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 II 試験

問 1

問 1 では，Web アプリケーションの脆弱性対策と不正アクセスに対するインシデント対応について出題した。全体として，正答率は高かった。

設問 1(1)a は，正答率が低かった。情報システムのアクセス制御に関する設計，実装をする際は，認証と認可の違いを理解しておいてほしい。

設問 2 は，全体的に正答率は高かったが，DB 側による SQL インジェクション対策に関する(4)では，単に DB 管理 TBL への参照権のはく奪や DB ログの取得のような解答が散見された。プログラムの修正漏れなどによって不正アクセスが発生する場合もあるので，DB 側の対策についても是非理解しておいてほしい。

設問 3(3)は，“ログの取得”や“不正アクセスを遮断するための装置（IPS）の導入”など，部分的な対策にとどまる解答が多かった。部分的な対策だけでは不正アクセスを防ぐことはできないことを知っておいてほしい。また，不正アクセスに限らずインシデント対応は，担当する技術者だけでなく，関係者全員が迅速かつ正確に対応ができなくてはならないことを理解しておいてほしい。

問 2

問 2 では，認証システムの企画・設計について出題した。全体として，正答率は高かった。

設問 2(3)では，SSO の特性には言及せずに，単に二要素認証のメリットを挙げたものや，二要素認証で防げるリスクだけを記述した解答が散見された。SSO 化されたすべてのシステム上では同一の認証情報が利用されることに留意して解答してほしかった。

設問 4(2)では不正なアクセスポイントに起因するリスクについての解答を期待していたが，認証情報に関するリスクだけに着目した解答が目立った。近年，無線 LAN はセキュリティ面での改善が進み，利便性との両立が図られるようになっている。利用の範囲も拡大しているので，最新の動向を踏まえつつ理解を深めることが望まれる。

設問 5(1)では共通認証システムを導入する目的を問うたが，目的そのものではなく，“認証情報やアカウントの一元管理”“システムの統合”“SSO の導入”といった具体的な要件を挙げた解答が多かった。RFP では，システムを導入する理由や目的を提案者に対して正しく伝えることが重要である。実務においても，セキュリティ上の要件や機能は業務上の目的を達成するための手段であるという視点を常に忘れないようにしてほしい。