2020 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

2020 年 9 月 25 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 45.6 点，午後Ⅱが 42.8 点でした。2020 年春期の公開模試は，午後Ⅰの平均点が 38.7 点，午後Ⅱの平均点が 42.4 点でしたから，平均点だけで評価すると，午後Ⅰは約 7 点アップしましたが，午後Ⅱはほぼ同じ点数でした。問題別の平均点は，午後Ⅰの問 1 が 23.7 点，問 2 が 22.6 点，問 3 が 20.0 点でした。午後Ⅱは，問 1 が 39.5 点，問 2 が 45.3 点で，問 2 の方が高いという結果になりました。

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。設問で何が問われているかを十分に確認し，下線部の記述だけではなく，その前後に記述された内容などを含め，よく整理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，3 問のうち 2 問を選択しますから，問 1（LAN におけるセキュリティ対策）と問 2（サーバ証明書の検証）の選択者が 76.1%，問 1 と問 3（Web サイトのセキュリティ）が 14.9%，問 2 と問 3 が 9.0%という状況でした。問ごとでは，問 1 が 45.5%，問 2 が 42.6%，問 3 が 11.9%でした。10 月 18 日に実施予定の本試験において，3 問のうち 2 問を選択する方法としては，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とよいでしょう。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，こうしたことが実行できるためには，問題の記述内容を十分に把握できるだけの知識が必要とされます。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 42.6%，問 2（マルウェア感染と対応）が 57.4%でした。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，午後Ⅰ試験と同様に，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，IPA 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ながら，問題の記述内容と照らし合わせて論理的に考えていくとよいでしょう。

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 LAN におけるセキュリティ対策

【採点基準】

［設問1］

（1）プロトコル名，機器名とも，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）a は，解答例どおりに対し 2 点。

［設問2］

（1）b，c は，解答例どおりに対し各 2 点。

（2）ホスト名は，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。

（3）d，e 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 6 点。「FW の ARP テーブルに V 主任の PC の IP アドレスと U 主任の PC の MAC アドレスを登録する」旨は，ARP テーブルを改ざんするための手口が指摘されていないので 3 点。その他は 0 点。

［設問3］

（1）f，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。
(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 23.7 点（平均正答率は 47.4%）であり，午後 I の 3 問の中では，最も高い点数でした。

設問 1 (1)の正答率は，想定していたよりもかなり低かったと思います。結論を導く条件が簡潔に記されておらず，少し考えにくい設問でしたから，〔サーバ侵入手口の調査〕に「T 君は，CRM サーバに記録されていたログイン失敗のログについて，……，SSH を使ってログイン試行したという結論に至った」と記載してありました。しかし，このことには，気付かなかったのでしょうか。(2)の正答率も低かったと思います。ログを照合する際には，各機器の時刻が合っているかどうかが重要ですから，難易度は低いと考えていましたが，問題の展開上，考える視点が別の方向に向かってしまったようです。(3)は，よく出来ていました。

設問 2 (1)～(3)の正答率は高かったようです。ARP キャッシュポイズニングの仕組みについてよく理解されていると思います。一方，(4)は，GARP を用いて，FW の ARP テーブルを改ざんする手口を具体的に述べるものですが，正答率は低かったと思います。設問では「マルウェア X がサーバからの応答パケットを盗聴するために，ARP テーブルを改ざんする手口」を尋ねていますが，GARP メッセージの送信先が FW ではなく，V 主任の PC などの解答も散見されました。設問で問われていることは何かを，常に意識するようにしましょう。

設問 3 (1)の空欄 f，(2)は，DHCP スヌーピングに関する問題です。SC 試験ではこれまで出題されたことがないので，今回，正解できなくても問題ありませんが，(1)の空欄 g は，「ネットワーク接続時に [g] による認証」とあります。解答群の（エ）～（カ）のうち，クライアント証明書を使って認証に使用されるものは何かを考えれば，おのずと選択できるものは限られると思います。(3)の正答率は高く，LAN の盗聴対策として VLAN を利用することはよく理解されていると感じられました。

