平成 22 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，セキュアプログラミングの分野から，主にレースコンディションの発生の仕組みと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 2(2)は，正答率が低かった。レースコンディションという用語は，脆弱性を理解，説明する上で必須であるので確実に理解してほしい。また，設問 2(4)も正答率が低かった。レースコンディションの有無をテストするためには，“多数の”リクエストを“同時に”発行するというテスト方法が必須であることを理解しておいてほしい。

設問 3 は，URL 推測に関して出題したが正答率は高かった。URL 推測に対する対策は Web サイト構築において必須の事項であり，確実に対策を行うことを期待したい。

問 2

問 2 では，PC に保存するデータの暗号化と，暗号化したデータをバックアップする際に検討すべき点について出題した。全体として正答率は想定どおりだった。

設問 1 では，暗号化の基本的な仕組みを出題した(1)は，正答率が高かったが，TPM に関して出題した(2)は，選択肢形式であるにもかかわらず正答率が低かった。TPM が搭載されている PC も多くなっているので，TPM の基本的な機能は理解しておいてほしい。

設問 2 は，正答率は高かった。バックアップに限らず，何らかの対策を検討する際には，その対策を導入することで新たなリスクが生じないか確認する必要性について認識しておいてほしい。

設問 3 は，正答率は低かった。暗号化データのバックアップを検討する際には，バックアップデータの確実なリストアと，安全な保管を実現するために，データ保存形式と，鍵管理方法の理解が必要となってくる。代表的な暗号化アプリケーションについてはどのような対策が必要かを是非理解しておいてほしい。

問 3

問 3 では，個人情報保護に関連して，企業間で情報を安全に受け渡す方法について出題した。全体として正答率は想定どおりだった。

設問 1(3)は，正答率が低かった。証明書の真正性を確認するため，紙媒体や電話など，フィンガプリントのオフラインでの入手方法について解答してほしかったが，機密性に着目してしまい，暗号化を挙げた解答が多かった。

設問 2(1)も，正答率が低かった。登記事項証明書の所在地に実在する企業からの申込みであることを確認できる点を解答してほしかったが，“メールで送信すると盗聴のおそれがある”など，ほかの方法の欠点だけを述べた解答が散見された。(2)は，正答率が高かった。初期パスワードを推定されないようにするために，ランダムな文字列や乱数を含めるべきであるということは，よく理解されていた。

問 4

問 4 では，新種のウイルスに感染した場合の駆除手順や再感染防止策の立案について出題した。全体として正答率は想定どおりだった。

設問 2 の a 及び c は，正答率が低かった。モニタポートのない L2SW に接続したパケットモニタで感染 PC を特定するためには，ブロードキャストパケットを監視しなければならないことに気づいてほしかった。

設問 4(1)は，正答率は低かった。X ウイルスの感染方法から，同一ネットワーク上に感染 PC がある場合に，感染する可能性があることに注目して，解答してほしかった。