令和７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，サプライチェーンセキュリティを題材に，委託先の管理及び開発プロセスにおけ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平均的であった。

設問 2(1)は，正答率がやや高かった。JavaScript が正しく動作しない配置方法の解答が散見された。本文中で示されているシステム構成を理解した上で解答してほしい。

設問 4 は，正答率が平均的であった。脆弱性管理における SBOM 利用の利点を問う問題であったが，SBOM の利用方法が説明できておらず，SBOM の定義を記載しただけの解答が散見された。各種ガイドラインで利用が推進されていく分野であるので，SBOM の利用の方法や目的を正確に理解してほしい。

設問 5(2)は，正答率が低かった。SAST，DAST，IAST といった開発プロセスで活用するセキュリティテストツールについて，それぞれの特徴を理解してほしい。

問２

問 2 では，脆弱性管理を題材に，脆弱性，その深刻度レベル及び対応優先度について出題した。全体として正答率は平均的であった。

設問 1 は，正答率が平均的であった。本文中で示されている Web サイトの仕様が考慮されていない解答が散見された。本文をよく読んで解答してほしい。

設問 4(1)は，正答率が低かった。CVSSv3 の評価指標のうち，Attack Complexity（AC）の攻撃条件の複雑さについて出題をしたが，多くの受験生が C（Confidentiality Impact）の機密性への影響として解答していた。各評価指標の意味を理解して解答してほしい。

設問 5(1)は，正答率が低かった。CVSSv3 の現状値と EPSS 値を比較して，手間の掛かる理由と掛からない理由を出題した。CVSSv3 の現状値と EPSS 値の利用手順を理解していない解答が散見された。それぞれの利用方法を具体的に理解してほしい。

問３

問 3 では，スマートフォン用アプリケーションプログラム（以下，スマホアプリという）を題材に，脆弱性，それを悪用した攻撃手法及び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(3)は，正答率が低かった。クラウドストレージサービスのアクセスキーを不正利用することによって，ストレージ上の全利用者の写真をダウンロードする具体的な方法を問う問題であったが，抽象的な解答が散見された。設問文をよく読んで解答してほしい。

設問 2(3)は，正答率が低かった。プライベート認証局のルート証明書を端末にインストールすることによって，サーバ証明書の検証エラーを解消させる方法を問う問題であった。同様の方法は，ネットワーク機器の TLS インスペクション機能などでも利用されるので，理解してほしい。

設問 3 は，正答率が平均的であった。署名付き URL の適切な生成場所を解答させる問題であったが，攻撃者による解析が容易なスマホアプリ上という解答が散見された。秘密情報の処理をサーバ上で完結させ安全を確保する実装は，クライアントサーバ型でも採用される基本的な方法なので，理解してほしい。

問４

問 4 では，IT 資産管理と脆弱性管理を題材に，アタックサーフェスマネジメント（ASM）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 のサーバの設定の変更内容を問う設問は，正答率が低かった。本文中で示された事象が，CDN サービスや Web サーバの使用終了後の DNS の CNAME レコード削除漏れによってサブドメインテイクオーバーが起きていることを理解した上で，その具体的な対策方法を解答してほしい。

設問 3(1)，(2) は，正答率が平均的であった。本文中で示された状況を踏まえて公開サーバの稼働状況の調査方法を問う問題である。実際の現場でも，状況に応じて調査方法を選ぶ知識が必要なので，理解を深めてほしい。

設問 3(3)は，正答率が平均的であった。継続する場合としない場合を取り違えて反対を解答するケアレスミスと思われる解答が散見された。長文を根気よく読み解いた上で，慎重に解答してほしい。

設問 4(2)，(3)は，正答率が低かった。対応の優先度を考える上では，脆弱性の技術的な特性，脆弱性を取り巻く現状，ユーザーの環境が重要であるとされ，KEV カタログが現状の評価に活用されるので，理解してほしい。