平成 28 年度　春期　情報セキュリティスペシャリスト試験　採点講評

午後 I 試験

問 1

問 1 では，懸賞システムの開発を題材に，XSS（クロスサイトスクリプティング）脆弱性及び CSRF（クロスサイトリクエストフォージェリ）脆弱性に関する知識と対策方法について出題した。全体として正答率は低かった。

設問 1(4)は，正答率が低かった。図 7 の攻撃用 HTML ではフレームを使用しているものの，反射型 XSS 脆弱性の典型的な攻撃パターンについて理解していれば正答できる問題であった。基本的な XSS 脆弱性の原理についてよく理解しておいてほしい。

設問 3(1)は，正答率が低かった。攻撃者の視点から，ページ遷移に基づく解答を期待したが，Web ブラウザの設定によるスクリプトの無効化に関する解答をした受験者が多かった。

問 2

問 2 では，DMZ 上の機器のセキュリティ設定の点検を題材に，システム管理者に必要となるネットワークセキュリティに関する設計及び運用の知識について出題した。全体として正答率は低かった。

設問 1b は，正答率が低かった。標的型攻撃の多くは偽装した電子メールから開始される。電子メールを悪用した攻撃手法とそれに対する対策について理解を深めてほしい。

設問 3(1)は，正答率が低かった。DNS 名前解決通信では UDP が使われている。UDP の仕組みも理解した上で，DNS サーバのセキュリティ設定を行ってほしい。

設問 4 変更内容では，エンベロープとメールヘッダの違いを理解していない解答が散見された。SMTP の仕組み及び電子メールの構造は，偽装した電子メールへの対策を行う上で基本となるので，よく理解しておいてほしい。

問 3

問 3 では，スマートフォンアプリケーションの試験を題材に，サーバ証明書の検証不備に焦点を当て，検証機能を確認するための試験方法及び試験環境，並びにサーバ証明書の検証不備を用いた中間者攻撃の基礎的な知識及び攻撃環境について出題した。全体として正答率は高かった。

設問 1 は，全体的に正答率は高かったが，(1)と(2)については，S システムの構成とサーバ証明書の検証試験環境の対応を理解していない解答が散見された。

設問 2 は，(1)e と(2)の正答率が低かった。(1)e については，中間者攻撃が成功するサーバ証明書として，プライベート認証局で発行されたサーバ証明書だけを選んだ解答が散見された。サーバ証明書の検証不備の状況によっては，商用認証局が発行したサーバ証明書でも中間者攻撃が成功することを理解しておいてほしい。(2)については，無線 LAN アクセスポイントへの接続の仕組みを理解していない解答が散見された。