問2 サーバ証明書の検証

【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，e は，解答例どおりに対し各 2 点。
(3) b ～ d，f 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 6 点。その他は，基本的に 0 点。
(5) クロスルート証明書の公開鍵，クロスルート証明書の署名とも，解答例どおりに対し各 3 点。

［設問2］

(1) 解答例どおりに対し 6 点。
(2) g 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 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。

【講評】

平均点は 22.6 点（平均正答率は 45.2%）であり，午後 I の中では，問 1 に次ぐ点数でした。

設問 1 (1)は，比較的正答率が高く，DNS キャッシュポイズニング攻撃に関する対策はおおむね理解されていると思われます。(2)，(3)の正答率はまずまずでしたが，空欄 d のコモンネーム，空欄 f の OCSP の正答率は若干低かったようです。(4)の正答率は，少し低かったと思います。「DV 証明書ではアドレスバーに鍵マークが表示されない」旨の答案が散見されました。アドレスバーの表示については，普遍ではないので注意が必要ですが，基本的には URL が「https://」のサイトにアクセスすれば，アドレスバーには鍵マークが表示されます。つまり，サーバ証明書を保持したサイトにアクセスすれば，鍵マークが表示されます。そこで，DV 証明書，OV 証明書，SV 証明書の違いについては十分に理解しておくことが必要です。例えば，フィッシングサイトなどは正規にドメイン名を取得し，ドメイン名の発行権を確認しただけで発行される DV 証明書を用いる事例が多くなっており，注意喚起が行われています。こうしたサーバ証明書の違いに加え，S/MIME 証明書，コードサイニング証明書などの公開鍵証明書の種類なども理解しておくとよいでしょう。また，問題文では，サーバ証明書の検証方法にも触れていますので，再度，基本的な知識を十分に整理するようにしてください。(5)も，少し正答率が低かったようです。例えば，クロスルート証明書の署名を検証するためには，現在利用できる署名は何かを考える必要があります。基本的な知識をベースにしながら，論理的に考えていく姿勢を身に付けるようにしましょう。

設問 2 は，全体的に正答率が低かったと思います。(1)は，CONNECT メソッドの仕様に関するものです。最近，CONNECT メソッドを悪用する例も出題されたことがありますので，その詳細を把握しておくとよいでしょう。(3)は，プロキシサーバで HTTPS セッションを終

端する際の注意点の一つです。サーバ証明書の検証に当たっては，サーバ証明書にあるコモンネームと，アクセスするサイトの FQDN との照合が行われることを理解していれば，正解できると思われます。一方，(4)のプロキシサーバのルート証明書をインストールすることについては，比較的理解されているようでした。

問3 Web サイトのセキュリティ

【採点基準】

［設問1］

a は，解答例どおりに対し 3 点。

［設問2］

(1) b，c は，解答例どおりに対し各 3 点。

(2) d 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 6 点。その他は，基本的に 0 点。

(3) e は，解答例どおりに対し 3 点。

(4) f は，解答例どおりに対し 2 点。

［設問3］

(1) g ～ 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 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】

平均点は 20.0 点（平均正答率は 40.1%）でした。午後 I の 3 問の中では，選択者数が最も少なく，点数も，最も低いものでした。一方，一部の受験者は，かなり高い得点をあげていたようです。

設問 1 は，HttpOnly に限らず，Cookie の属性などについては，Web アクセスにおける基本的な仕組みの一つですから，十分に理解しておきましょう。

設問 2 (1)～(3)は，比較的正答率が高かった半面，(4)の正答率は，低かったようです。答案の中には「&lt」のように「;」が記載されていないものが散見されましたが，些細なミスで合格基準点に届かないこともあります。解答作成に当たっては，丁寧に行うことを常に心掛けるようにしましょう。

設問 3 は，全体的に正答率が低かったと思います。Same-Origin Policy など，Web アクセスにおけるセキュリティ上の考え方のほか，Web 技術全般に関する知識などは，IPA が公開している資料などを基にして，さらに理解を深めていくとよいでしょう。

＜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) 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 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) b 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 6 点。その他は，基本的に 0 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。

