令和６年度　秋期　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，ソフトウェア開発会社の社内システムの運用及びインシデントレスポンスを題材に，ログを調査する能力及び技術的対策を立案について出題した。全体として正答率は平均的であった。

設問１(3)は，正答率が高かった。被害の可能性を複数のログから適切に読み取ることができていた。

設問１(8)は，正答率が平均的であった。どのログを確認するかの記述がない解答が多かった。マルウェアの動作によって，どのログに何が記録されているかを考え，検知の仕組みを設計できる能力を培ってほしい。

設問 2ｆは，正答率がやや低かった。ファイルサーバのアクセス権を最小限にするといった解答が散見されたが，マルウェアは，特別な権限なしにファイルを持ち出している。ファイルの持出しに対する技術的対策は複数考えられるが，インシデントで起きたファイルの持出しを防止できる対策を選択してほしい。

問２

問 2 では，電子メール（以下，メールという）のドメイン名の変更を機にした新たなメールサービスの導入を題材に，メールサービスの設定，変更前のドメイン名の契約維持の要否，及び DMARC の導入について出題した。全体として正答率は平均的であった。

設問 2 は，正答率が平均的であった。“S/MIME”といった解答が散見された。“S/MIME”は，MIME の仕組みを使ったメール本文及び添付ファイルの暗号化の方式であって，SMTP を暗号化する方式ではない。メールに関連する暗号技術及び通信プロトコルについて，よく理解してほしい。

設問 3(1)は，正答率が低かった。DKIM の仕組み及び表 6 のタグの内容を用いれば，正答を導くことができる。DKIM の仕組みについて，よく理解してほしい。

設問 5(2)SPF は，正答率がやや低かった。メールの Subject に通番情報を付加するといった解答が散見された。SPF では，Subject を判定対象としていない。SPF の仕組みについて，よく理解してほしい。

設問 5(2)DKIM は，正答率が平均的であった。表 6 の h タグにおいて，Subject を判定対象として含んでいる。メールの Subject に通番情報を付加すると，DKIM による認証が失敗する。DKIM の仕組みと，メーリングリストの設定を理解した上で，解答してほしい。

問３

問 3 では，EC サイトのクレジットカード情報の漏えいを題材に，Web サイトの改ざん手法と影響を受けた利用者の調査について出題した。全体として正答率は平均的であった。

設問１c は，正答率がやや低かった。クロスサイトスクリプティング（XSS）脆弱性は反射型，格納型，DOM ベースの 3 種類あるが，ログから攻撃を分析するためにもそれらの違いを理解してほしい。

設問 2(1)は，正答率がやや低かった。書換え対象のラジオボタンの選択肢が残っていたり，余計な改ざんがされていたりといった改ざん内容に過不足のある解答が散見された。HTML，DOM の仕組みを利用した画面の書換えは攻撃で悪用される可能性があるので，よく理解してほしい。

設問 3(1)は，正答率が平均的であった。通信を盗聴する，キーロガーを仕掛けるといった解答が散見された。クレジットカード情報がクエリパラメータとして送られ，かつ Web サーバのアクセスログにリクエスト URI が記録されることを理解した上で解答してほしい。

問４

問 4 では，個人情報を取り扱う Web サイトに対するセキュリティ診断を題材に，診断ツールで検出された脆弱性について，悪用された場合の被害及び被害を低減するための対策について出題した。全体として正答率は平均的であった。

設問 1(2)は，正答率が高かった。セッションフィクセーション脆弱性について，よく理解できていた。

設問 1(5)f は，正答率が低かった。攻撃による被害を軽減する HTTP ヘッダーについて，設定した場合の効果をよく理解してほしい。

設問 2g は，正答率が低かった。攻撃の後の流れに合っていない解答が散見された。Web サイトの全体の機能を考慮し，脆弱性を組み合わせて悪用する攻撃を考える能力を培ってほしい。

設問 3 は，正答率がやや低かった。被害を軽減できない誤答が散見された。Web サイトでは，取り扱う情報の機密性などに応じた，認証やアクセス制限が必要である。それぞれの Web サイトの特性を考慮したセキュリティ対策を策定する能力を培ってほしい。