2018 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

2018 年 9 月 25 日 (株)アイテック IT 人材教育研究部

【訂正とお詫び】

午後Ⅱ問題 問 2 設問 4 (2) において,「なお, コード署名証明書は, ダウンロードするソフトウェアに含まれており, 認証局の秘密鍵で署名されているものとする」と表記すべきところを,「認証局の秘密鍵」ではなく, 誤って「Web サーバの公開鍵」としてしまい, 受験者の方々には大変なご迷惑をおかけいたしました。改めて深くお詫び申し上げます。

■ 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 42.4 点, 午後Ⅱが 38.9 点でした。問題別では, 午後Ⅰの問 1 が 25.0 点, 問 2 が 23.6 点, 問 3 が 16.4 点で, 問 1 の平均点が, 最も高くなりました。また, 午後Ⅱは, 問 1 が 37.0 点, 問 2 が 39.9 点で, 問 2 の方が少し高くなりました。2018 年春期の公開模試は, 午後Ⅰの平均点が 45.5 点, 午後Ⅱの平均点が 38.2 点でしたから, 平均点で評価すると, 午後Ⅰは若干低下しましたが, 午後Ⅱは, ほとんど差がないといえます。また, 採点結果から判断すると, 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分かれたという印象を受けました。

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, 的を射た解答をなかなか作成することができません。今回の模試でも, こうした解答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 (Web サイトのセキュリティ対策) の選択者が 41.0%, 問 2 (TLS の暗号アルゴリズム) が 17.1%, 問 3 (情報システムのモバイル利用) が 41.9%で, 多くの受験者が問 1 と問 3 を選択していたことになります。なお, 本試験の午後Ⅰ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。本試験実施日までの期間で, 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 サイトのセキュリティ対策) の選択者が 34.8%, 問 2 (マルウェア対策の見直し) が 65.2%でした。以前は, Web 関連のセキュリティ問題については敬遠する傾向が見られましたが, それが徐々に緩和されるようになっています。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 Web サイトのセキュリティ対策

【採点基準】

[設問1]

(1) a は, 解答例どおりに対し 3 点。

(2) b, c 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) 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。
(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) d 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 5 点。その他は，基本的に 0 点。

【講評】

平均点は 25.0 点（平均正答率は 50.0%）であり，午後 I の中では，最も高い点数でした。問題の記述内容や条件などを考慮しながら，解答を作成することができたからではないでしょうか。

設問 1 (1)，(2)は，少し専門知識が要求されることから，正答率はそれほど高くなかったようです。これに対し，(3)～(6)は，想定していたよりも正答率は高かったと思います。なお，(3)，(4)については，下線の意味や設問の問われていることを十分に考慮せず，事象の説明にとどまっている解答が散見されました。例えば，(3)はセキュリティの監視において 400 番台のログを定期的に確認する理由が問われています。このため，セキュリティ上の観点に基づいて，解答することが必要ですが，単に HTTP のステータスコードを説明した答案が見受けられました。本試験では，設問で問われていることを確認し，下線部だけに着目して解答を作成するのではなく，問題文の前後に記述されている内容を考慮しながら，解答を作成するようにしましょう。

設問 2 (1)，(3)の正答率は，高かったと思います。しかし，(2)は，問題文に記述されている「プラグインの開発コミュニティは，現在，活動を停止している団体も多い」をそのまま引用した答案が散見されました。活動を停止すると，セキュリティ上，どのような問題が発生するかという観点から，一歩踏み込んで，その理由を具体的に答えるなどの工夫をしていくことが必要です。

問2 TLS の暗号アルゴリズム

【採点基準】

［設問1］

a，b は，解答例どおりに対し各 2 点。

［設問2］

(1) c ～ f は，解答例どおりに対し各 2 点。
(2) 解答例どおりに対し 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。
(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) 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 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) 解答例どおりに対し 6 点。

【講評】

平均点は 23.6 点（平均正答率は 47.2%）で，午後 I の 3 問の中では，問 1 とともに高い点数でした。問 2 の選択者数の比率（17.1%）が示すように，暗号技術の知識を有している受験者が，主にこの問題を選択した結果と考えられます。

設問 1 は，字句の記号選択の問題でしたから，正答率はまずまずだったと思います。

設問 2 (1)は，基本的な字句を答える問題でしたから，全体的に正答率は高くなりました。ただし，空欄 e の楕円曲線上の離散対数問題に DH を適用した用語を答える問題の正答率は低かったようです。(2)のクライアント側で生成する共通鍵の基となるデータの名称を答える問題の正答率は低かったと思います。TLS に限らず，暗号プロトコルで使用される鍵交換方式は，重要な位置付けとなる技術ですから，その仕組みを十分に理解しておくとよいでしょう。(3)，(4)の正答率は，低かったようです。特に(3)については，PFS の意味は比較的重要ですから，その意味をよく理解しておくとよいでしょう。

設問 3 (1)は，空欄 g の正答率は高かった半面，空欄 h の正答率は低かったと思います。専門知識については，一つ一つの積み重ねが必要となります。日ごろから学習する姿勢を貫いていくようにしましょう。(2)，(3)は，想定よりも正答率が高く，基本的な暗号技術の知識についてはかなり身についていることが伺えました。(4)は，もう少し正答率が低くなると考えていましたが，問題の記述内容や条件をうまく反映しながら，答案を作成されたと感じられました。

問3 情報システムのモバイル利用

【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 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) 解答例と同様の趣旨（IdP で利用者認証が一元的行われる旨が必要）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。
(4) c は，解答例どおりに対し 4 点。
(5) d 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。

