令和７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，従業員による Web アプリケーションへの攻撃を題材としたインシデントを通して，脆弱性の分析，攻撃手法の特定，及び対策の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 は，正答率がやや低かった。Content Security Policy（CSP）を理解することは，堅牢な Web システムを開発及び構築する上で重要である。リソース読込みの制御を適切に行うために，CSP の内容や緩和効果について理解を深めてほしい。

設問 2 は，(1)～(4)の正答率が高かった。図 3 及び図 4 から攻撃内容を読み取ることができている受験者が多かった。一方で，(5)の正答率がやや低かった。CSP による制御を回避する攻撃手法について考察することは，攻撃者によるスクリプト実行を防ぐ対策を立案する上で重要である。CSP の仕組みについて理解を深めてほしい。

設問 4 は，正答率が低かった。脆弱性を検出し修正するための開発プロセスを出題したが，“ログ分析を行う”や“ID の棚卸しを行う”，“アノマリ検知の仕組みを導入する”などの運用プロセスでの対策，“権限チェックを行う”，“多要素認証の仕組みを導入する”などの修正機能の追加，及び“WAF を導入する”などのセキュリティ製品導入に関する解答が散見された。開発プロセスに対する理解を深めてほしい。

問２

問 2 では，暗号資産交換業における暗号鍵の管理を題材に，暗号技術の適切な利用方法について出題した。全体として正答率は平均的であった。

設問 3(1)は，正答率がやや低かった。一般に，攻撃者が不正行為を行うために用いる手段を推測することは，セキュリティを強化する上で重要である。システム構成及び業務手順を詳細に把握し，既存業務における弱点を見つけられるようにしてほしい。

設問 3(2)は，正答率が低かった。“デジタル署名”という解答が多く見られた。さまざまな暗号技術をしっかり理解してほしい。

設問 4(1)は，正答率が平均的であった。情報の暗号化において暗号鍵としてパスワードを用いることは一般的であり，適切にパスワードを管理すれば情報の機密性を守ることができる。しかし，攻撃者が暗号文とパスワードを同時に入手できれば情報が攻撃者に知られてしまう。パスワードなどの暗号鍵及び暗号化した情報の管理方法を併せて検討してほしい。

問３

問 3 では，インターネットバンキングの利用とリモートワーク環境の導入を題材に，社内の IT 環境のセキュリティ対策及び VPN サービスの導入方法について出題した。全体として正答率は平均的であった。

設問 2 は，正答率がやや高かった。インターネットバンキングの振込みの流れやハードウェアトークンの特徴を理解し，攻撃手法を正しく想定できていることがうかがえる。

設問 4(2)は，正答率が低かった。社内から VPN サービスを利用する場合に，初期設定時及び VPN 接続前に必要な通信も踏まえて解答してほしい。

設問 5(1)は，正答率が平均的であった。外部の攻撃者の不正アクセスを防止する上で，リモートワーク環境における認証は重要な役割である。本環境で利用する認証基盤の仕様を踏まえ，スマートフォン故障時にもセキュリティ強度を落とすことのない代替策を解答してほしい。

問４

問４では，セキュリティ管理体制の構築について出題した。全体として正答率は平均的だった。

設問 3 は，正答率がやや低かった。提示された攻撃シナリオに対して有効な対策を問うたが，SCADA の利用者認証の強化という解答が散見された。マルウェアは，OS やアプリケーションの脆弱性を悪用したり，正常に認証された利用者をだましたりして実行される。マルウェア対策として利用者認証の強化はあまり効果がないことに注意してほしい。

設問 4 は，正答率が平均的だった。万一マルウェアなどによる被害が発生してしまった場合に，いかに早く復旧するかを問うたが，被害に至る攻撃を阻止する手段について言及した解答が散見された。迅速な復旧のためにはバックアップの取得など平常時に何を行うかが重要であり，この点についての解答を期待していた。レジリエンスという言葉に代表されるように，企業の社会的立場によっては，被害に至る経緯を解明するよりも，事業の復旧を優先する場合もあることを考えてほしい。