平成 24 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，Web アプリケーションの脆弱性検査の指摘事項への対応策について出題した。全体として正答率は低かった。

設問 2(1)(2)では，攻撃状況をログから解析する場合に，正当なアクセスと不正なアクセスを判別することが困難である具体的な状況を解答してほしかったが，正答率は低かった。特に(2)では，“IP アドレスを詐称した”とする解答が多かったが，本問での状況では IP アドレスの詐称は起き得ないことに気づいてほしかった。

設問 3(2)は，正答率が低かった。エスケープ処理はいつも同じようにすればよいものではなく，プログラムが満たすべき要件や，出力が渡される処理系によって，適切に処理しなければならない。エスケープ処理の本質をよく理解しておいてほしい。

問 2

問 2 では，Web アプリケーションに対する SQL インジェクション攻撃を受けた際のログ分析と，DB に格納されているパスワード情報を題材に，Web アプリケーションにおけるインシデント対応と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(1)は，正答率が低かった。表 1 のログを注意深く確認することで，窃取されていた会員 ID（cust_id）とパスワード（pwd）を select している ipH を選択できたはずである。(2)(3)は正答率が高く，不正ログイン試行とその対策であるアカウントロックに対する理解は進んでいると思われる。

設問 2(1)の中で g（選択平文）については正答率が著しく低かった。基本用語については理解を確実にしておいてほしい。(2)も正答率が低かった。利用者は複数のサイトで同じ認証情報の組合せを使い回している場合が多い。二次被害拡大防止のためにも利用者にとって必要なアクションが取れるような通知を心がけてほしい。

設問 3(1)は，外部サイトに誘導される場合にブラウザやそのプラグインの脆弱性を突かれるケースを題材にした。企業や組織内で頻発している事象であるので，誘導からマルウェアの感染とその後の活動までの仕組みを理解しておいてほしい。

問 3

問 3 では，委託先作業担当者の操作内容の証跡確保を題材として，操作ログを取得するパッケージソフトのセキュリティ上の考慮点について出題した。

設問 3(3)は，正答率が低かった。Z 社の作業担当者が保険サーバで行う不正な行為に関して，案 1 の機能を用いた検知手段を問う問題であったが，“M 社の従業員が操作ログをリアルタイムに監視する”といった，案 1 の機能とは全く関係のない検知手段を述べる解答が多かった。一般的な知見での解答ではなく，本文の記載内容に基づいて解答してほしかった。

設問 4(2)は，作業計画書に記載された作業担当者だけが特権 ID を利用できるようにするための制御を問う問題であったが，“適切な特権管理を行う”といった曖昧な内容の解答が散見された。案 2 を採用した後のシステム構成や保守作業時の運用を理解した上で，操作ログの取得と同様に中継サーバで制御する機能として，表 1 に示される PP2 の機能“利用者ごとのリモートアクセスの許可と拒否の制御”に気がついてほしかった。

問 4

問 4 では，標的型攻撃に関して出題した。この問で取り上げている標的型攻撃に遭遇した場合，設問 1 から 4 の全てにおいて，ウイルス対策ソフトが本来の機能を発揮できない場合があることを理解した上での解答を期待したが，その点の理解が不足している解答が目立った。

設問 2 は，TCP セッションのパケットキャプチャを出発点として未知のウイルスの解析を行う場合を例にとり，常駐してしまったウイルスの検出方法について出題した。この場合は，TCP ポート番号が大きな手がかりになるという点を理解してほしかったが，正答率は低かった。

設問 3 は，未知のウイルスに感染しているかもしれないという状況下で必要なデータファイルを確保する作業の方法について出題した。既知であれ未知であれウイルスの感染が疑われる OS 環境では，その OS を起動してはいけないことを踏まえた解答を期待したが，正答率は低かった。