令和５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，Web アプリケーションプログラムの脆弱性悪用によって発生したインシデントへの対応を題材に，悪用されたクロスサイトスクリプティング（XSS）脆弱性の把握と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 1(1)は，正答率は平均的であったが，スクリプトで DOM を使用していたことからか，“DOM Based XSS”と誤って解答する受験者が散見された。脆弱性の種類や埋め込まれた状況に応じた適切な対策を施すためにも，脆弱性は特徴や対策方法まで含めて，正確に理解してほしい。

設問 2 は，正答率が平均的であった。HTML やスクリプトをよく確認すれば解答ができたはずであるが，“開発者ツールで入力制限を削除してから投稿した”のように，確認が不足していると考えられる解答が一部に見られた。攻撃者の残した痕跡を注意深く確認し，攻撃者の行った攻撃の方法を正確に把握する能力を培ってほしい。

設問 3(3)は，正答率が高かった。攻撃によって起きるかもしれない被害を推察して解答する必要がある問題であったが，EC サイトにおいて cookie が攻撃者に取得されることの影響について，よく理解されていた。

問２

問 2 では，アパレル業におけるセキュリティ対策の見直しを題材に，サーバ証明書の検証，秘密鍵の管理及び無線 LAN 環境の見直しについて出題した。全体として正答率は平均的であった。

設問 1(2)は，正答率が低かった。攻撃者が偽サイトを用意したとしても，HTTPS でアクセスするのであれば，サーバ証明書の検証に失敗する。サーバ証明書の検証は，通信の安全性を確保するうえで基本的な知識であるので，具体的にどういった事項を検証するのかということまで含めて，よく理解しておいてほしい。

設問 3(2)は，正答率がやや高かったが，“公開鍵”や“サーバ証明書”といった解答が一部に見られた。PKI は，様々なセキュリティ技術の基礎となる重要な技術であるので，どのような場面でどのように利用されているのか，よく理解しておいてほしい。

設問 3(7)は，正答率が高かった。ファイアウォールの全てのフィルタリング設定と無線 LAN 環境の見直しに伴う影響を理解して解答する必要があったが，適切に理解されていた。

問３

問 3 では，継続的インテグレーションサービスを提供する企業とその利用企業におけるセキュリティインシデント対応を題材に，クラウドサービスを使ったシステムで起こりうる攻撃手法とその防御について出題した。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。コンテナにおけるシステムの動作は，仮想化技術の基本である。どのような権限や仕組みによって実行されるか，コンテナを使ったシステムの構成及び特性をよく理解してほしい。

設問 2(5)は，正答率が低かった。WebAuthn をクライアント証明書認証やリスクベース認証などほかの認証方法と誤認した解答が多かった。WebAuthn はフィッシング耐性がある認証方法である。Passkey という新たな方式も登場し，普及し始めている。ほかの認証方法とどのように異なるのか，技術的な仕組みを含め，よく理解してほしい。

設問 3(3)は，正答率がやや低かった。“電子署名を暗号化できる”，“秘密鍵が漏えいしても安全である”などといった，暗号技術の利用方法についての不正確な理解に基づく解答が散見された。HSM を使うセキュリティ上の利点に加えて，暗号技術の適正な利用方法についても，正確に理解してほしい。

問４

問 4 では，業務委託関係にある百貨店と運送会社を題材に，個人情報に関するリスクアセスメントについて出題した。全体として正答率は平均的であった。

リスクアセスメントの中でも，リスク特定は担当者の知見が重要なプロセスである。本文内の状況説明と受験者自らの知見とを組み合わせてリスクを洗い出す能力を，設問 2 では問うた。多くの受験者が適切な解答を記述していたが，特定したリスクが具体性に欠けており，リスク分析の段階で被害の大きさや発生頻度の評価ができていない解答が散見された。また，“W 社外の第三者”や“W 社へのサイバー攻撃”といったリスクの前提に合っていない解答も一部に見られた。

リスクアセスメントは，組織の秘密情報を保護するための基本的なプロセスであり，このプロセスで大きなリスクの見落としがあると，重大なインシデントの発生につながってしまうおそれがある。情報処理安全確保支援士（登録セキスペ）の専門性が発揮されるべき重要なプロセスであるので，リスクアセスメントの流れについて理解するとともに，その流れの中で，脅威を想定して攻撃シナリオを作成する方法及び攻撃シナリオを分析する方法について理解を深めるよう，学習を進めてほしい。