に関するセキュアプログラミングの問題でしたから，選択対象から外した受験者が多かったと考えられます。テクニカルエンジニア（情報セキュリティ）試験の出題傾向から判断すれば，今春の試験でもセキュアプログラミングに関する問題が出題されることは，ほぼ間違いないと考えられます。しかし，午後Ⅰ試験は，4 問の中から 2 問を選択すればよいので，セキュアプログラミングの問題を得意としない場合には，選択対象から外し，改めて準備をする必要はないでしょう。あくまでも，午後Ⅰ試験は，得意分野の問題を選択するようにしてください。

午後Ⅱ試験の問 1 と問 2 の選択者の比率は，約 3 対 7 という状況でした。問 1 は，無線 LAN のセキュリティとセキュアプログラミングの問題でしたから，問 2 を選択した方が，多かったということでしょう。また，平均点でも，問 2 のほうが高かったように思います。このため，模試の総合評価は問 1 の選択者には厳しく，問 2 の選択者には甘く出るかと思いますので，模試の判定結果は一つの目安として考えてください。いずれにしても，4 月の試験で最大限の力を発揮し，良い結果を残すことが大切です。

なお，今回の模試の採点状況から判断すると，答案の中には問題の条件を考慮していなかったり，設問で問われていることに対し適切に解答していなかったりするものが多く見受けられました。特に，記述式問題については，設問で何が問われているかを必ず確認し，解答を作成することが重要です。また，不要な修飾語はできるだけ削除し，ポイントになる内容を分かりやすく記述することが必要です。今回の模試でも，設問で問われていること以外の内容を答えているものや，むだな修飾語が多く，肝心なことが記入できていないようなものも数多く見受けられました。これらの点については，本番の試験までには，ぜひ修正してほしい事項です。また，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持って，午後Ⅱ試験の最後まで全力を出し切り（あきらめず）問題に取り組み，ぜひ合格するようにしてください。

＜午後Ⅰ＞

問1 プログラム開発のセキュリティ

[訂正とお詫び]

設問 3 (2)において，「本文中の下線について，…」とすべきところ，「本文中の下線②について，…」となっておりました。「下線②」ではなく，正しくは「下線」です。お詫びして訂正させていただきます。

[採点基準]

[設問1]

a ～ g は，解答例どおりのみ各 2 点。ただし，空欄 a については，文字列長に順ずる表現であればよい。

[設問2]
（1）解答例および，それと同等の表現に対し 2 点。
（2）「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 8 点。「オーバフローし，9，0 があふれた」などの表現は 4 点。その他は 0 点。
（3）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 8 点。内容が今一歩のものは 4 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]
言語の詳細を問うような問題が一部，含まれていたためか，全体的な正答率は，想定していたよりも低かったようです。

個別の設問では，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。なぜならテクニカルエンジニア（情報セキュリティ）試験では，「セキュアプログラミング講座」の中の題材をもとに出題していることが多かったからです。

問2 リモートアクセス環境の構築

[採点基準]
[設問1]
（1）a 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 6 点。その他は，基本的に 0 点。
[設問2]
（1）b ～ 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。内容が今一歩のものは 3 点。その他は 0 点。
（3）TCP のチェックサムエラーを発生させる理由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 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 4 点。その他は，基本的に 0 点。

[講評]
セキュリティプロトコルを中心とした問題でしたから，正答率は，午後 I 問題の 4 問の中では，最も低かったように思います。

リモートアクセス環境を構築するためには，通信の安全性を確保する必要性から，一般に VPN を構築することがよく行われます。この VPN については，通信相手の真正性，通信の機密性（暗号化），送受信するメッセージの完全性（メッセージ認証）という三つの要素を満たすことによって，はじめて安全性が確保されます。このことは，よく理解しておく必要があります。なお，暗号化すればメッセージ認証は必要ないと考えている人が，かなりいます。しかし，送受信されるメッセージは，暗号化していたとしても“0”，“1”のビット列に過ぎません。このため，メッセージの伝送途中で“0”を“1”に変更されると，受信側には誤ったメッセージとして届いてしまいます。例えば，ソフトウェアのコードが機能しなくなったり，1 が 100 になってしまったりします。したがって，セキュリティを高めるためには，こうしたことはすべて排除できるようにしておくこと（メッセージ認証を行うこと）が必要になります。

