2025 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

2025 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試験の平均点は，36.3 点でした。問題別の平均点は，問 1 が 13.2 点，問 2 が 22.7 点，問 3 が 14.8 点，問 4 が 22.6 点という結果でした。2025 年春の公開模試における午後試験の平均点は 45.2 点でしたから，点数的にはかなり低下する結果となりました。

また，公開模試でも，本試験にならって，記述式の設問における字数指定をほとんどなくし，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，10 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はなく，その前後に記述された内容なども含め，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（セキュリティ対策の見直し）の選択者が 13.4%，問 1 と問 3（マルウェア対策）が 16.5%，問 1 と問 4（クラウド環境のセキュリティ対策）が 3.0%，問 2 と問 3 が 29.3%，問 2 と問 4 が 5.5%，問 3 と問 4 が 32.3%という状況でした。問題ごとでは，問 1 が 16.5%，問 2 が 24.1%，問 3 が 39.0%，問 4 が 20.4%でした。

10 月 12 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）a は，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（例えば，攻撃者が用意する画面が，予約確認画面の透明な状態で利用者から見て手前に表示される旨の答案）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）解答例どおりに対し 2 点。

[設問2]

（1）解答例どおり（完答）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 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（サイト X にログイン済みの利用者を攻撃者の Web サイトに誘導した後の動作が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]

解答例と同様の趣旨が適切に指摘されているもの（パスワードレス認証であること，接続先のオリジンを

検証することの二つが解答されているもの）に対し6点。一方だけを指摘したものは3点。その他は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4点。その他は，基本的に0点。

（2）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4点。その他は，基本的に0点。

（3）解答例どおりに対し2点。

（4）c 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 13.2 点に過ぎず，4 問の中では，最も低い点数にとどまりました。選択者数については，全体の16.5%であり，Web セキュリティの問題は少し敬遠される傾向にあるといえます。

設問 1 (2)の正答率は，やや低かったと思います。答案を見ると，理屈は理解されているものの，それが必ずしも分かりやすく表現されていなかったように見受けられました。

設問 2 (1)の正答率は，高くなると想定していましたが，そうではありませんでした。(1)は，Same-Origin の基本的な知識ですから，しっかり把握しておくようにしましょう。設問 2 (2)で問われていることは，悪意のあるサイトにアクセスして，その応答に含まれる攻撃スクリプトがサイトXで実行されても，サイトXのcookie が窃取されない理由です。オリジンの異なるサイトには cookie が送信されない旨の答案が散見されました。設問 2 (3)，(4)でも問われていることと，少し異なる観点から答案が作成されていたように見受けられました。また，Same-Origin の制約があると，クロスオリジンのリソースアクセスに支障をきたすので，サーバ側が許可した範囲に限りそのアクセスを許可する仕組みとして CORS（Cross-Origin Resource Sharing）があります。こうした基本的な知識を一つ一つ理解し，全体の関係が明確になるようにしていくとよいでしょう。

設問 3 は，パスキーに関する問題です。FIDO2 が，パスワードスプレー攻撃，並びに MITM 攻撃の二つに対して，効果がある理由をそれぞれ述べることが必要ですから，丁寧に解答を作成するようにしましょう。

設問 4 (1)，(3)の正答率は，平均的でしたが，(2)，(4)の正答率は，低かったと思います。設問で問われていることをしっかりと見極めた上で，問題の条件などをよく確認しながら，解答を作成するように心掛けていくようにしましょう。

問2　セキュリティ対策の見直し

【採点基準】

［設問1］

（1）a～e は，解答例どおりに対し各2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。

（4）g は，解答例どおりに対し2点。

［設問2］

（1）h は，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に対し4点。その他は，基本的に0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。

［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。指摘内容が今一歩のものは2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。

（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 22.7 点であり，4 問の中では，最も高い点数でした。一方，選択者数の比率は 24.1%でしたから，平均的な選択率であったといえます。

設問 1 (1)の正答率は，やや低かったようです。State パラメータ，nonce は，それぞれどのような攻撃に対して有効になるのかをはじめ，PKCE（Proof Key for Code Exchange）の検証コードとチャレンジコードとの関係，アクセストークンと ID トークンとの違いなど，基本的な仕組みを十分に把握しておくとよいでしょう。(2)の正答率は平均的であった半面，(3)の正答率は，低かったと思います。(4)の正答率は，やや高く，TLS 証明書のライフサイクルの問題などについては，よく理解されているようです。

設問 2 は，SPF，DKIM，DMARC という送信ドメイン認証技術の問題です。(1)を除き，そのほかの記述式の設問の正答率は，やや低かったという印象を受けました。(2)は，表面的に解答するのではなく，D さんと U 氏の会話を注意深く読んで，何が原因になっているかなどを

見極めることが必要です。そして，エンベロープ FROM とヘッダーFROM のドメインに何が設定されているかを，考えていきましょう。(3)は，SPF 認証の問題点ともいえるもので，攻撃者がドメインを正規に取得し，そのドメインの権威DNSサーバにSPFレコードを登録すると，SPF 認証に成功してしまいます。このような知識は基本的なものですから，よく把握しておきましょう。(4)は，表 5（DMARC レポートの内容（抜粋））を十分に理解した上で，解答を導いていくことが必要です。このため，問題の記述内容については，十分に理解できるだけの知識を身に付けるようにしましょう。

