令和２年度　10 月　情報処理安全確保支援士試験　採点講評

午後Ⅰ試験

問１

問 1 では，スマートフォン用決済アプリケーションプログラムの開発を題材に，メッセージ認証を用いたなりすまし対策及びスクリーニング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(1)“問題”は，正答率がやや低かった。本問で扱うバーコードは，仕様上，決済のなりすましにつながるおそれがある。決済のなりすましが成功してしまう原因と防ぐ手段をよく理解してほしい。

設問 2(2)は，正答率が低かった。サーバ証明書のフィールドと，その検証方法をよく理解してほしい。

設問 3(1)は，正答率がやや高かった一方で，(2)“修正後の処理”の正答率は平均的だった。“修正後の処理”では，登録されているメールアドレスにエラーを通知するといった誤った解答が多かった。スクリーニングを防止するには，会員登録されている場合とされていない場合で表示内容を同じにする必要があることをよく理解してほしい。

問２

問 2 では，電子メールの暗号化を題材に，S/MIME を使った電子メールシステムの設計について出題した。全体として，正答率は平均的であった。

設問 1(2)は，正答率がやや低かった。SSH や FTP といった解答が散見された。OCSP は，X.509 公開鍵証明書の失効状態をタイムリーに確認できるプロトコルである。OCSP の仕組みをよく理解してほしい。

設問 2(1)は，正答率が平均的であった。SMTP over TLS 及び POP3 over TLS によって，通信は暗号されるが，メールサーバ上の電子メールは暗号化されていないということをよく理解してほしい。

設問 2(3)は，正答率が高かった。S/MIME での電子メールの復号の仕様について，よく理解されていた。

問３

問 3 では，EC サイトの脆弱(ぜい)性診断を題材に，診断を受ける企業での診断計画の策定について出題した。全体として，正答率は平均的であった。

設問 1 は，(1)の正答率が高かった。プラットフォーム診断を実施する際のネットワーク型 IPS の基本的な挙動は，よく理解されていた。一方，(3)は正答率が低かった。診断 PC の接続箇所を，管理 LAN にある接続箇所から選択した誤った解答が多かった。表 2 の“診断 1”は，インターネットから本番 Web サーバへの攻撃を想定した診断を内部のネットワークから実施するものであり，管理 LAN からでは適切な診断ができない。脆弱性診断の計画策定においては，どのような脅威を想定したものなのかを念頭に置くことが重要である。

設問 2(1)～(3)は，診断対象システムの業務影響や，既存のセキュリティ機器の運用への影響に関するマネジメントの問題であった。診断において重要であるので，よく理解してほしい。

©2021　独立行政法人情報処理推進機構