平成 28 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，組込み機器を利用したシステムのセキュリティ対策について出題した。

設問 2(2)は，パスワード強度に依存しない SSH のログイン認証方式について問う問題である。正答率は低かった。辞書攻撃への対策には，公開鍵認証を有効にすることに加えて，パスワード認証を無効化する設定が必要であるということを理解してほしい。

設問 3(2)は，SSH のホスト鍵が組込み機器の同一モデルで全て同じである場合に，同じホスト鍵を使ってどのような攻撃が行われるかについて問う問題である。ホスト鍵は，SSH サーバの真正性を担保するものであるが，その目的を理解していない解答が多く見受けられた。同一のホスト鍵が使われた場合，SSH サーバのなりすましに気付くことができないので，中間者攻撃による通信内容の盗聴や改ざんが行われてしまうということを理解してほしい。

設問 3(4)は，イメージファイルを復号するための鍵を，攻撃者がどのように入手するかについて問う問題である。平文の状態の鍵を探すといった攻撃側の視点を踏まえて対策が立案できるようになることを期待したい。

問 2

問 2 では，ソフトウェアの脆弱性，特に，バッファオーバフロー（以下，BOF という）脆弱性の対策について出題した。

設問 2(1)は，C / C++での関数呼出し時のスタックの状況に関する問題である。正答率は低かった。いわゆる攻撃ベクタの一つなので，基本的な知識として確認をしてほしい。

設問 3(3)は，ヒープベース BOF 脆弱性を悪用する攻撃を引き起こすコードの改修に関する問題である。正答率は低かった。この問題では，プログラムの引数は仕様でサイズの上限が定義されており，この上限を利用することによってオーバフローを防ぐ。受験者には，この観点で正しい改修に気が付いてほしかった。

設問 4 は，いずれも，BOF 脆弱性を悪用する攻撃とその対策技術の有効範囲を問う問題である。正答率は低かった。今回のヒープベース BOF 脆弱性を悪用する攻撃は，常に成功するものではなく，このケースでは OS に依存することを問うている。データ実行防止機能は，スタックベース BOF 脆弱性の対策技術であり，ヒープベース BOF 脆弱性には効果がない。セキュリティ技術者としては，これらの知識は身に付けておいてほしい。

問 3

問 3 では，プロキシサーバを用いたマルウェア対策について出題した。

設問 3(1)は，プロキシサーバのログに関する問題である。正答率は低かった。ログから送信元 PC を特定できない理由について，他者に誤解なく伝わるように，必要な情報を正確に記述してほしかった。

設問 3(2)は，プロキシサーバが処理する HTTP ヘッダに関する問題である。正答率は低かった。広く使われている HTTP プロトコルについての知識を深めてほしい。

設問 4(1)は，プロキシサーバの認証機能を通過する最新のマルウェアに関する問題である。正答率は低かった。認証機能を通過する仕組みについて，他者に誤解なく伝わるように，必要な情報を正確に記述してほしかった。