2017 秋 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 9 月 21 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 40.3 点，午後Ⅱが 42.4 点でした。問題別では，午後Ⅰの問 1 が 21.8 点，問 2 が 18.0 点，問 3 が 21.7 点で，問 1 の平均点が，最も高くなりました。午後Ⅱは，問 1 が 38.9 点，問 2 が 47.1 点で，問 2 の方が高い点数でした。2017 年春期の公開模試では，午後Ⅰの平均点が 37.9 点，午後Ⅱの平均点が 37.7 点でしたから，平均点で評価すると，午後Ⅰは少し向上，午後Ⅱはかなり向上したといえます。また，採点結果から判断すると，本試験に向けて着実に準備が進められている受験者の方が，これまでの模試の受験者に比べると，比較的多く見られたように感じられました。

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（標的型攻撃への対策）の選択者が 45.1%，問 2（マルウェア感染の調査と対応）が 42.1%，問 3（Web サイトのセキュリティ）が 12.8%でした。このため，多くの受験者が，問 1 と問 2 を選択していたことになります。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，まず必要になります。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とよいでしょう。

午後Ⅱ試験は，問 1（学習支援事業のセキュリティ）の選択者が 57.2%，問 2（モバイル環境におけるセキュリティ対策）が 42.8%で，問 1 の選択者が問 2 の選択者を上回る結果となりました。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 標的型攻撃への対策

【採点基準】

[設問1]

（1）a，b は，解答例どおりに対し各 2 点。

（2）解答例と同様の趣旨（添付ファイルが自動的に実行される旨の記述が必要）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 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 4 点。その他は，基本的に 0 点。

（3）c，d は，解答例どおりに対し各 2 点。

（4）e，f は，解答例どおりに対し各 2 点。

（5）解答例どおり（完答）に対し 6 点。

(6) 解答例と同様の趣旨（ARP ポイズニング，又はネットワークモニタなどの攻撃手法を述べているもの）が適切に指摘されているものに対し 6 点。単に認証情報の盗聴など，今一歩の指摘内容は 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 6 点。その他は，基本的に 0 点。

【講評】

平均点は 21.8 点（平均正答率は 43.5%）で，午後 I の中では，最も高い点数でした。標的型攻撃に関する基本的な知識については，よく理解されているように見受けられました。

設問 1 は，全体的にまずまずの正答率だったと思います。マルウェアに感染する可能性が考えられる事象としては，「ソフトウェアに脆弱性がある場合」と，「不正なコードを実行する場合」の二つがあります。添付ファイルを開くということは，添付ファイルを開くためにコードを実行することになりますが，そのコードの中に，不正なコードが埋め込まれていると，マルウェアに感染するなどといった被害に遭ってしまいます。こうした基本的な事項についてはよく整理しておきましょう。

設問 2 は，(5)，(6)を除き，正答率は高かったようです。(5)の VLAN のグループ分けは，問題の条件が十分に考慮されていないように見受けられました。例えば，サーバの中で同じ機能をもつものを同一 VLAN グループにするなどの誤答が目立ちました。VLAN に分けた場合，異なる VLAN に所属するサーバ同士は，お互いに通信ができなくなります。こうしたことを念頭におき，FW のルールを考慮してグループ分けを考えることが必要です。特に，支援士の午後試験では，問題の条件を十分に整理しながら考察していくことが大切です。このため，本試験では，問題文を丁寧に読んで解答を作成するように心掛けてください。

問2 マルウェア感染の調査と対応

【採点基準】

［設問1］

(1) 下線①，下線②とも，解答例どおりに対し各 4 点。

(2) 解答例どおりに対し 6 点。

［設問2］

(1) a は，解答例どおりに対し 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。

［設問3］

(1) b，c 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 4 点。その他は，基本的に 0 点。

(3) 解答例と同様の趣旨（S 社又は T 社の Web サーバのどちらか一方でよい）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 18.0 点（平均正答率は 35.9%）でした。平均点では，午後 I の 3 問の中で，最も低い点数にとどまりました。その要因としては，設問 1 の正答率が低かったことが挙げられます。

