2016 秋 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

2016 年 9 月 26 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 41.9 点，午後Ⅱが 37.2 点でした。問題別では，午後Ⅰの問 1 が 15.3 点，問 2 が 20.3 点，問 3 が 25.6 点で，問 3 の平均点が，最も高くなりました。また，午後Ⅱは，問 1 が 29.3 点，問 2 が 39.3 点で，10 点ほどの差が見られました。2016 年春期の公開模試では，午後Ⅰの平均点が 35.7 点，午後Ⅱの平均点が 34.9 点でしたから，平均点で評価すると，午後Ⅰ，午後Ⅱとも高くなりましたが，採点結果から受けた印象としては，知識レベルの極めて高い一部の受験者と，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（公開鍵基盤を利用した認証強化）の選択者が 26.5%，問 2（Web アクセスのセキュリティ）が 35.2%，問 3（マルウェアの不正侵入対策）が 38.3%で，問題間における偏りは，比較的少なかったといえます。なお，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 システムの定期点検）の選択者が 19.6%，問 2（マルウェア対策）が 80.4%で，大半の受験者は，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 公開鍵基盤を利用した認証強化

【採点基準】

[設問1]

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

（3）c，d は，解答例どおりに対し各 4 点。なお，「自営 CA のルート証明書」は「自営 CA の公開鍵」でも正解とします。

（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。指摘内容が今一歩のものは 3 点。その他は 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）e，f 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。

【講評】

平均点は 15.3 点（平均正答率は 30.5%）であり，午後 I の中では，最も低い点数でした。公開鍵証明書の検証方法などの基本的なことが十分に理解されていないように感じられます。

設問 1 (2)，(3)，(4)は，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，多くの受験者が正解できると考えていましたが，誤答が目立ちました。(3)については，インターネットを利用する際には，信頼できる第三者機関のルート証明書が，あらかじめプレインストールされていますので，ほとんど気にかけることはありません。しかし，自営 CA などを使用する際には，自営 CA のルート証明書を，それぞれの装置にインストールすることが必要です。例えば，クライアント (MPC) には，クライアント証明書（クライアントの公開鍵証明書），クライアントの秘密鍵及び自営 CA のルート証明書をインストールしなければなりません。(4)についても，クライアント証明書の検証方法だけが問われていれば，証明書にある署名を CA の公開鍵で検証すると答えることができたはずです。しかし，文章中の関係を踏まえながら解答を求められると，正答率が低くなる傾向があります。基本的な知識については，しっかりと把握しどのような状況でも正解できるようにしましょう。

設問 2 (1)は，属性証明書とは何かがよく理解されていなかったようです。(2)は，暗号化に使用する秘密鍵と，署名に使用する秘密鍵の違いを問うものでしたが，このような知識も十分に整理できていなかったようです。その半面，(3)，(4)は，まずまずの正答率でした。

問2 Web アクセスのセキュリティ

【採点基準】

[設問1]

(1) a は，解答例どおりに対し 3 点。
(2) 解答例どおりに対し各 3 点。
(3) Web サイトは，解答例どおりに対し 2 点。不用意な操作は，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。
(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) b ～ e は，解答例どおりに対し各 3 点。
(2) 解答例と同様の趣旨（ログを分析する旨）が適切に指摘されているものに対し 5 点。その他（ログを取得する旨など）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 5 点。その他は，基本的に 0 点。

【講評】

平均点は 20.3 点（平均正答率は 40.6%）で，午後 I の 3 問の中では，平均点でも選択者数でも，中間に位置することになりました。

設問 1 (1)，(2)は，単に知識を問うものでしたから，正答率は低かったように思います。(3)の正答率は，高かった半面，(4)は専門的な知識が必要でしたから，正答率は低いものにとどまりました。いずれにしても，Web システムに関するセキュリティについては，試験では最頻出テーマの一つになっています。IPA が公開している Web に関連するセキュリティの資料については，十分に学習しておくことが必要です。

