# 平成 27 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，連休明けの標的型攻撃によるウイルス感染を題材にして，ウイルス対策について出題した。

設問 1(2)の b は，正答率が低かった。オープリゾルバを踏み台にする攻撃事例もあるので，DNS の仕組みと設定をよく理解しておいてほしい。

設問 1(2)の c は，正答率が低かった。不正中継防止を確実に行うために，SMTP の仕組みをよく理解しておいてほしい。

設問 4(2)は，正答率が低かった。パターンマッチングの方式を誤った解答が目立った。パターンマッチングは，URL フィルタリングだけでなく，ログ分析でも使用される。パターンマッチングについて学習しておいてほしい。

設問 4(3)は，ウイルス感染が同報メールによるものであることを理解していない解答が散見された。同報メールによってウイルス感染が発生した場合の，調査及び対処の範囲を理解しておいてほしい。

### 問２

問 2 では，マルウェアの感染方法を想定した上で，LAN の分離，他の組織と接続したネットワークの構築について出題した。全体として，正答率は高かった。

設問 1 及び設問 3 は，LAN を分離した上で安全にデータを送受信する仕組みについて出題した。このような仕組みの設計に当たっては，脅威を洗い出した上で，それらの脅威に直面した場合に情報資産を守れるのかを検討する必要がある。セキュリティ技術者として，日々現れる新しい脅威について理解するとともに，各種の対策が脅威に対して有効かどうか評価する能力を身につけてほしい。

設問 4 は，Web サーバへアクセスする端末の認証に関する問題である。(2)は，PKI の基本とも言える内容である。また，(3)及び(4)では，証明書の有効性検証では，端末がもっている秘密鍵（鍵ペア）の正当性を検証していることを理解していない解答が目立った。これらを理解できていなければ，PKI を応用したシステムを設計することができないので，確実に理解してほしい。