平成 29 年度　春期　情報処理安全確保支援士試験　採点講評

午後 I 試験

問 1

問 1 では，ARP ポイズニングを題材に，通信の盗聴とその対策方法について出題した。

設問 1(1)は a が b，c と比較して正答率が低かった。他セグメントとの通信を盗聴される場合，ゲートウェイとの間の通信が攻撃者に中継されてしまうことを理解し，ARP の仕組みを理解していれば正答できる問題であった。ARP テーブルがどのように改ざんされると盗聴が成立するのか，理解しておいてほしい。

設問 2 は正答率が低かった。中間者攻撃によって，通信を経路の途中で一度復号し，再度暗号化するという形で中継されると，暗号化通信を利用していても通信内容を盗聴され得る。そのような攻撃を防ぐためには，サーバ証明書検証などの手段で通信相手の真正性を確認する必要があることを理解しておいてほしい。

設問 3(1)は正答率が高かった。ネットワークセグメントを分離したことによって，対象通信が PC セグメントを通過しなくなり，盗聴を防げるようになることが良く理解されているようであった。

問 2

問 2 では，Web サイトにおける脆弱(ぜい)性を題材に，脆弱性に関する知識とその対策方法について出題した。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。ログイン記録が取得する情報から何を L 氏に確認すればよいかが分かれば正答できる問題であった。不正ログインされていないことを結論づけるために，何と何の値が一致していることが確認できればよいかを本文中から読み取ってほしかった。

設問 2(3)d は，パスワード変更画面で現在のパスワードを入力させることがなぜ CSRF（クロスサイトリクエストフォージェリ）の対策になるかを理解していれば正答できる問題であった。CSRF の対策についてよく理解しておいてほしい。

設問 3(3)は，正答率が低かった。利用者が一部の HTML の要素の入力を許可されているという仕様を考慮した対策を期待したが，エスケープ処理を行うなどの一般的な XSS（クロスサイトスクリプティング）の対策を解答した受験者が多かった。アプリケーションソフトウェアの仕様によっては，一般的な対策が必ずしも適切な対策とはならないことを理解しておいてほしい。

問 3

問 3 では，クラウドサービスに対する認証連携を題材に，SAML を用いた認証連携と，その仕組みを利用したアクセス制御の方法について出題した。全体として正答率は高かった。

設問 1 は正答率が高かった。クラウドサービス側に記録されるログイン記録について，よく理解されているようであった。

設問 2 は全体的に正答率が高かった。ただし，設問 2(5)については，IdP と SP が直接通信できない点を考慮していない解答が散見された。SAML では IdP と SP 間での認証情報の連携方式が複数存在し，本文中に記載した通信内容は一例である。今回の方式だけでなく，SAML の認証連携の仕組みを広く理解しておいてほしい。

設問 3 は正答率が低かった。特に交通費精算サービスへのログインに失敗する理由については，IdP と LDAP サーバの役割を混同した解答が一部に見られた。SAML における各主体の役割を理解しておいてほしい。