2015 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

2015 年 9 月 28 日 (株)アイテック IT 教育研究開発部

■ 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 36.7 点，午後Ⅱが 31.9 点でした。問題別では，午後Ⅰの問 1 が 14.5 点，問 2 が 22.2 点，問 3 が 16.0 点で，問 2 の平均点が最も高くなりました。また，午後Ⅱは，問 1 が 28.5 点，問 2 が 40.0 点で，かなりの差が見られました。2015 年春期の公開模試では，午後Ⅰの平均点が 42.0 点，午後Ⅱの平均点が 36.5 点でしたから，平均点で評価すると，午後Ⅰ，午後Ⅱともに低下したことになります。

採点結果から受けた印象としては，記述式の設問では，下線部にだけ注目しそれに関することを取り上げて解答を作成していたり，設問で指示されていることにあまり注意せず，各自がも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たりすると思われる答案が多く見られました。合格するためには，問題の記述内容や設問の指示に従って，素直に答案を作成していくことが必要です。こうした事項については，本番の試験に向けて必ず改善していってほしいと思います。また，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ようにしましょう。なお，問題によっては，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，例えば，「必要最小限の範囲に対してだけ権限を与える」などと解答しても，それでは具体的と見なされません。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（リモート接続システム）の選択者が 42.1%，問 2（スマートフォンアプリケーションの開発）が 47.9%，問 3（セキュアプログラミング）が 10.0%で多くの受験者が問 1 と問 2 を選択していたことになります。なお，午後Ⅰ試験で出題される問題数は 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思われます。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 サービスのセキュリティ対策）の選択者が 69.9%，問 2（無線 LAN のセキュリティ対策）が 30.1%で，約 7 対 3 という比率で問 1 の選択者が多くなりました。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達していれば，問題文で記述された内容を基にして考察していけば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）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 リモート接続システム

【採点基準】

［設問1］

（1）解答例どおりに対し各 3 点。その他は 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。

（3）解答例と同様の趣旨（A 社が許可していない MD 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 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 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 5 点。その他は 0 点。

(3) 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 5 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 6 点。その他は，基本的に 0 点。

【講評】

平均点は 14.5 点（平均正答率は 29.0%）でした。午後 I の 3 問の中では，選択者数は問 2 についで多かった半面，平均点では最も低くなりました。

設問 1 (1)の正答率はかなり低く，三つとも正解した答案は，極めて少なかったようです。この設問では TLS のクライアント認証及びサーバ認証を行うために，MD にインストールする必要がある情報が問われています。また，クライアントは MD，サーバは GW サーバが該当します。TLS の通信シーケンスでは，まず，GW サーバからサーバ証明書が送られてくるので，MD はそのサーバ証明書を検証する必要があります。その際，GW サーバのサーバ証明書が正しいかどうかは，ルート証明書にある公開鍵を用いて検証します。このため，MD にはあらかじめ CA のルート証明書をインストールする必要があります（インターネット上にある Web サーバにアクセスする際にもサーバ証明書の検証を行いますが，CA のルート証明書は，多くの場合，ブラウザにプレインストールされていますので，改めてルート証明書をインストールする必要はありません）。次に，GW サーバが MD を認証するには，MD が作成したディジタル署名を，GW サーバが検証することになります。MD がディジタル署名を作成するには，自身の秘密鍵が必要ですし，TLS の通信シーケンスでは，MD のクライアント証明書を GW サーバに送る必要があります。このため，MD の秘密鍵，クライアント証明書をインストールする必要があります。こうした基本的な事項は，十分に把握しておくことが必要です。(2)は，基本的なものでしたが，アカウントをロックすることに気付けなかった答案も見られました。その半面，(3)の正答率は，比較的高かったようです。

設問 2 では，(1)，(2)，(4)は，まずまずの正答率でしたが，(3)，(5)は低かったと思います。少し技術的な内容になると，正答率が低くなる傾向が見られますので，専門用語の意味などは，よく理解しておきましょう。

問2 スマートフォンアプリケーションの開発

【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各 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 4 点。その他は 0 点。

[設問2]

