2017 春 情報処理安全確保支援士 全国統一公開模試 講評と採点基準

2017 年 3 月 24 日 (株)アイテック IT 人材教育研究部

■ 全体講評

今回の公開模試における午後Ⅰ，午後Ⅱ試験の平均点は，午後Ⅰが 37.9 点，午後Ⅱが 37.7 点でした。問題別では，午後Ⅰの問 1 が 16.7 点，問 2 が 18.9 点，問 3 が 21.3 点で，問 3 の平均点が，最も高くなりました。午後Ⅱは，問 1 が 36.2 点，問 2 が 38.4 点で，ほとんど差がないといえます。2016 年秋期の公開模試では，午後Ⅰの平均点が 41.9 点，午後Ⅱの平均点が 37.2 点でしたから，平均点で評価すると，午後Ⅰは低下，午後Ⅱはわずかばかり向上しました。採点結果から受けた印象としては，本試験に向けて準備が十分な受験者と，まだまだ準備不足という受験者に別れたように思います。

合格基準点をクリアするには，記述式の問題に対する取組み方が重要になってきます。記述式の問題の多くは，下線に関するものが出題されます。すると，解答を作成する際，どうしても下線部だけに注目しがちです。しかし，下線部だけに注目してしまうと，その前後にある条件などを見落としてしまい，的を射た答案をなかなか作成することができません。今回の模試でも，こうした答案が数多く見られました。設問で問われていることを確認した上で，下線部に関する全体の関係をよく把握し，解答を作成するようにしましょう。なお，記述式の問題においては，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条件が付けられています。このため，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とよいでしょう。

次に，問題ごとの選択状況を紹介しておきます。午後Ⅰ試験は，問 1（暗号アルゴリズム）の選択者が 26.9%，問 2（インシデント対応）が 46.3%，問 3（Web サイトのセキュリティ）が 26.8%でした。問題内容からほとんどの受験者は問 2 を選択したものの，残りは問 1 か問 3 にせざるを得なかったと思われます。本試験の午後Ⅰで出題される問題数も 3 問ですから，各自が得意とする分野の問題をいち早く見つけ出し，それに集中して取り組むことが必要になると考えられます。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 点強を得点するだけで，午後Ⅰ試験はクリアすることができます。しかし，このようなことが可能になるには，問題の記述内容を十分に把握できるだけの知識が，まず必要とされます。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試験は，問 1（Web サイトの脆弱性検査）の選択者が 27.9%，問 2（マルウェア対策）が 72.1%で，多くの受験者は，問 2 を選択していました。午後Ⅱ試験は，様々なセキュリティ分野の知識が問われる総合問題として出題されることが多いので，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とよいでしょう。また，試験センターでは「試験結果に問題の難易差が認められた場合には，基準点の変更を行うことがあります」としています。このため，午後Ⅱ試験においては，問 1 と問 2 の難易差をあまり気にせず，一度選択すると決めた問題を最後までやり遂げることが大切です。問題選択に迷ってしまうと，2 問とも手をつけ，かえって失敗することになってしまいます。

午後Ⅰ，午後Ⅱ試験の記述式問題の多くは，問題文の中に解答を導くためのヒントが記述されています。一定の知識レベルに到達していれば，問題文で記述された内容を基にして正解を導き出すことができます。しかし，受験者によっては問題文の記述内容をそのまま引用して解答を作成している例も多く見られます。単なる引用では正解になることは極めて少ないので，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論理的に考えていくようにしましょう。

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もって，午後Ⅱ試験の最後まで全力を出し切り（あきらめずに）問題に取り組んで，ぜひ合格するようにしましょう。

＜午後Ⅰ＞

問1 暗号アルゴリズム

【採点基準】

［設問1］

（1）解答例どおりに対し 3 点。

（2）a，b は，解答例どおりに対し各 2 点。

（3）c ～ e は，解答例どおりに対し各 2 点。

（4）解答例と同様の趣旨（ハッシュ値が同じになる，異なるサーバ証明書が作成される）が適切に指摘されているものに対し 8 点。単にハッシュ値の衝突を指摘したものは 4 点。その他は 0 点。

（5）f は，解答例どおりに対し 2 点。計算量は，解答例どおりに対し 3 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）解答例と同様の趣旨（平文が同じブロックは，同じ暗号文になること）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。

【講評】

平均点は 16.7 点（平均正答率は 33.4%）であり，午後 I の中では，最も低い点数でした。暗号に関する技術的な知識については，まだまだ理解されていないように見受けられます。

