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 II 試験

問 1

問 1 では，CSIRT 構築とセキュリティ設計について出題した。

設問 3 は，正答率が低かった。(1)は，運用管理セグメントを新設すれば防げるが，現状の構成では防げない具体的な攻撃のシナリオを問うたが，攻撃のシナリオが不明確なまま OA 用 PC がマルウェアに感染するという状況だけを説明した解答や，運用管理セグメントを新設しても防げない攻撃のシナリオについての解答が散見された。(2)は，リバースブルートフォース攻撃の検知方法を問うたが，A 社の LDAP サーバの運用管理への考慮がない解答や，単にリバースブルートフォース攻撃を説明した解答が散見された。

設問 6 は，正答率が高かった。ファイアウォールに関する脆弱(ぜいじゃく)性を A 社のケースについて評価する設問であったが，CVSS についてよく理解されているようであった。

問 2

問 2 では，モバイル端末のマルウェア感染を題材に，セキュリティインシデント発生時の対応について出題した。全体として正答率は高かった。

設問 1(1)は，正答率が低かった。C&C サーバが，HTTP リクエストヘッダの User-Agent に応じて HTTP ステータスコードを変化させていることを，表 3 と本文から読み取ってほしかった。攻撃の仕組みを理解するためにも，HTTP についてはよく理解しておいてほしい。

設問 2 及び設問 3(1)b は，正答率が低かった。マルウェアをダウンロードさせ実行させる攻撃方法，及び不正なコードを実行するための攻撃方法を理解しておいてほしい。

設問 5(4)は，VDI からクラウドサービスにアクセスする方式をよく理解していない解答が散見された。