平成 26 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 I 試験

問 1

問 1 では，運用の観点も含めて，ソフトウエアにおける脆弱性の代表例の一つであるバッファオーバフローについて出題した。全体に正答率は想定以上に低く，バッファオーバフローの仕組みなどの技術について誤解が多く見受けられた。

設問 1 の b と d は，OS におけるセキュリティ技術に関する問題である。プログラミング開発においての知識と併せて，セキュリティに関する知識として再度確認してほしい。

設問 2 は，スタックバッファオーバフロー攻撃を具体的に理解し，説明できる能力を求める問題である。本問のスタックバッファオーバフロー攻撃自体は，バッファオーバフロー攻撃の中でも基本的な例であるが，正確な知識がなければ，解答は困難である。最近の OS のセキュリティ対策技術も，このような知識を前提としていると言えるので，受験者にはこの機会にこれらの知識を確認してほしい。

設問 3 及び設問 4 は，バッファオーバフロー攻撃の仕組みとは別に，潜在的に脆弱性をもつシステムを運用する場面での脅威及びその対処をストーリーに合わせて解答する問題である。脆弱性やその対策に関する技術的知識を前提としており，それらを含めた周辺技術の理解を深めてほしい。

問 2

問 2 では，暗号に関する知識，及び SSL クライアント認証を利用した認証システムの設計について出題した。全体として，正答率は平均的であった。

設問 1(1)及び(2)は，攻撃への耐性の視点から，様々な種類の暗号技術を比較する問題であった。本問の正答率はおおむね想定どおりであった。本問にあるように，攻撃への耐性の視点から，異なった種類の暗号技術を比較評価する方法を理解し，今後活用してほしい。

設問 2(1)は，正答率が若干低かった。端末のディスク内のデータの削除に言及する解答が目立ったが，本問の状況においては，端末に発行された証明書を利用停止させる方法が最も適切である。

設問 3(1)は，正答率が低かった。代理店内に設置されたネットワークの管理に言及する解答が散見されたが，Q システムはインターネット経由でアクセスできるので，代理店内のネットワーク管理で対応できる範囲は限られている。

設問 2 や設問 3 が解答できるように，また，技術一辺倒ではなく，弱点を補う運用や役割分担など，幅広い視点をもって，目標とするセキュリティレベルを達成するシステムの設計を行えるように，理解を深めてほしい。

問 3

問 3 では，マルウェア感染へ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 は，標的型攻撃の入口対策として，メールのフィルタリングルールについて出題した。正答率は高かった。ただし，設問 1(2)は，フィルタリングルールの仕様を正確に記述していない解答も散見された。記載されている機能仕様をよく理解して解答してほしい。

設問 2 は，標的型攻撃の出口対策として，ファイアウォール及びプロキシサーバでの対策について出題した。正答率は高かった。

設問 3 は，マルウェアの感染拡大を抑制するための内部ネットワークでの対策に関して出題した。実際に運用されている事例を理解してほしい。

設問 4 は，パスワードとハッシュの知識について出題した。正答率は低かった。ソルトの使用による効果については，基本的な知識であり，仕組みを含めて理解してほしい。

標的型攻撃対策では，IPA が 2014 年 9 月に“「高度標的型攻撃」対策に向けたシステム設計ガイド”を公開しており，体系的に学習するとともに，実運用にも役立ててほしい。