2025 春 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

2025 年 3 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試験の平均点は，45.2 点でした。問題別の平均点は，問 1 が 19.0 点，問 2 が 15.0 点，問 3 が 23.2 点，問 4 が 30.1 点という結果でした。2024 年秋の公開模試における午後試験の平均点は 38.9 点でしたから，点数的には向上しています。

また，今回の公開模試から，本試験にならって，記述式の設問における字数指定を行数指定に変更しました。その結果，1 行内に 30 字を超える文字を記入する答案が散見されるようになりましたが，1 行は 20 マスに対応していることから，cookie などの英単語を含むことを考慮しても，字数的には 1 行に 25 字程度を目安にするのが妥当だと考えられます。こうしたことも考慮し，4 月の本試験を受験されるとよいでしょう。

午後試験において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，こうした解答が少なからず見られました。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なく，その前後に記述されている内容なども含め，よく整理し解答を作成することが大切です。なお，記述式の問題については，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，採点者に理解されやすい解答を作成するようにしましょう。

次に，問題ごとの選択状況を紹介します。問 1（Web サイトのセキュリティ）と問 2（Web システムのサービス連携）の選択者が 11.5%，問 1 と問 3（セキュリティインシデント）が 5.7%，問 1 と問 4（サイバー攻撃への対策）が 5.1%，問 2 と問 3 が 21.7%，問 2 と問 4 が 22.3%，問 3 と問 4 が 33.7%という状況でした。問題ごとでは，問 1 が 11.1%，問 2 が 27.7%，問 3 が 30.6%，問 4 が 30.6%でした。

4 月 20 日に実施予定の本試験において，4 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，午後試験はクリアすることができます。しかし，こうしたことを達成するには，問題の記述内容を十分に把握するだけの知識が要求されます。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，問題文に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，下線に関する設問の場合，その下線部だけに着目して答案を作成するという傾向が見られます。すると，問題に設定されている条件をほとんど考慮することなく，ご自身の知識や下線に関する内容から思いつくことだけを解答してしまいます。前述したように，午後試験では，設問で問われていることを十分に確認した上で，問題の条件を適宜，チェックしながら合理的に導かれる解答を作成していくことが極めて重要です。技術知識面だけではなく，こうした訓練を積み重ねていくことも必要になります。

いずれにしても，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，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。

問1 Web サイトのセキュリティ

【採点基準】

［設問1］

（1）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（会員に cookie を窃取するスクリプトを含むリクエストを罠サイトに送信させること，及びレスポンス中のスクリプトによって窃取した cookie の値を用いて会員にサイト A にアクセスさせること）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) XSS 脆弱性，CSRF 脆弱性ともに，項番が正しく，理由も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）a は，解答例どおりに対し 2 点。

（3）b～d は，解答例どおりに対し各 2 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 4 点。その他は，基本的に 0 点。

（2）e，f は，解答例と同様の意味をもつものに対し各 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 4 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 4 点。その他は，基本的に 0 点。

【講評】

平均点は 19.0 点と，4 問の中では，問 2 に次いで低い点数にとどまりました。選択者数については，全体の 11.1%であり，Web のセキュリティ問題は敬遠される傾向が見られます。

設問 1 では，(1)，(2)の正答率が低かったと思います。例えば，(1)は，問題文に「診断では，リクエストボディに格納されたスクリプトが確認画面で実行された」とあるので，この表現に着目すれば，GET ではなく，POST メソッドが使われていると判断できます。このように，問題の記述内容に従って選択肢を絞れば，正解できることがより多くなると考えられます。(2)は，XSS 脆弱性と CSRF 脆弱性の両方を悪用するという条件などを，どのように反映させるかなどがうまく整理できず，悪用する方法について，解答として分かりやすい説明ができていないように見受けられました。一方，(3)は，比較的正答率が高かったと思います。cookie 属性については，出題頻度が高いので，どのような動作をするものかを，よく把握するようにしましょう。

設問 2 の正答率は平均的だったと思われます。(1)は，設問で問われていることは，B コンテンツを導入済みの利用者が，他の利用者のオーダーした B コンテンツを，ディレクトリトラバーサル脆弱性を悪用して，ダウンロードする方法を具体的に指摘してほしかったと思います。(2)は，比較的正答率が低く，(3)は，想定より正答率は高かったのではないでしょうか。

設問 3 (1)は，攻撃者にとって有効な情報は，表 4（利用者登録機能の応答メッセージ（抜粋））の中では，項番 2 の「利用者 ID が登録済みです」であると判断できます。つまり，登録されている利用者 ID が分かっていれば，それだけ攻撃が成功しやすくなります。こうした点に着目して答案を作成するように改善してほしいと思います。(2)は，診断ユーザーではない加工データが応答されたという問題を解決するには，図 6（参照 API の仕様と脆弱性を検出した手順）を基にして，API キーと対応する利用者 ID と，参照 API のリクエストの送信先 URL に含まれる利用者 ID が一致するかどうかをチェックすることが必要になります。(3)，(4)は，想定よりも正答率は低かったと思われます。できる限り問題の記述内容に基づいて解答を導いていったり，HTTPS を用いる利点は，通信の暗号化のほか，何があるかといった観点から解答を考えていったりすることが必要であると思われます。

