平成 23 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，Web アプリケーションのセキュアプログラミングに関して，C++と Java での脆弱性対策の共通点と相違点を正しく認識しているかどうか出題した。全体として正答率は想定どおりだった。

設問 1 のコード上から変数名を選択する問題では，(1)は比較対象もあり正答率は高かったが，(6)は正答率は低かった。(4)は代表的な脆弱性を解答群から選択する問題で正答率は高かったが，“コマンドインジェクション”という誤った解答が多かった。設問 1 の中ではプログラミング技法について複数出題したが，開発標準に関する経験が少ないためか，正確に記述できているものが少なかった。

設問 2 では，二つの言語の特性を表す用語を答える問題だったが，(1)～(3)全て正答率は高かった。

設問 3 では，二つの言語を比較してバッファオーバフロー攻撃が可能になる言語特性を問うたが，問題文を丁寧に読んでいないのか，単純なバッファオーバフローの範囲までの解答が多く，正答率が低かった。

セキュアプログラミングについて，脆弱性対策の手段だけではなく，その発生理由や防御メカニズムも含めて，正確な情報を理解して，活用できるようにしてほしい。

問 2

問 2 では，開発プロジェクトの設計工程における，セキュリティの観点から行うレビューについて出題した。全体として正答率は想定どおりだった。

設問 2 は全体的に正答率が高かった。利用者 ID の状態を意識してログイン処理のフローを設計することは，システムのセキュリティを確保するためにも重要であり，実務においても確実にできることを期待したい。

設問 3 は正答率がやや低かった。現行システムの設計や運用手順を十分に理解しないままシステムに不用意な機能追加を行うと，セキュリティ上の問題が発生する可能性があること，及びそういったセキュリティ上の問題を発見するための組織的なレビューが重要であることを再認識してほしい。

設問 4 は正答率が低かった。問題文中に記載されたシステムの変更点だけを書いている解答が散見された。状況設定を理解した上で，仮パスワードを知り得るのが誰であるのかに注目して解答してほしかった。

問 3

問 3 では，HTTPS 通信時におけるプロキシでのログ取得を題材として，HTTPS 通信時の動作及び証明書の検証について出題した。全体として正答率は低かった。

設問 1 は(3)の正答率が低かった。昨今のインターネットの利用形態の多くが HTTP プロトコルをベースとしている状況を踏まえ，情報セキュリティ技術者としても HTTP プロトコルの基本的な仕様は是非理解しておいてほしい。

設問 2 は(2)の正答率が低かった。証明書に関する確認事項として，有効期限や CRL の確認を挙げる受験者が多く見られたが，想定する脅威に対してそれぞれの確認事項がどの程度有効であるのかを意識して解答してほしかった。

設問 3 は全体的に正答率が低かった。暗号化された通信路が二つ存在するという応用的な問題ではあったが，HTTPS 通信時の処理の流れを理解していれば解ける問題である。重要なところなので HTTPS 通信の基礎を理解してほしい。

問 4

問 4 では，内部統制を題材に，情報セキュリティマネジメントの基本知識及び外部サービス利用時の情報セキュリティの確保について出題した。全体として正答率は想定どおりだった。

設問 1 及び設問 2 は穴埋め問題であり，高い正答率を期待したが，設問 2c 以外は正答率が低かった。これらの用語や内容は，情報セキュリティに関する基本的な知識であり，しっかりと理解してほしい。また，設問 2e は，誤って“破棄や管理”と解答した受験者が多かった。クリアデスクの意味を考えてほしい。

設問 3 では，(1)，(2)は正答率が高かったが，(3)は正答率が低かった。管理的対策としてどのような対策が効果的かを考えて解答してほしかった。

設問 4 では，(1)は正答率が高かったが，(2)は低かった。統制状況に関する報告書では，利用者 ID の登録に関してどのような項目の記述が必要かを理解して解答してほしかったが，不十分な解答が多かった。