(1) 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 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 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) 下線④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。アクセス権が読取り権限に限定されていないものは 3 点。その他は 0 点。下線⑤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各 6 点。その他は，基本的に 0 点。

【講評】

平均点は 22.2 点（平均正答率は 44.5%）で，午後 I の 3 問の中では最も高くなりました。また，この問題の選択者は 47.9%でしたから，ほぼ全ての受験者が選択していたことになります。

設問 1 の正答率は，全体的に高かったようですが，(1)の図 2（前回パスワードを保存するモードの画面）の見直し案については，強引な答案も見られました。例えば，パスワードを非表示にするチェックボックスを削除する，非表示のチェックボックスを外してもパスワードを表示しないなどの答案です。もう少し問題の記述内容並びに図 2 の画面遷移から，表示モードを変更した場合には，どのように仕様変更すべきかを，素直に指摘してほしかったと思います。

設問 2 (1)の正答率は，低かったようです。問 1 の空欄 a と同様，専門用語を答える問題は，正答率が下がる傾向にあります。用語の意味は，正しく理解しておくとよいでしょう。(2)は，問題の条件が加味されていない答案が多く見られ，正答率はそれほど高くなかったと思います。(3)の下線③に関する設問も，下線③の前に記述されている「スマホアプリのアプリ権限を不正アプリに悪用」という表現をそのまま引用したものが見られましたが，多くの場合，問題の表現をそのまま引用しても正解にならないケースが多いので，問題の流れから何が問われているかをしっかり見極めるようにしましょう。

設問 3 は，正答率が高かったと思います。なお，(2)の下線④の答案については，アクセス権が読取り権限に限定されていないものが散見されました。

問3 セキュアプログラミング

【採点基準】

［設問1］
（1）a ～ g は，解答例どおりに対し各 2 点。
（2）解答例どおりに対し 6 点。その他は 0 点。
（3）解答例どおり，又は「"%s¥n", buffer」に対し 6 点。その他は 0 点。
（4）機能名は，解答例どおりに対し 2 点。その他は 0 点。動作は，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 4 点。その他は，基本的に 0 点。
［設問2］
（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各 4 点。その他は，基本的に 0 点。
（3）解答例どおりに対し 6 点。その他は 0 点。

【講評】
平均点は 16.0 点（平均正答率は 32.0%）でした。問題の選択上，問 2 を選択せざるを得ない受験者もいたと感じられましたが，平均点では問 1 よりも 1.5 点高い点数となりました。

設問 1 (1)の穴埋め問題の a，c，d，e は，まずまずの正答率でしたが，b の正解者は，ほとんど見られませんでした。スタック領域に格納されている変数と buffer に入力される文字数の関係を基に図を描きながら考えてほしかったと思います。(2)，(3)の正答率は低かったものの，(4)の正答率は高いものとなりました。

設問 2 は，全体的に正答率が低かったように思いますが，(3)の正答率は，想定以上に良かったと思います。

午後 I 試験の出題数は 3 問ですから，本番の試験でもセキュアプログラミングが含まれる問題を選択せざるを得ないケースが考えられます。その際の準備としては，IPA が公開している「セキュア・プログラミング講座」，「安全なウェブサイトの作り方」，「安全な SQL の呼び出し方」，「セキュアな Web サーバの構築と運用」などの資料を事前に学習しておくことが必要です。しかし，これらの資料を短期間でマスターすることは大変ですから，長期的に取り組んでいく方がよいでしょう。また，プログラミング言語についても，コードで記述された内容を理解できるようにしておくことも必要です。

＜午後Ⅱ＞
問1 Web サービ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 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2］
（1）解答例どおりに対し 4 点。
（2）想定される問題，事後的な対策とも，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。
（3）解答例どおりに対し 8 点。その他は 0 点。
［設問3］
（1）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 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。
［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各 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。

【講評】
問 1 の平均点は 28.5 点で，問 2 よりも 11.5 点低い結果でした。このため，問 1 を選択した受験者の評価は，かなり厳しいものとなっていますので，たとえ評価が低くても，あまり気にしないようにしましょう。