設問 1 は，全体的に想定していたよりも正答率が低かったように思います。設問 1 (2)は，解答群の中に公開鍵と秘密鍵の両方があれば，もっと正答率が上がったと思いますが，秘密鍵が記載されていなかったことから，迷った受験者もいたと考えられます。語句選択の場合には，消去法によって正解を確定することが必要になるケースもありますので，用語の意味は正確に理解しておきましょう。(4)は，サーバ証明書の作成において SHA-1 を利用した場合に発生する問題を問うものです。SHA-1 の脆弱性（ハッシュ値の衝突が起こり得ること）を理解していないような答案がかなり見られました。ハッシュ値の衝突とは何かなどの基本的な知識については，十分に理解しておきましょう。(5)は，暗号アルゴリズムの強度に関するものです。等価安全性とは，暗号アルゴリズムの強度を，共通鍵暗号における鍵の長さ（ビット数）に例えて表すようにしたもので，現在，112 ビットの等価安全性が必要とされています。問題文を読んでいけば，空欄 f に入れる数値は間違いなく記入できると想定していましたが，正答率はそれほど高くなかったようです。

設問 2 は，(4)を除き，全体的に正答率は低かったようです。(1)は，電子署名は公開鍵暗号方式を利用するので，より多くの処理時間が必要になるという点に気付かず，解答がうまく作成できていなかったようです。(2)は，HMAC の強度は何に依存しているかを問うものです。メッセージ認証コードの安全性については，送信者と受信者が共有する認証鍵（共通鍵）が必要であること，その強度は共通鍵の長さに依存していることなどを理解していることが必要です。(3)は，暗号利用モードに ECB モードを利用した場合の問題点を問うものです。この問題のポイントは，平文ブロックと暗号化したブロックが 1 対 1 に対応しているということです。例えば，平文ブロックに対して，全ての鍵（ビットパターン）で暗号化したものを用意し，暗号化したブロックに一致するものを探せば，それが平文に対応するので，その際に利用された鍵も判明するという仕組みです。こうした一つ一つの知識を積み重ねていき，支援士の午後試験で合格基準点をクリアするようにしましょう。

問2 インシデント対応

【採点基準】

[設問1]

(1) 機器名は，解答例どおりに対し 3 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 4 点。その他は，基本的に 0 点。
(2) a，b は，解答例どおりに対し各 3 点。
(3) 解答例どおり（完答）に対し 5 点。

[設問2]

(1) 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 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。単にイベントログの追加設定を行うなどの今一歩の内容は 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 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。その他（ログの分析などの指摘にとどまっているもの）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】

平均点は 18.9 点（平均正答率は 37.9%）で，午後 I の 3 問の中では，中間に位置することになりました。

設問 1 (1)は，想定していたよりも正答率は低かったと思います。誤答の多くは，「PC の Web ブラウザは，プロキシサーバを経由する」という記述だけに着目したものでした。もう少し他の条件も考慮し，解答を作成していくことが必要です。(2)は，専門知識に分類されるような問題ですが，試験では HTTP のメソッドやヘッダの意味については理解していることが求められますので，徐々にレベルアップしていきましょう。

設問 2 (1)は，業務サーバがマルウェアに感染している前提で考察する必要がありましたので，正答率は極めて低かったようです。(2)は，表 3（攻撃ツールの実行の痕跡（抜粋））だけに着目した答案が多く見られましたが，この設問では業務サーバへの影響調査に関するものです。イベントログの追加設定が必要になるのは，どの装置かといった点を明確にするようにしてほしいと思います。

設問 3 は，まずまずの正答率だったと思います。なお，(1)は，問題文を読めば，ログはログ管理サーバで保管されていることが分かります。ログ管理サーバがキーワードになりますので，必要なキーワードを明記し，解答は

丁寧に作成するように心掛けてください。

問3 Web サイトのセキュリティ

【採点基準】

［設問1］

（1）a ～ c は，解答例どおりに対し各 2 点。

（2）d ～ f は，解答例どおりに対し各 3 点。

（3）解答例と同様の趣旨（Referer ヘッダで通知されること）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）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）解答例どおりに対し 7 点。

（2）解答例どおりに対し 4 点。

【講評】

平均点は 21.3 点（平均正答率は 42.6%）であり，午後 I の 3 問の中では，最も高い点数でした。基本的な問題が多かったことから，受験者の中には満点近い点数をあげる人も見られました。

設問 1 (1)，(2)とも，想定していたよりも正答率は低かったようです。(2)の空欄 f に入れる secure 属性の正答率は高かった半面，Set-Cookie と Cookie との関係については，まだ十分に理解されていないようでした。

設問 2 は，(1)の正答率は極めて高く，セッション ID の発行方法については，十分に理解されていました。その半面，(2)，(3)のように少し高度の内容が問われると，正答率が下がってきます。少しずつでも構わないので，色々な知識を吸収するようにしていきましょう。

設問 3 (1)は，SQL の where 句の検索条件を考えないでユーザ ID（USERID）や旧パスワード（PASSWORD）に入力する情報だけを考えて答えたような答案が多かったという印象を受けました。例えば，USERID と PASSWORD は and 条件で結ばれていますが，旧パスワードの最後に「or 'A' = 'A」のように常に真となる条件を or で追加すると，全てのパスワードが更新されてしまいます。表面的に考えるのではなく，考えたパラメータを SQL 文の該当箇所に代入して考えていくようにしましょう。

