2009 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

2009 年 2 月 20 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，どれだけ身についているかを診断することを主な目的としています。また，新しい試験制度のもとで実施されることから，従来の試験との変更点などを確認することも必要です。例えば，従来のテクニカルエンジニア（情報セキュリティ）試験の午後Ⅰ試験は，4 問の中から 3 問を選択していました。しかし，SC 試験では，4 問の中から 2 問を選択して解答します。今回の総合実力診断模試では，3 問選択された受験者が少し見られました。そうした場合，本番の試験では最初の 2 問しか採点されませんので，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，どれだけ点数がとれ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いてください。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出題されると想定されます。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始め，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のみならず，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。SC 試験は，基本的にテクニカルエンジニア（情報セキュリティ）試験の延長線上にある試験ですから，出題内容は，かなり高度な技術分野から出題されると考えられます。なお，試験問題を考えていくうえでは，問題文に記述されている内容の範囲内で解答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つけていなければ，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していくことができません。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。本番の試験までは 1 か月半もありますから，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，かなり有望と考えられますが，すで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。一方，D または 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 試験でも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，そのうえ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ります。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うえで，解答を作成していけばよいのです。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必要だということです。

＜午後Ⅰ＞

問1 電子メールのセキュリティ

[採点基準]

[設問1]

（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 6 点。その他は，基本的に 0 点。

（3）「通信相手の認証」，「メッセージの改ざんを検出」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，それぞれ 4 点。その他は，基本的に 0 点。

[設問2]

（1）e～h は，解答例どおりのみ各 2 点。

（2）「秘密鍵は署名者本人しか所有していない」旨のキーワードが適切に指摘されているものに対し 6 点。その他は，基本的に 0 点。

[設問3]

(1) 比較対象および理由とも，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 4 点。その他は，基本的に 0 点。

(2) UDP のメッセージ長の制限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]

設問 1 の空欄 d は，ローカル IP という解答が見られました。RFC では，プライベート IP アドレスという用語を使用しているので，プライベートという字句で覚えておきましょう。なお，全体として正答率は低かったようです。

ネットワークを流れる電子メールの大半は，迷惑メールであるといわれています。このため，電子メールのセキュリティ対策としては，迷惑メール対策を理解することが必要です。そのためには，まず，電子メール転送に関する技術的な仕組みを把握しておかなければなりません。ISP ではボットなどが動的 IP アドレスを使って迷惑メールを送信することを防止するため，OP25B などの対策を実施しています。なぜ，OP25B が有効なのか，あるいは OP25B 適用時の問題は何かなどといったことのほか，SPF/SenderID や DKIM などの新しい送信ドメイン認証といった技術を含め，幅広く理解していくようにしましょう。

問2 Web の私的利用

[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)「プロキシサーバからのインターネット側への攻撃」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。内容が今一歩のものは 3 点。その他は 0 点。

(2) VLAN の構成ならびに VLAN 間の通信を禁止する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]

ログ検索用 Web アプリケーションを操作したログを記録する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) 送信元限定条件の指摘が適切にな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。

(2)「送信元限定条件に利用者を加える」，および「利用者 ID のログを採取する」旨が両方とも指摘されているものに対し 6 点。片方の指摘しかない場合は 3 点。その他は 0 点。

(3)「アクセス許可された通信のログを採取する」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。

[講評]

設問 1 は，空欄に入れる字句を選択する問題ですから，正答率は高かったと思います。欲を言えば，全問正解してほしい問題です。設問 2 は，少し技術的な問題でしたから，的を射た解答は少なかったようです。設問 3 は，プライバシ保護の趣旨に反した調査が行われないようにする技術的な対策を答える問題でしたが，監査のための操作ログを取得する旨を指摘した答案は，比較的少なかったようです。

設問 4 は，フィルタリングの条件を解答するものです。答案を見た限りでは，図 3 の「R 社フィルタリングソフトの概要」の内容を十分に確認しないで，解答を作成しているように見受けられました。試験では，与えられた問題の条件の範囲内で解答を作成していくことが基本です。設問 4 では，「R 社フィルタリングソフトの機能を踏まえ」と指示されているので，この条件に素直に従って解答案を考えていくことが必要です。設問の指示に忠実に従うことが点数アップの基本ですから，本番の試験では，設問で問われていることを必ず確認したうえで解答を作成するようにしてください。

問3 リモートアクセスシステムの構築

[採点基準]

[設問1]

a～g 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，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) 解答例どおりのみ 3 点。

(2) 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 6 点。その他は，基本的に 0 点。

(4)「SV の公開鍵をすり替える」旨を指摘する場合には中間者攻撃というキーワードが必要であり，これらが適切に指摘されているものに対し 6 点。中間者

攻撃が指摘されていない場合などは 3 点。その他は 0 点。もう一つは「アドレス詐称を行い，偽のサーバを構築する」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]

設問 1 の空欄 f，g は，情報セキュリティの 3 要素の用語が正しく覚えられていなかったようで，正答率は比較的低かったようです。3 要素とは，通信の機密性（暗号化），通信相手の真正性（ユーザ認証），メッセージの完全性（メッセージ認証）のことですから，正確に覚えておきましょう。

設問 2 (1)は，公開鍵証明書（サーバ証明書）が正しいかどうかは，その証明書に改ざんがないかどうかによって確認します。その方法としては，CA の署名を CA の公開鍵で復号した結果と，公開鍵証明書から求めたハッシュ値が一致するかどうかで判断します。認証技術は，二つのものを比較することによって正しいかどうかを確認しますので，この点はよく理解しておきましょう。

