平成 25 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Ⅱ試験

問 1

問 1 では，マルウェア感染事例を題材に，調査と調査結果に基づく対策立案について出題した。本問では，事実を正確に把握した解答を求めており，問題文中に記載された各事象を時系列で整理することを期待した。問全体としての正答率は高かったが，解答内容から，マルウェア感染事例やその調査手法における，受験者の具体的な知識や経験の差が感じられた。

設問 1(2)は，正答率が低かった。マルウェア P について解答した受験者が多かったが，本設問で問うている時点では，マルウェア P 自体は検出・駆除済であることを把握してほしかった。

設問 4(3)は，正答率が低かった。プロキシサーバでの認証機能を用いる対策は，IPA が公開している“『標的型メール攻撃』対策に向けたシステム設計ガイド”内でも述べられている対策である。問題文中では，対策が万全ではない場合があることを記載しているが，実際のマルウェア対策を検討する上でも，各認証方式の違い，プロキシ製品や UTM 製品における認証機能の実装の違い，また対策が有効なマルウェアの範囲についても理解して検討を進めてほしい。

問 2

問 2 では，会社貸与のモバイル PC を利用した既存のリモートアクセス環境を拡張し，個人所有のスマートフォンを利用したリモートアクセス環境を構築する際の設計について出題した。実務経験をもつ受験者にとっては，正解を導きやすい問題であったと思われる。

設問 1(1)では，D 社が認めていないアクセスを正しく識別できているのに，それを防ぐ対策を正確に記述できていない解答が多かった。ファイアウォールのルールから，モバイル PC とスマートフォンという二つの用途ごとに通信経路を分離する必要があることを導き出してほしかったが，どちらか一方の記述にとどまっている解答が多かった。また，ファイアウォールのルールとして，問題文中に記載されている Web メールサーバ及び VPN に関する条件を十分に理解していないと思われる解答も多かった。問題解決においては，対策が，与えられた条件を満たしているか，論理的な観点から検証する必要があることに注意してほしい。

設問 2(1)は，正答率が低かった。製品 E，携帯電話事業者のサービスのそれぞれでのデータ消去に必要な条件の違いから，製品 E でないとデータ消去が行えない二つの条件を導き出してほしかったが，一方の条件の記述にとどまっている解答や，条件を正確に記述できていない解答が多かった。解答においては，与えられた条件を理解し，論理的に考えて解答を記述してほしい。

設問 2(2)は，正答率が低かった。問題文中に記載されている条件から，原因となるスマートフォンの仕様を識別してほしかったが，原因となる仕様を，正しく識別できていない又は正確に記載できていない解答が多かった。要件や制約を抽出及び整理し，正確に記述する必要があることを再認識してほしい。