平成 20 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，社内ネットワークにおけるボット感染端末への対応について出題した。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。図 2 の迷惑メールのヘッダ情報の Received: from に記載される IP アドレス（下線（ii））は，by で示される V 社の smtp01.v-sya.co.jp によって記録されるので，送信者側で詐称することはできない。迷惑メールの送受信が疑われる場面において，そのヘッダ情報を読み解く能力は重要である。

設問 3(2)において，ボットは外部の指令サーバから様々なコマンドやコードを受け取る特徴がある。ウイルス対策ソフトによる検知を難しくする仕組みとして，既存のファイル感染型のウイルスやネットワーク感染型のワームには見られない新たな脅威である，コードの更新までを解答に含めてほしかった。

設問 3(3)では，既存のウイルスに見られる，ファイルを不可視化する設定やログの改ざんによる隠ぺいについての解答が多かった。rootkit には，API のフックや OS コマンドの入替えによって自身のこん跡を隠す特徴があることを理解しておいてほしい。

問 2

問 2 では，SYN Flood 攻撃の仕組みとその対策について出題した。全体として，正答率は高かった。

設問 1 では，c，d の正答率が低かった。TCP の接続確立手順や，これを悪用する SYN Flood 攻撃の仕組みを，正確に理解していないと思われる解答が散見された。

設問 2 では，(1)の正答率が低かった。ハーフオープン状態が維持されるために，メモリなどの資源が使用され，ついには，正当な接続要求に応答できなくなることを理解しておいてほしい。

設問 3 は，SYN Flood 攻撃の対策方法について問うたが，正答率は低かった。特に，何のタイムアウト時間を短くするのかが明記されていない解答が散見された。ルータや Web サーバで対策を併用することで，より効果が上がることを理解しておいてほしい。

問 3

問 3 では，通信データの保護について出題した。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。(1)では，光回線を切断することを明示しない解答が多かった。また，“スイッチのミラーポートを利用する”など，光回線の状態監視では検知できない方法を記述した解答が見受けられた。(2)では，光回線の場合でも可能な方法を記述した解答が見受けられた。いずれも，設問で問われている下線①，下線②の内容を十分に理解していなかったことによるものと思われる。光回線においては，切断検知によって新たな不正機器の接続を検知できること，電気ケーブルを用いた通信回線と比較して漏えい電磁波による盗聴リスクが小さいことを理解しておいてほしい。

設問 2 では，(2)の c と d の両方を正しく解答できている受験者は少なかった。また，(3)ウの正答率が低かった。取引先の構内ネットワークに関する制約（C 社データセンタと同程度のセキュリティ対策の実施を求めることができないこと）を考慮していなかったと思われる。方式選択においては，システム全体の要件と制約を踏まえた判断が必要であることを理解しておいてほしい。

問 4

問 4 では，ISMS 構築時のリスクマネジメントについて出題した。全体として，正答率は高かった。

設問 3 は，正答率が低かった。不正書出しを防ぐ方法を具体的に記述していない解答が多かった。リスクに対する管理策について，技術的にはどのようにすれば実現できるのかを把握しておいてほしい。

設問 4(2)では，“類推しやすいパスワードの禁止”など，OS に設定できない項目を挙げた解答が見られた。利用者に対する推奨項目と OS に設定できる項目は必ずしも一致しないことを認識してほしかった。

設問 4(3)は，正答率が低かった。同じパスワードであってもソルトが異なるとハッシュ値が異なるので，攻撃者は，ソルトごとにハッシュ値のテーブルを作成しなければならなくなり，これによって攻撃を受けにくくすることができることを理解しておいてほしい。