平成 27 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，ソフトウェアの脆弱性への対応について出題した。

設問 1 は，情報セキュリティの 3 要素とその根拠となる理由を問う問題であったが，3 要素の意味を誤解している解答が散見された。情報セキュリティの 3 要素は，基本的な知識であり，正確に理解してほしい。

設問 2 は，攻撃コードによるアクセスログのファイルをどこに作成するかを表中の字句を用いて解答する問題であり，正答率は高かった。

設問 3(1)は，WAF の設定を攻撃内容から判断して，解答する問題であったが，正答率は低かった。問題文中の全ての攻撃パターンと WAF のルールを比較することで解答できる問題であったが，完全には防御できない組合せの解答が散見された。

設問 4 は，WAF に関する検証内容を問う問題であったが，正答率は高かった。ただし，WAF ではなく修正モジュール適用に関する検証内容を解答した例も散見された。問題文をよく読んで解答してほしい。

WAF の理解を手助けする資料として，IPA が“Web Application Firewall 読本”を公開しているので，学習の参考とともに実運用にも役立ててほしい。

問 2

問 2 では，特権 ID の管理について出題した。

設問 1 は，特権 ID の管理者について問う問題であったが，正答率は高かった。

設問 2(1)は，特権 ID の種類によるモニタリングの可否について問う問題であったが，正答率が低かった。特権 ID の利用状況の違いによって，利用者の特定ができない場合があることを理解してほしい。

設問 3(1)は，特権 ID の利用に関し，委託先に確認すべき事項を問う問題であったが，正答率が低かった。特権 ID を管理するシステムを導入したとしても，不適切な利用を放置すればシステム導入の効果が期待できない。システムによる管理に加えて，人的，組織的な管理策が必要であることを理解してほしい。

特権 ID の管理は，情報漏えいの防止対策として重要な役割を果たしている。特権 ID の管理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，Web サイトでのインシデント対応について出題した。

設問 1 は，サーバの OS のログイン履歴を基に侵入された順番を判断する問題であったが，最初に侵入されたサーバを正しく答えられていない解答が見受けられた。WebAP サーバ 2 は，サーブレットコンテナから侵入されているため，OS のログイン履歴には記録が残らないことを理解してほしい。

設問 2 は，WebAP サーバ 2 のアクセスログを読み解く問題であったが，ベーシック認証の仕組みを正しく理解できていない解答が見受けられた。ベーシック認証のアクセスログ解析においては，ステータスコードに着目してほしい。

設問 4 は，セキュリティインシデントで発生した一連の攻撃を正しく理解できているか，対策の内容を通じて問う問題だったが，設問 4(b)は正答率が低かった。サーブレットコンテナの管理画面から侵入され，OS の自動的なログインという仕様を利用して侵入が拡大したというポイントを理解し，それぞれの原因に対する適切な対策が立案できるようになることを期待したい。