設問 1 は，全体的に正答率が低かったようです。例えば，(1)の穴埋め問題は，空欄 a ～ c の 3 問とも正解できた受験者は，極めて少数でした。午後 I 問 1，問 2 でも講評したように，用語の意味が正しく把握されていないように感じられました。(2)は，表 2 の内容からサーバ証明書の更新については，いつまでに，何を変更するのかをもっと具体的に指摘してほしかったと思います。(3)については，顧客のブラウザにプライベート認証局のルート証明書を手動でインストールするという状況を念頭に置きながら，認証局の秘密鍵が危殆化した際の対応を問いましたが，多くの答案は「新しいルート証明書を再インストールする」というものでした。ここでは，危殆化した秘密鍵の対応を問うていますので，ルート証明書を必ず削除しなければなりません。このほか，顧客側の対応にもかかわらず，CA 側の処理（CRL に登録する）を答えたものも見られました。(4)についても，CSR という行為が正しく理解されていないように見受けら

れ，CSR の情報が漏えいするなどの答案もありました。CSR の意味を理解していれば，あたりまえのことを答えるものでしたから，素直に答案を作成することを心掛けるようにしましょう。

設問 2 の正答率は，全体的に低かったようです。特に，(1)のリスクベース認証の正答率が低かったと思います。(2)の想定される問題は，「利便性が低下する」旨の答案は比較的よく見られましたが，事後的な対策の「アラートメールを顧客に通知する」ことを指摘した答案は，ほとんど見られませんでした。

設問 3 の正答率は，まずまずでした。DNS の仕組みについては，十分に理解されていると思われますが，(3)では，上位 DNS サーバに不正なサーバが登録されていないかを確認するなどの答案も散見されました。A 社として何を確認すべきかを，もっと的確に解答するようにしてほしかったと思います。

設問 4 の正答率は，全体的にまずまずでしたが，(1)では問題文を単に引用した答案も見られ，WAF を導入する対策がどのような場合に有効かという問いに的確に答えられていないようでした。(3)，(4)は，比較的正答率は良かったと思います。

問2 無線 LAN のセキュリティ対策

【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) 解答例どおりに対し 3 点。
(3) 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) 空欄 c に入れる字句，認証とも，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。
(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。指摘内容が今一歩のものは 4 点。その他は 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) 解答例どおりに対し 3 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。

［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 8 点。その他は，基本的に 0 点

［設問4］

(1) 項番は，解答例どおりに対し 2 点。内容は，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 6 点。その他は，基本的に 0 点。
(4) 解答例どおりに対し 3 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。

【講評】

問 2 の平均点は 40.0 点で，問 1 よりも 11.5 点高くなりました。無線 LAN のセキュリティに関する関心は高く，理解もかなり進んでいるように思われます。

設問 1 は，まずまずの正答率でしたが，(2)，(3)の用語問題は，比較的正答率が低かったと思います。

設問 2 は，(3)，(5)を除き，まずまずの正答率だったと思います。なお，(3)のパスフレーズの解析方法については，ハッシュ関数を用いた場合，ハッシュ値から元のパスフレーズを求めることはできません。そこで，パスフレーズの候補一つ一つに対して，他のパラメタを加え合わせたものにハッシュ値を適用したリストを作成し，収集したデータと合致するものを見つけ出し，パスフレーズを推測するという手法が採られます。このような手法についてはこれまで出題対象になっていますので，よく理解し応用が利くようにしておくとよいでしょう。

設問 3 は，全体的に正答率が高かったようですが，(2)では SSID の意味が理解されていないような答案が散見されました。

設問 4 (1)及び(3)の正答率は高かったようですが，(2)はプロキシサーバを経由しないのでセキュリティチェックができない旨が的確に指摘されていませんでした。(4)は技術用語を答えるものでしたから，想定よりも低い正答率になりました。(5)は技術問題でしたから，低い正答率にとどまりました。

なお，問 1，問 2 に共通する事項ですが，問題文を表面的にしか読み取っていない，問題の条件設定がどのようになっているかなどの把握が十分になされていない，自身の知識だけから安易に解答を作成しようとする傾向が強いなどといったことが感じられました。本番の試験では，問題文をよく読んで設問で問われていることに対し素直に答えていくようにしましょう。

以上