＜午後Ⅱ＞

問1 Web サイトの脆弱性検査

【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 6 点。その他は，基本的に 0 点。

（2）a，b は，解答例どおりに対し各 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。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）c は，解答例どおりに対し 3 点。

（3）d は，解答例どおりに対し 3 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。指摘内容が今一歩のものは 4 点。その他は 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各 6 点。その他は，基本的に 0 点。

［設問3］

（1）解答例どおりに対し 5 点。

（2）e，f は，解答例どおりに対し各 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）g は，解答例どおりに対し 3 点。

（5）解答例どおりに対し各 3 点。ただし，三つ以上，答えた場合は，一つにつき 3 点減点。

（6）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）h，i は，解答例どおりに対し各 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。

【講評】

問 1 の平均点は 36.2 点で，問 2 の 38.4 点を少し下回りました。問 1 の選択者は，Web システムのセキュリティを得意とする受験者が多かったと考えられますので，点数的にはあまり差がつかなかったのでしょう。

設問 1 (1)の正答率は，想定以上に高かったと思います。(2)の正答率も，まずまずでしたが，(3)の正答率はかなり低かったようです。Web アプリの脆弱性検査を行う際，検査用 PC から検査コードを Web サーバに送信しますが，途中に IPS が存在すると，一般に IPS で検査コードが破棄されますので，Web アプリの検査にはならないことに注意する必要があります。

設問 2 (1)の正答率は，比較的高かったと思います。

しかし，(2)は，期待していた正答率には及ばなかったように思います。プレースホルダは基本的な用語なので，よく覚えておきましょう。(4)，(5)については，問題の記述内容を表面的に捉えるのではなく，問題の流れや条件などを十分に考慮しながら解答を作成することが必要であったと感じられました。

設問 3 (1)～(4)は，まずまずの正答率のようでした。(5)のように，「全て選び，記号で答えよ」という指示がある場合，正解が一つだけの場合もあります。また，必要以上に答えると，減点の対象になることもありますので，できるだけ確実なものに絞って答えるようにしましょう。(6)は，専門知識が必要ですから，一部の受験者を除き，低い正答率にとどまったようです。

設問 4 (1)，(2)とも，少し専門知識が必要ですから，正答率は比較的低いものとなりました。(2)については，インターネット内において IP パケットを中継する際には，宛先 IP アドレスだけを参照し，送信元 IP アドレスを参照することはありません。このため，送信元 IP アドレスにプライベート IP アドレスが使用されていても受信側のファイアウォール(FW)まで到達しますから，FW で送信元がプライベート IP アドレスになっているパケットをフィルタリングする必要があります。

問2 マルウェア対策

【採点基準】

[設問1]

(1) 解答例どおりに対し 4 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) a，b は，解答例どおりに対し各 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各 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) 解答例どおりに対し各 3 点。ただし，三つ以上，答えた場合は，一つにつき 3 点減点。

(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5]

(1) c は，解答例どおりに対し 4 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。指摘内容が今一歩のものは 4 点。その他は 0 点。

(3) d ～ f は，解答例どおりに対し各 4 点。

[設問6]

(1) 解答例どおり（完答）に対し 6 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】

問 2 の平均点は 38.4 点であり，問 1 より 2.2 点も高くなりました。この平均点の示すように，マルウェアに対するセキュリティ対策の理解は，かなり進んでいると感じられました。また，選択者の比率も問 1 の約 2.5 倍という結果でした。

設問 1 (1)の正答率は低かった半面，(2)，(3)の正答率は，まずまずだったと思います。全体的に問題の条件をうまく反映した答案が作成されていたようです。

設問 2 は，標的型メールの特徴などを的確に答える必要がありましたので，正答率は少し低かったようです。

設問 3 は，(3)を除き，正答率は低かったと思います。特に(2)については，問題の背景を十分に考慮しないまま解答が作成されていたように感じられました。

設問 4 (1)は，解答群の中から三つ答えた答案が多く，減点対象になっていました。必要以上に答えると，減点の対象になることもありますので，できるだけ確実なものに絞って答えるようにしましょう。(2)については，マルウェアに感染するケースは，ソフトウェアの脆弱性を突かれる場合がほとんどです。セキュリティパッチを適用すれば，基本的にマルウェアに感染することはありません。こうした基本的な事項は，十分に押さえておきましょう。

設問 5 (1)は，バイトとビットの換算を忘れたような答案が散見されました。(3)は，正答率が高く，手順については，よく理解されていたようです。

設問 6 (2)では，多層防御という考え方を理解しておくとよいでしょう。

なお，本番の午後試験において合格基準点をクリアするには，問題の記述内容をベースにしながら，しっかり考え，正解を導いていくことが大切です。技術知識に加え，問題の読解力，全体の関係を相互に整理しながら考える洞察力などを，本番の試験に向けて，さらに磨いていくようにしてください。

以上