令和６年度　春期　情報処理安全確保支援士試験　採点講評

午後試験

問１

問 1 では，API セキュリティを題材に，セキュリティ設計及び脆弱性対応について出題した。全体として正答率は平均的であった。

設問 2(2)は，正答率がやや低かった。JSON Web Token（JWT）改ざんにおける検証方法を問うたが，既に実装されている対策を解答するなど，脆弱性を正しく理解していないと思われる解答が散見された。図 4 に示す仕様と表 3 に示す脆弱性を正しく理解してほしい。

設問 3(1)は，正答率がやや低かった。脆弱性の存在を判断するための仕組みについて問うたが，図 6 に示す攻撃の流れに合っていない解答が散見された。脆弱性対策では，脆弱性を悪用する攻撃の流れの理解が重要であることから，正確に理解してほしい。

設問 3(4)の利点については，正答率が高かった。WAF の利点と課題は正確に理解していると思われる。セキュリティ施策は導入前にトレードオフを検討してほしい。

問２

問 2 では，サイバー攻撃への対策を題材に，リモートワーク及び DDoS 攻撃に対するセキュリティ対策について出題した。全体として正答率はやや高かった。

設問 1(2)は，正答率が高かった。アノマリ型 IPS 機能で，しきい値の設定に関する問題であったが，IPS 機能の仕様を反対に理解していると思われる解答が散見された。機能は正確に理解してほしい。

設問 2(1)は，正答率が平均的であった。多要素認証を突破する攻撃について問うたが，手順が不足している解答や，設問とは異なる攻撃についての解答が散見された。攻撃を正確に理解することによって，対策も立てやすくなるので，正確に理解してほしい。

設問 3(2)は，正答率が平均的であった。SPA というプロトコルに関して本文中に示して効果を問うた。内容を理解して解答してほしい。

問３

問 3 では，クラウド環境で構築された Web サイトを題材に，脆弱性を悪用した攻撃手法とその対策について出題した。全体として正答率はやや低かった。

設問 1(2)は，正答率が低かった。クロスサイトスクリプティング（XSS）の検出箇所から，問合せ管理機能でスクリプトを実行できるのは管理者であることが分かる。一方，サイト X の機能概要から，利用者情報を取得するには，会員管理機能を利用すればよいことが分かる。この二つをどう結びつけるかを考えて，解答してほしい。

設問 2(1)は，正答率が低かった。クロスサイトリクエストフォージェリ（CSRF）の攻撃手法に関する問題であったが，攻撃者が取得したトークンを悪用する部分について解答できていない受験者が多かった。本文の状況に即して解答してほしい。

設問 4(3)は，正答率がやや低かった。クレデンシャル情報を取得する方式について解答できていない受験者が多かった。方式が二つあり，その違いに即して解答してほしい。

問４

問 4 では，Web アプリケーションの脆弱性対策を題材に，Linux の権限設定及びセキュアコーディングについて出題した。全体として正答率は平均的であった。

設問 2(5)は，正答率が低かった。Java 言語での例外処理仕様を理解していないと思われる解答が散見された。例外発生時の動作は脆弱性につながりやすい部分である。プログラム言語での適切な例外処理はセキュアコーディングの基本的内容であり，正確に理解してほしい。

設問 2(6)は，正答率がやや低かった。Java 言語には例外発生時でも必ず実行される処理を記述する仕組みが用意されており，リソースリークを防ぐために重要な仕組みである。正確に理解してほしい。