2010 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

2010 年 3 月 20 日 (株)アイテック 商品開発本部

■ 全体講評

今回の公開模試の採点結果から判断すると，4 月の本試験に向けて，準備がかなり進んでいる受験者と，まだまだ準備不足と思われる受験者に大別されるように感じられます。このため，全体の平均点は，少し低めだったと思います。ちなみに，午後 I 全体の平均点は 37.4 点でした。問題別では，問 1 が 20.2 点，問 2 が 13.9 点，問 3 が 19.1 点，問 4 が 21.2 点でした。午後Ⅱ試験は，全体の平均点が 38.2 点で，問 1 が 36.4 点，問 2 が 39.3 点という結果でした。なお，午後Ⅱの高得点者は，問 2 の選択者に多く見られました。

今回の公開模試の答案を見ると，問題で記述された内容，あるいは設問で指示されていることなどに従わず，各自が持ち合わせている知識や先入観などに基づいて解答を作成していると思われる答案が数多く見られました。問題の記述内容や設問の指示に従って答案を作成することが、合格するための絶対条件となります。4 月の本試験では，こうしたことに留意してほしいと思います。また，記述式の問題では，項目を複数，羅列した答案も見られましたが，こうした解答方法は避ける必要があります。それは，情報セキュリティスペシャリスト試験などの記述式問題では，それぞれの設問で求める解答は基本的に一つの内容を答えさせるようにしているからです。そこで，項目を複数挙げるのでなく，例えば，主語と述語，あるいは目的語は何かなどを明確にした上で解答を作成するようにしてください。例えば，設問で具体的に述べよと指示されている場合があります。こうしたケースでは，必要最小限の範囲に対してだけ権限を与えるなどの解答としてしまうと，具体的とは見なされません。権限が与えられるべき範囲を問題の記述から導き出し，それを具体的に表現することが必要です。

次に，問ごとの選択状況を紹介しておきます。午後 I 試験は，4 問の中から 2 問を選択しますので，平均的な選択率は 50%になります。今回は，問 1 と問 2 がネットワーク系，問 3 がデータベース系，問 4 が情報セキュリティマネジメント系を中心とした問題でしたから，選択率は，かなり偏っていました。具体的には，問 1（SIP と RTP のセキュリティ）の選択者が 26%，問 2（Web システムのセキュリティ）が 54%，問 3（データベースのアクセス制御）が 40%，問 4（情報漏えい防止対策）が 80%でした。午後 I 試験では，得意とする分野の問題を早く見極め，その問題で，できるだけ得点するようにしましょう。例えば，得意分野の問題で 40 点近くの点数を獲得できれば，もう一つの問題で 20 点強を得点すれば，午後 I 試験はクリアすることができます。そのためには，問題の記述内容を十分に把握できるだけの技術力が必要とされます。本番の試験日までの期間で，より一層のレベルアップを図るようにしましょう。

午後Ⅱ試験では，問 1（データベースのセキュリティ対策）の選択者が 38%，問 2（ネットワークのセキュリティ）が 62%という割合でした。なお，春期の情報セキュリティスペシャリストの午後Ⅱ試験では，様々な分野から総合問題になることが多いので，できるだけ各自が得意とする分野から構成されている問題を選択するようにしましょう。また，一度，選択した問題は最後までやり遂げることが大切です。専門知識を有していなければ解答できない問題も一部含まれていますが，多くの設問は，問題文で記述された内容に基づいて考えていけば，正解を導いていくことが可能なように工夫されています。設問で問われていることを十分に確認し，問題の記述内容と照らし合わせながら解答を導いていくようにしましょう。そして，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してください。試験当日は集中力，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）問題に取り組んで，ぜひ合格するようにしてください。

＜午後 I ＞

問1 SIP と RTP 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）TLS の利用は TCP が前提となっている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。

（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。ただし，e はクライアント，f はサーバでもよい。

（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て 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て 6 点。内容が今一歩のものは 3 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て各 4 点。単に VPN を構築するなどの指摘は 2 点。その他は 0 点。

