平成 28 年度　秋期　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，暗号技術及び認証技術と，IC カードを利用した利用者認証システムの設計について出題した。

設問 1 は，基礎的な暗号技術及び認証技術について問う問題である。正答率は高かった。

設問 2 は，IC カードと PKI を用いた利用者認証システムの運用設計について問う問題である。設問 2(3)“改善すべき不備”の問いについての正答率は低かった。PKI を利用した利用者認証システムにおいて，利用者証明書の失効情報が遅滞なく開示されることは重要である。このことを再度確認してほしい。

設問 3 は，サーバ証明書の検証について問う問題である。正答率は低かった。サーバ証明書及び TLS は，現時点において不可欠な基盤技術である。本設問で採り上げた事項も含め，サーバ証明書関係技術の特徴及び限界について理解を深めてほしい。

設問 4 は，IC カードを利用した利用者認証システムの設計及び効果について問う問題である。正答率は低かった。各種セキュリティ技術の特徴及び限界をよく理解し，条件・状況に照らして最適なセキュリティ技術及び適用方法を選び，最適なシステムを構築及び運用を設計できる人材になるように努めてほしい。

問 2

問 2 では，bash の脆弱性と，技術面と運用面における脆弱性対策の立案について出題した。

設問 1 は，脆弱性対応の基本的な考え方について問う問題である。正答率は高かった。

設問 2 は，bash の脆弱性に関する問題である。設問 2(4)のフィールド値として指定される文字列の問いについての正答率は低かった。脆弱性を理解する上で，どのようなコマンドがその要因となるかを把握することは重要である。コマンドを読み取る能力を深めてほしい。

設問 3 は，WAF による脆弱性対策について問う問題である。設問 3(3)のクラウド型 WAF の導入方法の問いについての正答率は低かった。外部のセキュリティサービスを利用する場合の設定は基本的な知識であるため，よく理解してほしい。

設問 4 は，脆弱性を悪用した攻撃手法について問う問題である。正答率は低かった。Web サーバに関する技術的な知識を深めるとともに，状況設定を勘案した上で，脆弱性を悪用することによってどのような攻撃手法が可能となるかを推測する能力を深めてほしい。

設問 5 は，運用面を考慮した脆弱性対策について問う問題である。適切な脆弱性対策を維持していくためには，運用面の配慮が不可欠となる。実現可能な対策を立案できる人材になるように努めてほしい。