

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サイトの脆弱性<sup>ぜい</sup>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。