設問 1 (1)，(2)とも，問題の条件が十分に考慮されていなかったように感じられました。組織内の PC からプロキシサーバを経由してインターネットにアクセスする際には，接続したい Web サーバの名前解決はプロキシサーバが行うこと，図 1 ではプロキシサーバと外部 DNS サーバは DMZ に配置されているので，両者の通信は FW を経由しない（表 2 の FW のルールにも記載されていない）ことなどが考慮されていなかったようです。特に，(2)は，表 1 を確認すれば，FW はステートフルパケットフィルタリングを行っていることが分かりますが，この条件を見落とした答案が少し見られました。パケットの流れは，十分に理解されていましたから，極めてもったいない解答だったと思います。

設問 2 (1)，(2)の正答率は，まずまずでした。(3)では，「業務サーバ内の業務情報が盗まれる」などの答案が見られましたが，図 2 に記載されているマルウェア U の特徴には，侵入した PC やサーバがもつ情報を盗み取るという内容はありません。あくまでも，「ネットワークスニファ機能を実行し，窃取した情報を外部に送信する」という特徴に着目し，解答を導いてほしかったと思います。また，(4)は，図 2 を参照し「ログイン記録が書き換えられている」と答えた答案が大半を占めていました。ログ情報については，問題文に全てログ管理サーバに転送され，ログ管理サーバのログは改ざんされていないと判断される旨の記述があります。このため，「コマンドが書き換えられている」ことに着目してほしかったと思います。思い込みだけで該当する記述を述べるのではなく，問題の記述内容を総合的に判断し，適切な解答を導いていくようにすれば，点数はもっとアップするでしょう。

設問 3 (1)は，LAN スイッチのポートや NIC の動作に関する専門知識が必要ですから，正答率はそれほど高く

はありませんでした。(2)，(3)も，想定よりも低い正答率だったと思われますが，これらの設問も問題文をよく読んで，論理的に考えて解答を導いていくことが必要だと考えられます。

問3 Web サイトのセキュリティ

【採点基準】

［設問1］

（1）a は，解答例どおりに対し 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。

（3）b ～ e は，解答例どおりに対し各 2 点。

［設問2］

（1）f は，解答例どおりに対し 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）Expires 属性，Domain 属性とも，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。

（4）解答例どおりに対し 4 点。

［設問3］

（1）g，h は，解答例どおりに対し各 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。

【講評】

平均点は 21.7 点（平均正答率は 43.3%）で，問 1 とほぼ同程度の点数でした。しかし，選択者数は 12.8%に過ぎず，Web サイトのセキュリティに関する知識を有している受験者に限られたものと思われます。

設問 1 (1)，(2)とも，正答率は低かったようです。特に，(1)については，ドット（.）を URL エンコードした答案が多く見られました。URL エンコードとは，URL に使用することができない文字を使用する場合は，URL エンコードした文字に置き換えることです。URL に使用できない文字が不明の場合には，空欄 a の前にある URL エンコード済みの URL に記載されている形式に着目すればよいのです。それを見れば，%3a（:），%2f（/）はエンコードされていますが，ドットはエンコードされていないことが分かります。そうすれば，誤りなく解答を作成できたと思います。

設問 2 の(1)，(3)は，クッキー（Cookie）に関する問題です。(1)の 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。また，(3)の Expires 属性の正答率はまずまずでしたが，Domain 属性の正答率は少し低かったようです。クッキーについては，本試験でもよく出題されますので，十分に理解を深めていくようにしましょう。(4)は，正答率が低かったです。Secure 属性が指定されている場合には，http 又は https から，https へ遷移する画面でクッキーが送信されるという基本をしっかりと押さえた上で，該当する遷移を全て選ぶようにするとよいでしょう。

設問 3 (1)の g は，よく理解されていましたが，h の正答率は低かったようです。(2)は，Web-AF を利用した Web サイトは，URL に特有の文字列が含まれるという特徴から，標的とする Web サイトを特定しやすいことに気が付いてほしかったと思います。