【講評】

平均点は 16.4 点（平均正答率は 32.8%）でした。午後 I の 3 問の中では，全体的に正答率が低く，最も低い点数になりました。

設問 1 (1)の正答率は，あまり高くありませんでした。攻撃の意味する内容などについては，それぞれの用語を正しく理解するようにしましょう。(2)は，パスワード認証と OTP 認証を組み合わせた問題は何かという観点に基づいた答案が散見され，A 社が許可する NPC に限定するという観点の答案は少なかったようです。問題全体の記述内容を考慮した上で，何が問題になるかをしっかりと見極めるようにしましょう。(3)は，接続元 IP アドレスが普段と異なる状況に着目した答案が散見され，Tor の匿名性については，あまり指摘されていませんでした。(4)は，(2)，(3)と比較すると，正答率は良かったと思いますが，これも問題文で提起されているセキュリティ上の問題は何かを押さえて答案を作成していくことがポイントになります。

設問 2 は，全体的に正答率が低かったと思います。(1)は，図 2 のシーケンスとその説明を十分に考察した上で解答が導かれていないと感じられました。(2)は，クッキーの仕組みに関する問題です。クッキーに関する問題は，出題頻度が比較的高いので，属性の種類や意味，属性を指定したときの動作などについてはよく理解しておくとよいでしょう。(3)は，(1)と同様に，図 2 のシーケンスなどが十分に考慮されずに答案が作成されていたように感じられました。(4)は，XML 署名を検証すると記述されています。署名を検証するとあれば，公開鍵が使用されることはほぼ間違いありませんから，誰の公開鍵を使用するかという点に着目し，解答を考えていくとよいでしょう。(5)は，問題の条件整理が複雑だったためか，正答率は低かったようです。

＜午後Ⅱ＞

問1 Web サイトのセキュリティ対策

【採点基準】

［設問1］
(1) a は，解答例どおりに対し 3 点。
(2) b は，解答例どおりに対し 3 点。

［設問2］
(1) c 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。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 8 点。
(2) d，e 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 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。
(2) f，g 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 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) h は，解答例どおりに対し 3 点。
(3) i 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。

［設問6］
(1) j は，解答例どおりに対し 3 点。
(2) k 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。
(3) 解答例どおりに対し 7 点。

【講評】

問 1 の平均点は 37.0 点で，問 2 より 3 点ほど低い点数にとどまりました。

設問 1 (1)の正答率は，やや低めでしたが，(2)は基本的な用語問題ですから，高かったようです。

設問 2 (1)は，英字で答えよという指示されていますので，設問の指示を見落とすことがないようにしましょ

う。(2)は，セッション固定化攻撃に関する対策ですから，正答率は高かったようです。(3)は，CSRF 攻撃に関するものですが，セッション固定化攻撃として解答を作成したものが散見されました。設問に関連する問題文は，注意深く読んでいくようにしましょう。

設問 3 (1)は，メールヘッダとメール本文は 1 行の空白行で区切られることはかなり理解されているようで，正答率は思ったよりは高かったと思います。

設問 4 は，専門知識が要求されることから，全体的に正答率は低かったようです。

設問 5 (1)～(3)，設問 6 (1)は，まずまずの正答率だったと思いますが，設問 6 (2)，(3)は，期待していたような正答率には及びませんでした。例えば，設問 6 (3)は，頭の中だけで考えるのではなく，図を描くなどしてクラウド型 WAF を導入した際の経路がどのように変化しているかなどを整理し，解答を考えるようにしましょう。

問2 マルウェア対策の見直し

【採点基準】

[設問1]

(1) a は，解答例どおりに対し 3 点。

(2) タイミング，特徴とも，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) b 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。

[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) c は，解答例どおりに対し 4 点。

(2) 再起動前に行う作業，再起動後に行う作業とも，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。

[設問4]

(1) d は，解答例どおりに対し 4 点。

(2) コード署名証明書及びコード署名の二つの検証について，適切に指摘されているものに対し 8 点。どちらか一方の指摘にとどまっているものは 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。

[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。

(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) 解答例どおりに対し 6 点。

【講評】

問 2 の平均点は 39.9 点であり，問 1 より約 3 点高くなりました。なお，問 2 の選択者数は，問 1 の約 2 倍弱の選択者数でした。

設問 1 の(1)，(2)の正答率はまずまずでしたが，(3)は想定よりも低い正答率でした。O さんと F 主任の会話の中において，何が検討されているかなどを注意深く考慮しながら，解答を考えていくとよいでしょう。

設問 2 (2)は，セキュリティ対策の機能を回避する手口が問われていますが，マルウェアが攻撃する方法を答えた答案などが散見されました。必ず設問で問われていることを確認するようにしましょう。

設問 3 (1)の計算問題は，バイトからビットへの換算忘れなどの誤答が散見されました。

設問 4 は，全体的に正答率が低かったようです。特に，(2)は，PC で行うコード署名の検証を行う手順を述べるものですが，コード署名の検証を行うためには，コードをダウンロードしたサーバが正当なものであり，コード自体にも改ざんがないことを確認しなければなりません。この署名の検証に当たっては，送信者側の公開鍵を用いて行います。そして，送信者側の公開鍵の真正性については，認証局が署名した利用者の公開鍵証明書を，認証局の公開鍵で検証することが必要です。こうした事項は，十分に理解されていると思いますが，問題の文脈において，解答を求められると，途端に正答率が低くなる傾向が見られます。署名の検証に関しては，どのような背景の下で出題されても，正確に答えられるようにすることが必要です。署名を認証局に問い合わせることなどはありませんので，基本的な知識に基づいて正確な解答を作成するように心掛けてください。

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，本試験に向けて，さらに磨いていくようにしていただきたいと思います。

以上