【講評】
SIP と RTP のセキュリティをテーマにした問題でしたから，選択率は最も低くなりました。その半面，選択者が限られたことから、正答率はまずまずでした。
設問 1 (1)や設問 2 (1)は，セキュリティの基本的な穴埋め問題です。全問正解できるように，基本的な技術用語については，よく覚えておきましょう。また，空欄 e と f は，逆に答えた解答も多くありましたが，公開鍵証明書の使い方や，その検証方法などについては，十分に理解しておきましょう。
設問 2 (2)は，公開鍵を使って秘密情報を送信する基本的な問題でした。正答率は高いと想定していましたが，必ずしもそうとは言い切れませんでした。
設問 2 (3)については，MAC（メッセージ認証コード）を生成する際の留意点を，よく理解するようにしましょう。例えば，メッセージの改ざんを検出するには，送信メッセージのハッシュ値をとって，それを通信相手に送れば，改ざんを検出できるというように考えてはいけません。ハッシュ値を生成する場合には，通信する 2 者間で共有する認証鍵（MAC シークレット）を使用しなければ，全く役に立たないということです。それは，送信メッセージとハッシュ値を盗聴され，改ざんしたメッセージとそのハッシュ値に差し替えられた場合には，受信者は，それを改ざんのない正しいメッセージとして受信してしまうからです。そこで，認証鍵などの秘密情報を必ず使用する必要があるのです。そして，HMAC では認証鍵（この問題では，マスタシークレットを認証鍵として使用します）とメッセージを用いて，ハッシュ値を生成するようにしています。

問2 Web システムのセキュリティ

【採点基準】
［設問1］
a ～ d は，解答例どおりのみ各 2 点。ただし，a はホスト名，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。
(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) アは，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。
(2) 解答例と同様の趣旨が適切に指摘されているもののほか，「外部の IP アドレスからキャッシュサーバあての DNS クエリパケット」という旨の指摘に対し 6 点。外部の IP アドレスから DMZ あての DNS クエリパケット（この表現では，コンテンツサーバに対する正規の DNS クエリパケットも含まれ，正規のパケットまでも遮断してしまう）などの指摘は，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。内容が今一歩のものは 3 点。その他は 0 点。

【講評】
DNS に関するセキュリティに詳しい受験者は高得点でした。しかし，記述式の解答が多く，必ずしも適切に表現できていなかったことなどから，全体として正答率は最も低くなりました。
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 (2)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ようにしましょう。

問3 データベースのアクセス制御

【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) 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)「共有する従業者の中で最大のアクセス権限を付与する」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。その他は，基本的に 0 点。

［設問3］

(1) b は，解答例と同様の用語に対してのみ 2 点。

(2) 一般社員か，派遣社員のいずれか一方が適切に指摘されていれば 6 点。その他は，基本的に 0 点。

［設問4］

(1) c は，解答例と同様の用語に対してのみ 2 点。

(2) d は，解答例どおりのみ 4 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5］

(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。

【講評】

この問題の選択者は，データベース技術を理解している受験者が多いと想定されるので，全体として正答率はまずまずという結果でした。

この問題でも，設問で指示された以外のことを解答したり，問題の条件の確認が不十分だったりしたと思われるようなところが，幾つか見受けられました。例えば，設問 2 (2)の設問の指示は，「アクセス制御の観点から」という指示にもかかわらず，「アカウントの共用はアクセスした人を特定できない」などの責任追跡性の理由を指摘したものが，かなりありました。

設問 4 (3)では，データベースアクセスツールを用いて，直接データベースを操作するという不正アクセスのリスクが低減できる理由を求めました。しかし，問題文の記述内容に基づき，アクセスツールでは，ユーザ情報を用いないのでアクセスできないことを指摘した解答は，非常に少なかったと思います。