設問 3 は，(1)～(4)とも，正答率は，やや高かったと思います。グループに与える権限や，認証と認可の関係，UEBA（User and Entity Behavior Analytics）の仕組み，従業員の不正を抑止するための対策などについては，概ね理解されていると感じられました。

問3 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 1 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）c～e，f～h は，それぞれ完答で，各 3 点。

（4）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。

（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 4 点。その他は，基本的に 0 点。

［設問2］

（1）j は，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 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。

［設問3］

（1）k，l 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。指摘内容が今一歩のものは 3 点。その他は 0 点。

【講評】

平均点は 14.8 点にとどまりましたが，午後の 4 問の中では，問 1 よりも少し高い点数でした。選択者数の比率は 39.0%で，最も多い受験者が選択していました。

設問 1 (1)の正答率は平均的でした。(2)は，PC にマルウェアが送り込まれた状態において，そのマルウェアが攻撃者のサーバとHTTPS通信を行うパターンを答えるものです。そして，設問では「HTTPS 通信は，VPN サーバを経由する通信ではない」という条件が付けられていますので，攻撃者のサーバが VPN サーバを経由して，マルウェアに感染した PC との通信を行うものを除外して考えることが必要ですが，攻撃者のサーバからの指令に従ってマルウェアがHTTPS通信を行う旨の答案も散見されました。あくまでも問題及び設問の条件などを見極めながら，解答を考えていくことが大切です。(3)は，F-PC-20 に侵入したマルウェアが，ARP スプーフィングという手法を用いて，F-PC-30 とファイルサーバとの通信を盗聴する方法を問いましたが，安易に解答を作成されているという印象を受けました。このような問題は，頭の中で考えるのではなく，図を描くようにして考えるとよいでしょう。また，ARP スプーフィングは，同じネットワークセグメント内の機器同士の通信に対して行われる攻撃ですから，対象の機器は，F-PC-30 と L3SW になります。こうした基本的な知識を用いて，丁寧に解答を考えていくことも必要です。(4)は，図 4（ランサムウェアによる暗号化の動作）を基に解答を作成していくことがポイントです。(5)も，正答率は少し低かったと思います。

設問 2 (1)の正答率は，平均的でしたが，(2)の正答率は少し低かったです。TLS クライアント認証を行う上で重要なことは，クライアント（M-PC）にインストールされたクライアント秘密鍵で認証が行われるということです。このため，M-PC にインストールされたクライアント秘密鍵を，ほかの機器にエクスポートされないようにしなければなりません。(3)，(4)の正答率は平均的でした。

設問 3 (1)のうち，空欄 k の正答率は，少し低かったです。(2)は，IoC に関する知識を問うものですから，IoC に関する知識を整理して，その知識をこれから有効に活用するようにしてください。

問4 クラウド環境のセキュリティ対策

【採点基準】

［設問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。

［設問2］

（1）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）a，b 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。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 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 6 点。その他は，基本的に 0 点。

［設問4］

（1）c，d は，解答例どおりに対し各 1 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 22.6 点で，午後 I の中では，問 2 とほぼ同程度の点数でした。選択者数の比率は 20.4%で，問 1 よりも少し高い比率になりました。

設問 1 の正答率は，平均的でした。ローカルブレイクアウト機能は，概ね理解されているようです。

設問 2 (1)の正答率は，高かったですが，(2)の正答率は，平均的でした。(2)は，許可されていない SaaS への接続を監視することなどといった答案も散見されましたが，下線③の中にある，「機密情報の漏えいを防止する観点」に着目することが必要ですから，設問をよく確認しながら答案を作成することを，常に心掛けてほしいと思います。(3)の正答率は，高かったですが，(4)の正答率は，低かったです。FIDO2 の認証方式は，パスワードレス認証であることはよく理解されていますが，認証器と認証サーバとの間は，公開鍵暗号方式で認証が行われます。つまり，認証器は自身の秘密鍵を使用して署名を作成しますが，この署名対象データとして使用されるものが，認証サーバから送られてくるチャレンジコードです。なお，認証器で使用する秘密鍵については，生体認証などによって認証が行われた後，秘密鍵が使用できるという仕組みになっています。

設問 3 (1)の正答率は高く，(2)の正答率は，やや低かったです。社内からインターネットにある機器に対して VPN 接続を行うには，インターネット側にある機器から社内に対して接続要求を受けると，そこがセキュリティホールになる可能性がありますので，社内から外部へ接続することが基本です。

設問 4 (1)，(2)の正答率は平均的でした。(3)の正答率は，やや低かったと思います。DNS クライアントとキャッシュ DNS サーバとの間，キャッシュ DNS サーバと権威 DNS サーバとの間は，それぞれ別の技術が使用されますので，よく理解しておくとよいでしょう。(4)の正答率も，低かったと思います。

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，必然的に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になります。このため，10 月 12 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