設問 3 (1)は，比較的正答率が高かった半面，(2)は想定よりも低い正答率だったように思います。公開鍵暗号方式の仕組みも基本技術の一つですから，しっかりと理解しておきましょう。

問4 プログラム開発におけるセキュリティ対策

[採点基準]

[設問1]

a～h は，解答例どおりのみ各 2 点。

[設問2]

（1）x～z 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]

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]

平成 19 年度春期のテクニカルエンジニア（情報セキュリティ）試験で出題された午後Ⅰ問 1 をベースにした問題です。セキュアプログラミングを選択する受験者は，ある程度，限られるので，選択者数は，午後Ⅰの 4 問の中では，最も少なくなっていました。

問 4 は，C 言語などを理解している受験者が選択したためか，正答率はそれほど低くなかったようです。しかし，設問 2 (1)の空欄 x～z に入れる数値は，地道に計算をしないで解答したようなところが見られ，正答率は比較的低かったようです。なお，バッファオーバフローについては，バッファの終端を示すナル文字の扱いがポイントになるので，この点はよく理解しておきましょう。

＜午後Ⅱ＞

問1 Web サイトのセキュリティ

[採点基準]

[設問1]

（1）a～c は，解答例どおりのみ各 2 点。

（2）ヘッダ名の Referer を記述し，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）「ランダムに生成する」旨の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。

（4）「セッション ID を書き換える」，「URL を絶対パスに書き換える」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）ユーザ ID，旧パスワード，新パスワードの三つとも正しい場合だけ 8 点。

（2）解答例どおりのみ各 3 点。

（3）方法は「バインドメカニズム」，もしくは「プリペアドステートメント」というキーワードが指摘されているものに対し 4 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 6 点。その他は，基本的に 0 点。

[設問3]

（1）d～j は，解答例どおりのみ各 2 点。

（2）方法，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 6 点。その他は，基本的に 0 点。

（3）「SSL の暗号化を解く」，「クッキー情報によって振り分ける」の二つ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。

（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）「NTP サーバから時刻情報を受け，時刻同期を行う」旨が適切に指摘されているものに対し 8 点。なお，「時刻同期をとる」など，NTP サーバからの供給を受ける旨が指摘されていない場合は 4 点。その他は 0 点。

[講評]

受験者は, 問 1 のほうが難しいと判断したようであり, 問 1 と問 2 の選択者の比率は, ほぼ 1 対 2 という状況でした。また，平均点で見ても問 1 が約 30 点だったのに対し，問 2 が約 45 点でした。本番の試験では，問 1 と問 2 で, このような差があっても点数調整は行われないと考えられますので, 自分が得意とする分野の問題を選択することが重要になってきます。

設問 1 は，比較的正答率は高かったようですが，Web アクセス時における GET と POST メソッドの使い方，HTTP ヘッダの使い方は，自分なりに整理し，よく理解しておいてください。

設問 2 は，一部の受験者を除き，正答率は低かったようです。攻撃手法などは，できるだけ多くの事例を研究して，その手法などの理解を深めていってください。

設問 3 (1)は，正答率は比較的高かったようですが，空欄 g に入れる字句として, VIP という答案が見られました。VIP でアクセスするのは間違いありませんが，VIP はどの装置が持つ IP アドレスであるかを答える必要があります。(3)では，負荷分散装置が SSL アクセラレータを実装しているので, SSL アクセラレータが SSL の暗号を解き, HTTP ヘッダにあるクッキー情報によって振分け先の Web サーバを決めています。試験で合格するには，こうした基本事項を一つひとつ積み重ねていくことが必要ですから，地道に努力していきましょう。

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～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 6 点。内容が今一歩のものは 3 点。その他は 0 点。

[設問2]

（1）e～g 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。

（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）h～j 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）k 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。

（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 のアドレスに書き変わる」旨のキーワードが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。

（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。その他は，基本的に 0 点。

[講評]

全体的に，正答率は高かったようです。なお，正答率が低かった個別の設問としては，設問 2 (2)や(3)，(5)のほか，設問 3 (2)，設問 5 (1)や(2)の検知できなかった理由などがあります。

IPsec については，通信する両端の装置が，IP パケットの暗号化やメッセージ認証に使用する共通鍵を作成する必要があります。しかし，安全でない通信路を使って，共通の秘密情報を作り出すことが必要になります。そこで, IKE というプロトコルを使って鍵交換を行います。IKE には，いくつかの方式が規定されています。その中で, 事前共有鍵方式は, Diffie-Hellman という鍵配送方式を使って, それぞれの装置が持つ秘密情報から作成された公開値を通信路に流し, 相手から受け取った公開値と自分自身の持つ秘密情報から, 共通の情報を作り出すというものです。こうした技術的に突っ込んだ内容が，平成 19 年度のテクニカルエンジニア（情報セキュリティ）試験で出題されています。このため，SSL や IEEE802.1X，さらに無線 LAN の暗号化方式などについても, 詳細な技術内容が出題される可能性があります。

以上のように, 情報セキュリティ技術の本質を理解していくには，こうしたことを積み重ねていくことが必要になります。着実にレベルアップを図りながら，試験での合格を目指すようにしていきましょう。

以上