平成 21 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，社内ネットワークから発信される攻撃に対して，踏み台となっている PC や DNS サーバの不備を，ネットワークモニタを使って突き止める手法について出題した。全体として正答率はやや低かった。

設問 1(4)は，正答率が低かった。企業の DNS サーバにおいて，本来応答する必要のない外部ホストからの外部アドレスの問合せを許していると，DNS Reflection 攻撃の踏み台に悪用されるおそれがある。“ 修正 ” についての解答には，問合せ元と問合せ対象の両者を含めてほしかった。DNS サーバには，そのプロトコル上の性質から様々な脆弱性が指摘されており，設定には細心の注意が必要であることを理解してほしい。

設問 2(1)では，パケットモニタの状況から異常を読み取る能力を問うている。正しい通信手順とマルウェアの通信パターンの差異についての理解を求めているが，“ パケット量が多い ” などのあいまいな解答が散見された。

設問 3(2)は，マルウェアが hosts ファイルを改ざんして，ウイルス対策ソフトのアップデート機能を無効にすることで，PC に現れる異常について考える問いであった。マルウェアは自身の発見を逃れるために，様々な設定を改ざんするが，パケットの送信状況を外部からモニタすることで異常を検知できる場合があることを理解しておいてほしい。

問 2

問 2 では，Web サーバプログラムの脆弱性対策について出題した。全体として正答率は想定どおりだった。

設問 1 は，正答率がやや低かった。(2)では，攻撃が成功する可能性や，攻撃が成功した場合の被害の大きさを解答した誤答が散見された。攻撃が試みられる可能性が高いことと，その攻撃が成功する可能性が高いことは，それぞれ別の特性であることを考えて解答してほしかった。

設問 2 は，正答率が低かった。特に(2)は正答率が著しく低く，その中でも，“ クエリストリングは暗号化されない ” という誤った解答が目立った。今後も Web アプリケーションの利用は増加すると思われるので，HTTPS において暗号化される範囲と GET，POST メソッドの動作の違いについて，確実に理解しておいてほしい。

設問 3 は，正答率が高かった。修正プログラムは日々提供されるものだが，修正プログラムそのものに起因してトラブルが発生する可能性について考えた上で適用作業を実施する必要があることは，おおむね理解できていた。

問 3

問 3 では，Web アプリケーション開発時の脆弱性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)では，どのような方法で他人になりすますかを問うたが，“ cookie の値が容易に書き換えられるから ” のように原因だけを述べ，方法が明示されていない解答が多かった。また，クロスサイトスクリプティング対策を問うた(3)は，正答率が低かった。<>& ”’ などの HTML 構造に影響を与える文字を適切に置換しても，出力される箇所によってはスクリプトが動作してしまうことを理解しておいてほしい。

設問 2 は，全体的に正答率が高かった。透過的データ暗号化機能によるリスク対策や，Web アプリケーションで管理される利用者のパスワード情報の保護については，適切に理解されているものと推察できる。

問 4

問 4 では，特権 ID 管理の重要性と課題，及びその改善方法について出題した。全体として，正答率は低かった。

設問 1(1)は，選択肢からの解答であったにもかかわらず正答率が低かった。セキュリティの関連技術と同様に，セキュリティの関連法規についても世の中の動向を知っておいてもらいたい。

設問 2(3)は，正答率が低かった。特に，ログサーバ内のログに対してアクセス権を設定することだけを記述した解答が多かった。特権 ID は，システムに対して強力な権限をもった ID であるので，その管理を改善する際には，システム設定などの技術的側面だけでなく，使用者の範囲や使用手続など，運用に関する部分も含めて検討する必要があることを理解しておいてほしい。