問2 Web システムのサービス連携

【採点基準】

[設問1]

(1) a は，解答例どおりに対し 2 点。
(2) b～d は，解答例どおりに対し 3 点（完答）。
(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) e～h は，解答例どおりに対し各 1 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) i は，解答例どおりに対し 3 点。
(2) j 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 6 点。その他は，基本的に 0 点。
(4) k～m は，解答例どおりに対し各 1 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 5 点。その他は，基本的に 0 点。

【講評】

平均点は 15.0 点であり，4 問の中では，最も低い点数でした。一方，選択者数の比率は 27.7%でしたから，ほぼ平均的な選択率になりました。

設問 1 (1)の正答率はやや低く，(2)の正答率は高かったです。認証連携の基本的な流れなどについては，よく理解されていると思います。(3)は，図 1（IDaaS と連携する利用者認証の強化の概要）の内容を確認すれば，解答を導くことができると想定していました。しかし，認可サーバが発行する ID トークンに含まれる情報を，参照するサーバが行う具体的な処理のイメージを思い浮かべられなかったようで，適切な解答を作成できていなかったように感じられました。(4)は，認証連携のシーケンスにおいて，CSRF 攻撃の対策のために使用される state パラメータの検証方法に関する字句選択の穴埋め問題でしたが，正答率はそれほど高くなかったと思われます。(5)は，nonce パラメータの役割を問うもので，問題文中の「RP は，発行した nonce パラメータをセッションと紐づけて管理し，……」という記述に基づいて，解答を作成してほしかった問題です。nonce パラメータは，ID トークンを不正に入手した攻撃者が行うリプレ

イ攻撃の対策のために使用されるものです。state パラメータの役割とともに，よく理解しておくとよいでしょう。

設問 2 は，正答率は少し低かったと思います。正答率を高めるようにするには，幅広く Web 関連の技術や認証連携の仕組みを理解していくことが求められます。特に(2)の空欄 j に入れる字句については，図 5（OAuth 2.0 を用いるサーバ連携の構成要素と流れ）のサーバ C は，サービス M のリソースサーバに対して，自動投稿処理を実行可能にするには，どのようなことを許可しているかという観点から考えるとよいでしょう。(3)も，図 5 の「(3) 認可要求」と「(7) アクセストークン要求」を対比させながら，表 2 の番号(7)で使用されている Authorization ヘッダーの使用目的を考えることが必要です。(4)は，PKCE（Proof Key for Code Exchange）の仕組みを考える問題でしたが，空欄 l に入れる検証コードと，空欄 m に入れるチャレンジコードを逆に答えた答案が多く見られました。

設問 3 (1), (2)の正答率は，やや低かったです。(1)は，TLS クライアント認証を行う際に，開発 PC にインストールされるクライアント証明書は，どの CA から発行され，その CA のルート証明書はどこに登録されているかを，問題文の記述に基づいて答えるものでしたが，必ずしもその状況を読み取ることができていなかったように見受けられました。(2)は，インシデントが発生した場合に，影響の拡大を防ぐためにサービス Q において行うべき対処を問うものでしたが，問題の条件を素直に反映して作成された答案は少なかったと思われます。

問3 セキュリティインシデント

【採点基準】

［設問1］

（1）a～c は，解答例どおりに対し各 2 点。

（2）サーバ名，ポートとも解答例どおりに対し 4 点（完答）。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）d～f 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。

［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） g は，解答例どおりに対し 3 点。

（3）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 6 点。その他は，基本的に 0 点。

【講評】

平均点は 23.2 点でした。午後の 4 問の中では，問 3 の次に高い点数になりました。選択者数の比率は 30.6%で，問 4 と同じ比率になり，約半数以上の受験者が選択していたことになります。

設問 1 (1)，(2)とも正答率は高かったです。

設問 2 (1)は，権威 DNS サーバに TXT レコードを登録した場合，不正プログラムが DNS リクエストを送信し，その応答を受け取ることによって，リソースデータの内容に従って，新たな攻撃などの実行を試みる手法に関するものです。例えば，TXT レコードには任意のデータを登録できますから，攻撃者は，適宜，登録内容を変更することによって，様々な攻撃を試みることができます。こうした知識を有していれば，容易に解答を作成することができるのではないでしょうか。(2)の正答率は，平均的でした。空欄 e，f に入れる IP アドレスのうち，FW の DMZ 側インタフェースの IP アドレスを答えた答案が，少なかったという印象を受けました。(3)は，cron エントリーが，どのような動作をするかという知識がないと，なかなか正解を求めることは難しいと考えられるので，本試験に向けて，様々な知識を幅広く身に付けていくようにするとよいでしょう。