［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 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。指摘内容が今一歩のものは 4 点。その他は 0 点。

［設問4］

(1) g は，解答例どおりに対し 5 点。

(2) h，i 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。

［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) j は，解答例どおりに 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 6 点。その他は，基本的に 0 点。

【講評】

問 1 の平均点は 39.5 点で，問題の性質上，問 2 よりも低く，選択者数も少なくなったものと思われます。

設問 1 (2)，(3)の正答率は高かった半面，(1)，(4)は何となく理解しているものの，答案としては適切に表現されていないものが散見され，その結果として正答率は低くなったと思います。

設問 2 は，おおむねよくできていました。

設問 3 は，全体的に正答率が低かったようです。中でも(3)は，DNS に関する問題で，本試験でも，よく出題の対象になっている技術です。DNS の仕組みについては，十分に理解しておくとよいでしょう。

設問 4 (1)は，問題の条件を正しく反映して答案が作成されており，比較的正答率は良かったと思います。(2)の正答率も高かったようですが，(3)は WAF の機能に着目していないような答案が散見されました。(4)，(5)の正答率は，まずまずだったと思います。

設問 5 (1)は，Smurf 攻撃はどのような攻撃かを述べるものですが，Smurf 攻撃は，既に平成 31 年度春期午前Ⅱ試験でも出題されています。ICMP の応答パケットを大量に発生させ，それが攻撃対象に送られるようにしますので，ICMP の応答パケットを悪用することを明確に指摘することが必要です。(2)～(4)の正答率は，比較的低かったと思います。

問2 マルウェア感染と対応

【採点基準】

[設問1]

a ～ d は，解答例どおりに対し各 2 点。

[設問2]

e，f は，解答例どおりに対し各 3 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) g 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。

[設問4]

(1) h 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。

[設問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。

[設問6]

(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 5 点。その他は，基本的に 0 点。

(2) 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。指摘内容が今一歩のものは 3 点。その他は 0 点。

(3) j は，解答例どおりに対し 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各 5 点。その他は，基本的に 0 点。

[設問7]

(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) k ～ n 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各 5 点。その他は，基本的に 0 点。

【講評】

問 2 の選択者数は，問 1 の選択者数よりも少し多く，比率は約 1.35 倍でした。平均点は 45.3 点で，問 1 よりも 5.8 点高くなりました。

設問 1 は，空欄 a，b の正答率が低かったようです。

設問 2 の正答率は，高かったと思います。

設問 3 (2)の正答率は，高かった半面，(1)，(3)の正答率は低かったと思います。しかしながら，一部の受験者は，(1)について，マルウェアに感染した PC が，C&C サーバとの間で DNS プロトコルを使用した通信を遮断する必要性を，適切に指摘できていましたし，(3)については，FQDN に対して変化する IP アドレスに対応する必要性を指摘できていました。

設問 4 は，(1)，(2)とも，正答率は良かったと思います。

設問 5 は，少し難度が高いと思っていましたが，User-Agent ヘッダに着目し，C 社の標準ブラウザ以外のログを抽出することを適切に指摘した答案も見受けられました。

設問 6 (1)～(3)は，正答率は高かったと思いますが，(4)は，「OS のレジストリを書き換える事象」，「プログラムファイルを標準外フォルダに配置する事象」の 2 点とも指摘されたものは，少なかったと思います。

設問 7 (1)は，攻撃者がファイルをインターネット上のサーバに送信することから，ファイルの公開を取引材料にするという点に着目できると考えていましたので，正答率は高くなると想定していましたが，結果は低かったと思います。(2)の公開鍵暗号方式における公開鍵と秘密鍵の使い方は，署名に利用する場合と，情報の暗号化に利用する二つのケースがありますので，その違いを意識しながら選択する字句を決めるとよいでしょう。(3)の正答率は，高かったと思います。

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，設問で問われていることを十分に確認し，素直に解答を作成していくことが必要です。本試験に向け，セキュリティに関する知識のレベルを向上させ，解答の作成能力などに磨きをかけて，必ず合格するように努力していきましょう。

以上