＜午後Ⅱ＞

問1 学習支援事業のセキュリティ

【採点基準】

［設問1］

（1）a ～ d は，解答例どおりに対し各 2 点。

（2）e ～ g は，解答例どおりに対し各 2 点。

（3）h ～ k は，解答例どおりに対し各 2 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2］

（1）解答例と同様の趣旨（正規の DNS サーバと同じディジタル署名を作成できない，又は同じ秘密鍵を有していない）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）サービスは，解答例どおりに対し 2 点。手続は，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。IP53B の対象外にする固定 IP アドレスを申請するなど，具体性が欠けるものは 3 点。その他は 0 点。

（3）解答例どおりに対し 4 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）l ～ n は，解答例どおりに対し各 2 点。

［設問4］

（1）o ～ q は，解答例どおりに対し各 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。

（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】

問 1 の平均点は 38.9 点で，問 2 の 47.1 点を下回る結果でしたが，平均点で評価すると，これまでの模試に比較して，着実に知識が身に付いていると感じられる答案内容でした。なお，問 1 の選択者は，57.2%と，問 2 の選択者数を上回る結果でした。

設問 1 の正答率は，全体的にまずまずでした。しかし，(2)の g の正答率は低かったと思います。これは，図 1 の注記 2 のアドレス変換の状況が考慮されていなかったことに起因しています。また，(3)は，パケットを送信する際の宛先 IP アドレスと送信元ポート番号の関係が十分に把握されていないように見受けられました。

設問 2 (1)の DNSSEC の仕組みについては，解説などをよく読んで，十分に理解してほしいと思います。また，一部の受験者は，署名と証明書の区別が十分になされていないと感じられました。こうした基本的な事項については，必ず把握するようにしましょう。(2)，(3)は，まずまずの正答率だったと思われます。

設問 3 (1)は，問題文の流れを整理していくと，“隔離”を採用することの理由は，大量のスパムメールを受信者に転送しないということが導けると思います。本試験においても，全体的な位置付けにおいて，何が課題になっているかを見極めた上で解答を作成してください。(2)の正答率は，低かったように思います。

設問 4 (2)の正答率は，想定よりもかなり低かったと思いますが，(5)の WAF では暗号化された HTTP メッセージを検査できないことについては，よく理解されていると思われます。

問2 モバイル環境におけるセキュリティ対策

【採点基準】

［設問1］

(1) a は，解答例どおりに対し 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) 解答例どおりに対し 4 点。

［設問2］

(1) b，c は，解答例どおりに対し各 2 点。
(2) d，e は，解答例どおりに対し各 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 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) f，g，i は，解答例どおりに対し各 2 点。
(2) h は，解答例どおりに対し 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。その他は，基本的に 0 点。
(4) 解答例どおりに対し 4 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。
(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。
(7) 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。単に，内部サーバセグメントへアクセスができないなど，具体性に欠けるものは 4 点。その他は 0 点。
(3) 解答例どおりに対し各 3 点。

【講評】

問 2 の平均点は 47.1 点であり，問 1 より 8.2 点も高くなりました。設問 1，設問 2，設問 4 の正答率が良かったことが，その要因と考えられます。一方，選択者数の比率は，問 1 に比較すると少なく，42.8%でした。これは，問 2 がセキュリティプロトコルに重点が置かれた内容になっていたからでしょう。

設問 1 は，全体的に正答率が高かったです。特に，プロキシサーバで行われる URL フィルタリングの効果については，よく理解されていました。

設問 2 は，(1)～(3)とも正答率が高く，(4)だけが少し低かったようです。基本的な問題については，難なく正解できていると思われます。

設問 3 (1)，(2)の正答率は，まずまずだったと思いますが，(3)～(7)のように，少し技術的な内容を問う設問に対しては，正答率が低くなる傾向が見られます。特に，(3)については，IPsec において同じ鍵を使用した場合の問題点を問いましたが，「鍵が漏えいし，なりすまされる」などの答案が少なからずありました。同じ鍵を使用した場合のリスクは，盗まれることではなく，鍵を解読されてしまうことですから，こうした基本的な事項は必ず押さえておくようにしましょう。また，(4)の IPsec で NAPT を通過することができない理由も，正答率が低かったと思います。

設問 4 (3)は，想定よりも高い正答率だったと思います。問題文をよく読めば，どのようなルールを追加すべきかが分かりますので，本試験でも問題の条件を考慮した上で，解答を作成するように心掛けていただきたいと思います。

以上