平成 19 年度　春期　テクニカルエンジニア（情報セキュリティ）試験　採点講評

午後 I 試験

問1

問 1 では，C++言語におけるセキュアプログラミングについて出題した。全体として，正答率は低かった。

設問 1 では，d の正答率が低かった。バッファオーバフローが起きると，権限昇格やシェルコードの実行などが起こり得ることを十分に認識してもらいたい。

設問 2 では，バッファオーバフローの発生の仕組みが理解できていないと思われる解答が散見された。特に(2)で，afile の内容の表示についてだけ記述した解答が多かった。コマンドライン引数を変更すれば，任意のファイルの内容を表示できることに気づいてほしかった。

設問 3 も正答率が低かった。セキュアプログラミングだけでなく，コンパイラや実行環境による検知と防止機能を併せて使用することによって，バッファオーバフローに対する多層防御が図れることを理解してほしい。

問2

問 2 では，ネットワークのセキュリティについて出題した。全体として，正答率は高かった。

設問 2(3)は，正答率が低かった。“ウイルスによる攻撃”という解答があったが，本文中の下線②にある“インターネットからの不正なアクセス”とはいえない。DMZ 上のサーバは攻撃を受けやすく，管理者権限を奪われて社内 LAN が攻撃されるリスクがあることを認識してもらいたい。

設問 3(2)では，“フォールスポジティブ”と“フォールスネガティブ”を取り違えている解答が見られた。それぞれの特徴を把握して，正確に理解しておいてほしい。

設問 3(4)では，IDS が FW と連携する機能として，TCP のリセットパケットの送出や FW のフィルタリングルールの動的な追加などに気づいてほしかった。FW との連携における問題点ではなく，IDS や FW 単独の問題点を指摘した誤った解答も見受けられた。また，単に“タイムラグがある”というだけではなく，タイムラグがあることによってどのようなリスクが発生するのか，まで解答に含めてほしかった。

問3

問 3 では，採取するログ情報の証拠能力に関わるセキュリティ技術について出題した。全体として，正答率は低かった。

設問 1 は，正答率が低かった。パスワード攻撃は現実にも多く発生しており，想定される脅威や，類推されにくいパスワードにするための手段に関する基礎知識をもってほしい。

設問 2(1)では，“イベントを記録する”のように監査ログの機能を記述した解答が多かった。“記録されたイベントによって発生した事実を確認できる”ことが監査ログの役割であり，目的である。技術を理解するだけでなく，対象業務システムにおいて，その技術が何のために必要であるか，どのような効果を業務システムにもたらすかを理解することが求められる。

設問 3 も，正答率が低かった。時刻の保証が，その時点での情報の存在証明になるという基本原理を理解しておいてほしい。

問4

問 4 では，社内のアンケートシステムにおける暗号方式について出題した。全体として，正答率は低かった。

設問 1(2)では，“線形攻撃を行う”といった誤った解答が見られた。対象業務の特性を正しく把握した上で，暗号技術を適切に利用することを理解してほしい。

設問 2(2)は，“各回答者しか知り得ない”，“署名が偽造できない”のどちらか一方だけを記述している解答が多かった。また，“本人しかアンケートファイルを開けないので”という解答が多かったが，自分のアンケートファイルから得られる情報を基に，他人のアンケートファイルを偽造する攻撃を防止する必要性があることを理解してほしかった。