平成 30 年度　春期　情報処理安全確保支援士試験　採点講評

午後 II 試験

問 1

問 1 では，セキュリティ対策の評価について出題した。全体として，正答率は高かった。

設問 1(1)，(2)は，DOM-based XSS に関する設問であったが，反射型 XSS について言及した解答が散見された。DOM-based XSS が引き起こされる原理についてよく理解しておいてほしい。また，設問 1(3)は，正答率が低かった。HttpOnly 属性は Cookie の値を不正に操作されることを防ぐために有効なので，よく理解しておいてほしい。

設問 3 は，全体的に正答率が高かった。本文中に示したデータベースサーバの移設に伴うリスクについて，正しく理解できていることがうかがわれた。

設問 4 は，全体的に正答率が高かった。設問 4(1)では，コンテナ方式だけに該当する確認事項について問うたが，DRM（Digital Rights Management）方式とコンテナ方式の両方に該当してしまう確認事項についての解答が一部に見受けられた。本文をよく読み，解答してほしかった。

問 2

問 2 では，Web サイトのセキュリティガイドラインの整備やセキュリティ診断の内製化を題材に，脆弱性に関する知識，管理方法及び検出方法について出題した。

設問 1(1)，(3)は，正答率が低かった。HTTP メソッドと Web サーバのアクセスログの関係は攻撃の監視・分析において，SSH の認証方式はシステム運用管理において，それぞれ必要となる知識であるので，よく理解しておいてほしい。

設問 2 は，正答率が高かった。脆弱性管理にはソフトウェア構成管理が必要なことについて，受験者の理解が進んでいることがうかがわれる。

設問 4(1)g は，DB に登録されていた全件数である 100 件という解答が散見された。SQL インジェクションが存在する場合にどのような SQL 文が実行されるかを考えて，解答してほしかった。

設問 4(4)k，l は，正答率が低かった。アクセス制御や認可制御の診断方法について，よく理解しておいてほしい。