設問 2 (1)は，e を除き，想定より正答率は低かったように思います。例えば，b に入れる字句は，マルウェアによる標的型攻撃などに関しては，従来の入口対策だけではなく，内部拡大対策，出口対策といった多層防御が必要であることから，簡単に正解できると思っていましたが，結果はそうではありませんでした。(2)も，「ログ監視の観点から」という条件を付けていましたので，「ログを分析する」というキーワードを答えられると考えていましたが，「ログを取得する」旨の答案が多く見られました。ログを取得しても，ログの分析をしない限り不正な兆候を発見することはできませんので，解答はできるだけ丁寧に作成していくようにしましょう。

問3 マルウェアの不正侵入対策

【採点基準】

[設問1]

(1) a ～ c 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 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。

[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各 4 点。その他は，基本的に 0 点。
(2) 解答例と同様の趣旨（アイコンの偽装，拡張子の偽装の 2 点）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。なお，二重拡張子による偽装と，RLO による偽装などの指摘は，同じ拡張子の偽装に当たるので，両方を指摘しても 4 点にしています。

［設問3］
（1）d ～ f は，解答例どおりに対し各 3 点。
（2）変更すべきルールは，解答例どおりに対し 2 点。
登録すべきルールは，解答例どおりに対し 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。

【講評】

平均点は 25.6 点（平均正答率は 51.1%）であり，午後 I の 3 問の中では，最も高い点数でした。

平均点の示すとおり，全体的に正答率は高く，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。

設問 1，設問 2 とも，想定以上によくできていたと思います。

設問 3 (1)の穴埋め問題は，設問 1 や設問 2 に比較すると，正答率は全体的に低めでしたが，e に入れる字句は，想定よりも良かったと思います。(2)の登録すべきルールのプロトコルについては，「80/tcp，443/tcp」と記入した答案がかなり見られました。ファイアウォールのルールについては，表 1 のフィルタリング設定から判断するのではなく，注記にある「プロキシサーバの待受けポートは 80/tcp である」という条件を考慮して作成してほしかったと思います。(3)の正解者も，ほとんど見られないと想定していましたが，想定以上の受験者が正解しており，最近の技術動向をしっかり把握されていると感じられました。

＜午後Ⅱ＞

問1 Web システムの定期点検

【訂正とお詫び】

設問 3 (3)において，「小数第 2 位を四捨五入して小数第 1 位まで求め，答えよ」とすべきところを，誤って「小数第 2 位を四捨五入して整数で答えよ」としてしまいました。受験者の方々に大変な混乱を与えるとともに，ご迷惑をおかけいたしました。改めてお詫び申し上げます。

【採点基準】

［設問1］
a ～ c は，解答例どおりに対し各 3 点。

［設問2］
（1）解答例と同様の趣旨（他の SSLv2 サーバと同じサーバ証明書を使用していること）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。
（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。

［設問3］
（1）d，e は，解答例どおりに対し各 3 点。
（2）f 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。指摘内容が今一歩のもの（件名に kensa が表示される旨）は 4 点。その他は 0 点。
（3）g は，「2.7」のほか，「3」，「2.67」は 4 点としました。その他は，式が正しくなく，計算間違いをしていると考えられるため，不正解にしました。

［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 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。
（5）h 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。
（6）解答例と同じ内容のものに対し 4 点。その他は，基本的に 0 点。

［設問5］
（1）i は，解答例どおりに対し 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。送信元 IP アドレスの指摘が一つだけの場合は 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各 3 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。指摘内容が今一歩のものは 4 点。その他は 0 点。

【講評】

問 1 の平均点は 29.3 点で，問 2 より 10 点も低い点数にとどまりました。公開模試では問 1 と問 2 に大きな差があったとしても，得点調整を行うことはありません。このため，問 1 を選択した受験者の評価は，問 2 と比較して，かなり厳しくなっていると思われます。問 1 の選択者は，こうした事情を考慮し評価表を見るとよいかもしれません。

