平成 29 年度　秋期　情報処理安全確保支援士試験　採点講評

午後 II 試験

問 1

問 1 では，クラウドサービスと IoT を組み合せたシステムを題材に，セキュリティについての検査と対策立案について出題した。

設問 1(1)及び設問 2(1)は，いずれも知識問題であり，正答率が高かった。情報セキュリティに関する一般的な用語については，受験者の知識が高いことがうかがえる。

設問 1(2)は，TCP/IP の 3 ウェイハンドシェークについての知識を問う問題であるが，特に“閉じている場合”について，正答率が低かった。サイバー攻撃に関するインシデント対応やセキュリティ検査においては，ネットワークの知識は重要である。基本的な事項は理解しておいてほしい。

設問 2(3)は，正答率が低かった。セキュリティ検査では，検査の目的に応じて，手法とテスト環境を検討し選択することが必要である。

設問 3(1)は，正答率が低かった。クラウドの利用拡大によって，クラウドにアクセスする端末が増える一方で，不正アクセス対策の重要度が増している。利用者認証だけでなく，端末を認証する方法についても理解を深めてほしい。

問 2

問 2 では，DBMS とハードウェアセキュリティモジュール（以下，HSM という）を用いたシステムを題材に，データ暗号化の設計について出題した。

設問 1(1)は，知識問題であるが，正答率が低かった。業界ごとの代表的なセキュリティ基準，データ暗号化に関する基準は，セキュリティ要件を定義する際に参照すべきものであり，代表的なものについては知識をもっておいてほしい。設問 1(2)及び設問 1(3)は，正答率が高かった。多くの受験者が，比較的簡単な前提条件に基づいて，リスクを特定したり数値化したりする能力をもっていることがうかがえる。

設問 2 は，HSM に関する知識問題であるが，(5)を除いて正答率があまり高くなかった。HSM は，データ暗号化に用いられる鍵を安全に管理する技術である。基本的な知識をもっておいてほしい。

設問 3(1)は，DBMS の暗号化機能，HSM，及び HSM をネットワーク経由で利用するためのソフトウェアの 3 種類の構成要素を組み合わせたデータ暗号化の設計に関する設問であるが，正答率が低かった。鍵を安全に保護した上でデータを暗号化する仕組みについての理解を深めてほしい。また，設問文で求められている解答形式から大きく逸脱した解答が多かった。他者と協力して業務を行う技術者は，問いと解答形式を正しく理解し，求められている解答を的確に表現できるよう基本的なコミュニケーション能力を身につけてほしい。

設問 4 は，セキュリティ対策後の残留リスクに関する設問であるが，正答率が低かった。セキュリティ対策の設計において，対策後の残留リスクを正しく分析する能力を身につけてほしい。