このように，情報セキュリティに関する問題を考えていくには，問題の本質はどこにあるのかといったことなどをよく考えるようにすることが必要です。

問3 情報セキュリティマネジメントの見直し

[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）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。
（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。内容が今一歩のもの，例えば，外部から内部への能動型の攻撃は禁止できる旨の指摘がなされていないものは 3 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 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。

[設問4]

（1）USB メモリにパスワードを設定する旨が，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。
（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]

正答率は，全体として少し低かったようです。その要因の一つとしては，設問 1 の穴埋め問題の正答率がかなり低かったことが挙げられます。助言型監査，保証型監査は，基本的な用語なので，よく覚えておきましょう。このほか，設問 2 (2)の正答率も，あまりよくありませんでした。

また，この問題では，設問で問われていること以外の内容を答えているケースも，多く見受けられました。例えば，設問 3 (1)では，ファイアウォール（FW）の設定内容が問われているにもかかわらず，FW で行う検査内容を答えたり，外部，内部，HTTP という三つの字句を用いないで解答を作成したりしている例がありました。また，設問 3 (2)では，メールソフトの設定を答える必要があるのに対し，テキスト形式のメールだけを受信するなど，受信方法などを答えているものが多くありました。本番の試験では，設問の指示に忠実に従って解答を作成していくようにしてください。

問4 ログ管理

[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）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。
（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（信頼できるディジタル署名で時刻情報を保証すること）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（記憶容量の増大とコストの増加を抑制すること）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，全体として高かったようです。さらに，設問で問われていることに注意しながら解答を作成していけば，得点はもっとアップしていくと考えられます。例えば，設問 2 (2)は，インターネット上にある NTP サーバから時刻情報を取得する方法について，可用性（認可されたエンティティが要求したときに，アクセス及び使用が可能である特性）の面から答えるものです。しかし，ネットワークの輻輳や，時刻の正確性などを指摘したものがありました。本試験では，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。

なお，時刻認証で使用される時刻については，TSA などの信頼できる第三者のディジタル署名によって保護される必要があります。それは，ディジタル署名を復号した結果と，タイムスタンプトークンにある時刻情報を比較し，両者が一致すれば時刻情報が改ざんされていないことが分かるからです。

＜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 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。

[設問2]

（1）c ～ 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。
（3）運用上の観点，防御上の観点とも，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 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。
（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 3］

（1）g ～ i は，解答例どおりのみ各 2 点。
（2）24 バイト以上と指摘しているものに対し 8 点。24 バイトを超える表現は 4 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）名称は，解答例どおりのみ 2 点。内容は，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 4 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，選択者数が少なく，正答率も全体として低かったようです。

情報セキュリティスペシャリスト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。

また，設問 3 (2)では，この問題における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 バイトを越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，十分に理解しておくことが必要です。

問 2　検疫ネットワークの構築

［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 8 点。内容が今一歩のものは 4 点。その他は 0 点。

［設問 2］

（1）f，g 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，例えば，社内ネットワークにアクセスできる字句がなく，IP アドレスを手動設定するなどの解答は 4 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。
（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。内容が今一歩のものは 4 点。その他は 0 点。

［設問 3］

（1）h 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）理由，対策とも，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 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）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 10 点。内容が今一歩のものは 5 点。その他は 0 点。

［講評］

全体として，正答率は高かったようです。個別の設問では，設問 1，2 の正答率は，それほど高いというわけではありませんでしたが，設問 3，4 は予想以上によくできていました。

なお，設問 3，4 の正答率が高いという理由は，各受験者が問題文に記述された内容を，よく把握しながら解答を作成した結果であると考えられます。高度試験では，特に問題の記述内容に沿って考察していくことが重要です。午後Ⅰ試験の答案では，問題の記述内容や設問の指示に従ったものは，それほど多くなかったと思われますが，この問題のように，問題の記述内容などをベースにしながら考えていけば，正解を導いていくことができます。本試験でも，こうした姿勢で臨むことを忘れないようにしてください。

以上