設問 1 は，サーバ証明書と，DNS のリソースレコードに関する基本的な用語でしたから，正答率は高くなると考えていましたが，結果は期待していたようにはなりませんでした。

設問 2 は，少し難度の高い問題でしたから，(1)，(2)の正答率は，ともに低かったようです。特に，(2)は，外部から IDC 内の PR サーバに対する SSLv2 と SSLv3

による接続試験という解答を期待していましたが，明確に指摘した答案は，極めて少なかったと思います。

設問 3 (1)の d は，まずまずの正答率でしたが，e は，低い正答率にとどまったようです。(2)は，技術絡みの問題でしたから，全体的に正答率は低かったようです。(3)は，計算問題ですが，計算式を正しく組み立てられていなかったり，バイトからビットへの換算忘れなどをしたりして，高い正答率にはならなかったようです。本番の試験では，ケアレスミスは致命傷になることもありますので，計算問題が出題された際には，必ず正解できるようにしましょう。

設問 4 は，(1)と(5)を除き，正答率は比較的良かったように思います。(1)は，署名は署名者の秘密鍵を用いてメッセージダイジェスト（ハッシュ値）を暗号化するため，秘密鍵がなければ署名を作成することはできません。しかし，SHA-1 の脆弱性をついて，ハッシュ値が同じようになる，異なる証明書を作成できたら，秘密鍵がなくても署名を付与できるというものです。どうすれば署名を付与できるか，もう一度，考えてみましょう。(5)の h に入れる字句は，対比させるブラックリスト方式の内容を見間違えたような答案が散見されました。

設問 4 は，(2)を除き，まずまずの正答率だったようです。

問2 マルウェア対策

【採点基準】

［設問1］

（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（業務サーバの共有フォルダというキーワードが必要）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）不適切な点，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 8 点。指摘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 6 点。その他は，基本的に 0 点。

（4）解答例と同様の趣旨（ネットワークに接続されていない外部記憶媒体がキーワード）が適切に指摘されているものに対し 6 点。指摘内容が今一歩のものは 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 8 点。「IPS などによるウイルスチェックを回避する」などは，下線⑥の前に記述された条件に合わないので，基本的に 0 点。

（2）c，d は，解答例どおりに対し各 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。「送信元を偽装したメール」，「送信元アドレスを詐称したメール」などは，送信元の何が偽装されているかが不明のため，基本的に 0 点。

［設問4］

（1）e は，解答例どおりに対し 4 点。

（2）解答例どおりに対し 8 点（完答）。

（3）f は，解答例どおりに対し 4 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 6 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 6 点。その他は，基本的に 0 点。

【講評】

問 2 の平均点は 39.3 点であり，問 1 より 10 点も高くなりました。このため，問 2 の選択者の評価は，かなり甘く評価されていますので，そのまま鵜呑みにするのではなく，少し厳しめに見るようにしてください。

設問 1，設問 2 は，全体的にまずまずの正答率だったと思います。

設問 3 は，少し技術知識が必要な問題であったことから，全体的に正答率は低かったようです。また，高得点者とそうでない受験者の差がついたところのようです。なお，設問 3 (3)は，採点基準でも述べたように，少し厳しく採点していますが，SPF などの送信ドメイン認証は，本試験でよく出題されますので，正しい知識を身に付けておくとよいでしょう。

設問 4 の(1)～(3)は，正答率は良くなかったようですが，(4)～(6)の正答率は，比較的良かったように思います。特に，(2)の FW のフィルタリングルールは，部門 LAN 及び管理 LAN からインターネットへ直接出ていく通信については，HTTP と HTTPS だけを対象にするのではなく，全てのサービスを対象にしなければ，適切なルールとはなりません。

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必要になります。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，さらに磨いていってほしいと思います。

以上