設問 3 の正答率は，少し高かったと思われます。(1)は，不正なプログラムなどはプロキシ認証を突破できないので，インターネット接続ができない旨の答案がありましたが，この設問では，なぜプロキシ認証を突破できないかという理由を述べた答案を正解にしています。(2), (3)の正答率は，平均的でした。(4)の正答率は，少し高かったと思われますが，具体的に答えることが求められているので，表 1（FW のフィルタリングルール）のどの項番を変更するかという点を指摘することがポイントになります。

問4 サイバー攻撃への対策

【採点基準】

［設問1］

（1）a～c は，解答例どおりに対し各 2 点。

（2）d，e は，解答例どおりに対し各 2 点。

（3）解答例どおりに対し 4 点。

［設問2］

（1）認証の 3 要素，VPN-GW で用いられる要素とも，解答例どおりに対し各 3 点（完答）。

（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）f，g は，解答例と同様の意味をもつ字句を指摘したものに対し各 3 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。

【講評】

平均点は 30.1 点で，午後 I の中では，最も高い点数でした。選択者数の比率は 30.6%で，問 3 と同じ比率になりましたが，平均点で評価すると，問 3 と問 4 を選択した受験者は，必然的に午後試験における点数が高くなります。このため，総合評価として判定される評価は，かなり甘い判定になっているはずですから，この評価に満足することなく，本試験に向けてさらにレベルアップする努力をしていくことが大切であると思われます。

設問 1 (1)，(2)とも，正答率は高かったです。(3)の無害化処理を答える用語問題は，平均的だったといえます。

設問 2 の(1)は，基本的な用語問題でしたから，正答率は高かったです。(2)の正答率も，プッシュ通知の問題点を十分に把握されていたようで，高かったです。(3)は，デジタル証明書によってクライアント認証を行う方式を採用した場合，リモート接続用 PC（R-PC）に必要とされる作業内容を答えるものでした。しかし，答案では，必ずしも作業内容を的確に指摘されているとは限らなかったことなどから，正答率は平均的だったといえます。

設問 3 (1)の空欄 f，g に入れる字句については，問 4 の中では，比較的正答率が低かったといえるのではないでしょうか。空欄 f，g に入れる字句については，空欄の前後にある記述を基に考えれば，正解に至ると思われます。例えば，空欄 g については，SPA パケットの最後尾フィールドには HMAC が格納されていると記述されています。このため，HMAC はどのような目的に使用されているかを考えれば，SPA パケットの改ざんを検知するので，「改ざん」という字句を入れることができます。答案の中には「盗聴」などの答えも見られましたが，こうした基本的な問題は取りこぼしをしないことが必要です。(2)，(3)の正答率は，比較的高かったと思います。

午後試験の試験時間は 2 時間 30 分，4 問の中から 2 問を選択して解答します。このため，1 問当たり 75 分を割り当てることができるので，時間的な余裕はあると思われます。例えば，最初に選択する問題を 2 問に絞ることができれば，その 2 問に集中することができます。おそらく，問題選択に当たって迷いが生じるのは，3 問の中から 2 問を選択する場合ではないでしょうか。このような場合には，問題選択に当てる時間として，20 分程度をあらかじめ見込んでおくこともよいかもしれません。

いずれにしても，解答する問題を決めると，その後は問題文を十分に読み込んでください。例えば，最初に読む際に，空欄に入れる字句が分かれば，その字句を入れておきましょう。一読した後，設問で問われていることを確認します。設問で問われている意味をよく理解し，その設問に関連する問題文を十分にチェックするようにしましょう。解答を導くための関係などを整理する際には，頭の中だけで考えるのではなく，メモのような形にして目に見えるようにして考えるとよいでしょう。そうすれば，条件の見落としなどが少なくなり，解答を作成しやすくなるはずです。

しかし，こうした作業がスムーズに実施できるようになるには，どうしてもセキュリティ関連の知識を十分にもち合わせているかどうかがポイントといえます。このため，4 月 20 日に行われる本試験の実施日に向け，より多くの知識を吸収するなどして，さらなるレベルアップを図るようにしましょう。

試験当日において，問題に向き合ってみると，全く歯が立たないなどの印象を受けることがありますが，十分な実力を付けていれば，問題を丁寧に読んでいくことによって，解決の糸口を見つけられるはずです。そして，自分自身の考えがまとまれば，的確で理解しやすい内容の答案を作成するようにしましょう。たとえ，行き詰ったりしても，必ず合格するという強い気持ちをもって，粘り強く取り組んでいくことを忘れないようにしましょう。

以上