平成 22 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 I 試験

問 1

問 1 では，セキュリティと費用のバランスをとった複数企業とのデータ伝送のセキュリティ設計について出題した。全体として正答率は低かった。

設問 3(2)は，正答率が低かった。作業報告書には運用担当者と保守担当者の氏名が記載され，個人が特定可能であるのに対して，通信ログに記録される運用担当者の利用者 ID 及び保守担当者の利用者 ID は，共用されているので，作業報告書と通信ログの突合せにおいて，個人が特定できないという点に気づいてほしかった。システムの運用・保守において利用者 ID を共用すると，特権の悪用が容易になり，かつ，インシデントが発生した場合の追跡調査が困難になってしまうことを再認識してほしい。

設問 4 は，正答率が低かった。クライアント PC が，案 1 では Z 社から各 SI ベンダに貸与される専用 PC であるのに対して，案 2 では各 SI ベンダが所有するベンダ PC を利用する点が大きく異なることに気づいてほしかった。企業間接続においては，各企業の管理範囲を明確にした上で，各社間のセキュリティポリシの整合性を確認する必要があることに注意してほしい。

問 2

問 2 では，複数の社内システムの ID 統合を題材として，ID のライフサイクル管理を出題した。全体として正答率は想定どおりだった。

設問 2 は，状況設定を理解した上で，契約が終了した派遣社員の ID を確実に削除するための工夫を問うたが，設問 2(3)の正答率は低かった。現場任せでは ID 削除が進まないという状況設定にもかかわらず，現場に任せるという誤った解答が散見された。問題文をよく読み，状況設定に注意して，実務的に解答をしてほしい。

設問 3 は，状況設定からセキュリティホールを探す問いだった。多くの受験者が正答には近かったが，解答すべきポイントを一部省略してしまった解答が見受けられた。必要条件を漏らさず解答するよう心がけてほしい。

設問 4 は，設問 3 のセキュリティホールを回避する具体的な手続を問うた。あいまいな表現や，その手続によって達成したい目的の記述が散見された。情報セキュリティスペシャリストの重要な役割は，セキュリティ対策を具体的に検討し実施することなので，実践的な対策を解答してほしい。

問 3

問 3 では，Web アプリケーションの保護のために，Web アプリケーションファイアウォール（WAF）を導入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低かった。

設問 3(1)は，正答率が低かった。悪意のある第三者が，ミドルウェアが発行するセッション ID を推定できた場合にも，WAF によって暗号化された後の値を推定することは困難である点に注目して解答してほしかった。

設問 3(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。クッキーへの不適切な属性付与によるセキュリティ事故を防止するためにも，クッキーについての基本的な知識を理解しておいてほしい。

設問 4 は，正答率が低かった。問題文中のネットワーク構成では，ブラウザと Web サーバ間で通信が SSL 暗号化されていると，シグネチャによる通信検査機能など WAF の機能が有効に動作しない点に気づいてほしかった。

問 4

問 4 では，マルウェア対策において，攻撃の特徴を踏まえた被害範囲の調査方法や再発防止策について出題した。全体として正答率は高かった。

設問 3(1)は，正答率が低かった。状況設定を理解して，被害があった顧客の範囲が明確になるような調査方法を解答してほしかった。“改ざんがないかブラウザから直接ページにアクセスして試す”といった，被害拡大につながりかねない危険な調査方法を解答している例が散見された。

設問 3(2)は，正答率が低かった。G 攻撃のシナリオから，テストサーバが改ざんされる条件を洗い出した上で，不正プログラム送り込みサイトが増えたときの URL フィルタの限界に注意して解答してほしかった。“テストサーバが改ざんされて不正プログラム送り込みサイトになった場合”など，テストサーバの改ざん内容を説明しようとする解答が散見された。