問4 情報漏えい防止対策

【採点基準】

［設問1］

(1) a ～ g は，解答例どおりのみ各 2 点。

(2) PDCA のサイクルを回す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) 添付ファイルの送信方法について Cc を設定する旨が適切に指摘されているものに対し 6 点。上長の承認を得た上で送信を許可する旨の指摘などは，基本的に 3 点。その他は 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。

【講評】

穴埋め問題が記号選択であったほか，ISMS 関連の問題が中心でしたから，大半の受験者が選択していました。正答率は，午後 I の 4 問の中では最も高くなりましたが，期待通りの点数ではありませんでした。

その要因は，問題の記述内容に従って，解答したものが少なかったことが挙げられます。例えば，設問 1 (2)の指示は，「ISMS のプロセスアプローチの観点」から解答を作成することです。プロセスアプローチとあるので，PDCA のサイクルを思いつくと考えていましたが，答案の中には「可搬媒体に関する運用ルール，技術的なセキュリティ対策には取り組んでいなかった」などの単に現状の問題点だけを指摘したものがかなり見られました。問題の記述内容を利用することは，解答を作成していく上で必要なことですが，設問で問われていることを考慮し，柔軟に考える姿勢を身に付けてほしいと思います。

また，設問 3 (1)では，問題文に「ファイルにパスワード付与や暗号化を行うことができる文書ソフトを使用しているが，格納してあるファイルにはそのようなセキュリティ対策が行われていなかった」という記述があります。しかし，文書ソフトを使ってパスワード付与（あるいは暗号化）する旨を，指摘した解答は少数にとどまっていました。本番の試験では，問題の条件を考慮した上で解答を作成していくようにしましょう。

＜午後Ⅱ＞

問1 データベース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 3 点。

(2) b は，解答例どおりのみ 3 点。

［設問2］
（1）d，e 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。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 8 点。その他は，基本的に 0 点。
（2）アは，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。
［設問4］
(1) 変更禁止期間を 12 日変更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）f は，解答例と同様の用語に対してのみ 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。
（4）工数が削減でき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5］
（1）g，h 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。
（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。

【講評】
記述式の問題が多く，適切に解答を作成できていなかったことなどから，全体的に正答率が低くなったと思います。午後Ⅱ試験では，合格基準点をクリアするには，記述式の問題にうまく対応していくことが必要です。
設問 1 の空欄 c に入れる字句の正答率が低かったことが気になります。この問題は，SQL インジェクション攻撃に対する基本的な知識の一つです。基本的な問題が正解できないのは，準備不足と考えられますので，本番の試験に向け大いにレベルアップが必要だと考えます。
設問 3 では，(1)の正答率が高かった半面，(2)の正答率がかなり落ちています。(1)が正解できれば，(2)も正解できるものですから，本番の試験では，問題の記述内容を考慮しながら冷静に対応していきましょう。
設問 4 では，アクセス権限は，それぞれのロールに与えます。どのロールから権限を削除し，どのロールに与えれば，最小権限を実現できるかなどといった観点から解答を作成するようにしましょう。

問2 ネットワークのセキュリティ
【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）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2］
（1）f ～ i 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 6 点。その他は，基本的に 0 点。
（3）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各 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）j ～ m 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。

【講評】
高得点者が比較的多く見られましたが，春期の情報セキュリティスペシャリスト試験では，総合的な範囲からの出題になると予想されます。ネットワークセキュリティだけではなく，その他のセキュリティ分野についても知識を修得していくようにしましょう。
また，午後Ⅱ試験では，新しい技術などを出題する場合，問題文で技術的な仕組みを紹介しながら出題することがあります。問題の記述内容などを十分に確認しながら解答を作成していくことが要求されるので，この点にはよく注意しましょう。いずれにしても，記述式の問題に適切に対応していくには，記述内容を十分に把握できるだけの技術知識を身に付けておくことが絶対条件です。技術レベルを十分にアップさせて本番の試験に臨むようにしましょう。

以上