平成 26 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，プログラム作成プロセスでの脆弱性の排除について出題した。全体として正答率が低く，理解が不足しているようであった。

設問 1 は，全体として正答率が高かった。Web アプリケーションにおけるクライアントサイドスクリプトの役割とセキュリティ上の限界については，脆弱性を排除するために確実に理解しておく必要がある。

設問 2 は，全体として正答率が低かった。設問 2(2)において，単にファイルサイズに着目した解答が多かったが，攻撃用にヘッダ部を改ざんするなどの特別な作り込みがされたファイルについても考慮することが必要である。

設問 3 は，全体として正答率が低かった。設問に挙げた不等式において，左辺及び右辺それぞれの演算で整数オーバフローが発生する可能性についての考慮が不足した解答が目立った。

問 2

問 2 では，電子メールの情報セキュリティ対策について出題した。全体として正答率は低かった。

設問 1(2)は，正答率が低かった。電子メールにおけるなりすましを拒否してもらうために，SPF(Sender Policy Framework)レコードの設定方法を是非知っておいてほしい。

設問 3(1)は，正答率が高かった。“MX レコードの設定を変更する”というように，IP アドレスとは関係ない設定について述べた解答が散見された。IP アドレス WL が，IP アドレスをマッチングに使うことについて注意して解答してほしい。

設問 3(2)は，正答率が低かった。“送信元の IP アドレスを詐称したパケットを送り込む”といった解答が目立った。しかし，SMTP は TCP 上で動作しているので，事実上，IP アドレスを詐称することはできないことを理解してほしい。

現在のメールシステムは，標的型攻撃の入口対策として重要な役割を果たしている。電子メールに関する情報セキュリティ対策について，理解を深めてほしい。

問 3

問 3 では，マルウェアへのセキュリティ対策について出題した。

設問 1(2)は，正答率が高かった。法人利用者がクライアント証明書による端末認証を実施していることから，利用者 ID とパスワードだけでは，X ネットサービスを利用できないことが，正しく理解されているようであった。しかし，乱数表を使用していないことに言及する解答も多く，設問の趣旨を捉えていない受験者も散見された。落ち着いて問題文を読んで解答してほしい。

設問 3(3)は，正答率が低かった。特に“入力値の改ざん”ではなく，“HMAC 値の改ざん”と誤って解答している受験者が多く，送金内容認証及び HMAC の仕組みについて正しく理解されていないようであった。マルウェアの攻撃手法について正しく理解してほしい。