平成 31 年度　春期　情報セキュリティマネジメント試験　採点講評

午後試験

問 1

問 1 では，サイバー攻撃を想定した演習における対応方針について出題した。

設問 1 は，(1)，(2)の正答率が低かった。(1)は，機能演習の具体的な“形式”を問うものである。パンデミック対策演習，ファジングテストなど，誤った解答が多く見受けられた。(2)は，偵察にダーク Web を用いるという行為を含まない解答が見受けられた。

設問 2 は，シナリオごとに，対応手順に従って取るべきアクションを問うものである。(3)はグループ 3 のシナリオ 2 の発表結果を“正”とした解答が見受けられた。本文を注意して読めば正答できたはずである。

設問 3(1)では，“1 偵察”段階の対策として，ログの記録を含んだ誤った解答が多く見受けられた。通常のアクセスと偵察のアクセスの区別は困難であることに気付いてほしい。

設問 4 は，正答率が高かった。組織の状況を考慮したサイバー攻撃対応演習の効果について，よく理解していたようである。

情報セキュリティに関する脅威や対策は年々変化しており，攻撃を受けたときの被害拡大防止の重要性が高まっている。それに伴い，サイバー攻撃対応演習などの対策も欠かせなくなっている。情報セキュリティリーダは，積極的にサイバー攻撃を想定した演習を活用して，情報セキュリティの維持，改善を図ってほしい。

問 2

問 2 では，企業における ISMS の活動を題材にして，SNS の利用における情報セキュリティリスクアセスメント及びリスク対応，オンラインショッピングサイトのポータルサイトでの利用権限の管理について出題した。

設問 2 は，正答率が低かった。(1)では，個人情報の保護に関する法律又は情報セキュリティ方針を含む誤った解答が多く見受けられた。また，(2)では，JIS Q 27017 を選んだ解答が見受けられた。適用される法令やガイドラインの動向に日頃から注意を払い，ISMS 規程などの文書を見直すことが必要である。

設問 3 は，正答率が高かったが，(1)では，SNS に直接関係しない SPF（Sender Policy Framework）を含む誤った解答が，(3)では，取引先との私的な交流を含む誤った解答が見受けられた。SNS の特性を考慮し，本文中で与えられた条件をよく確認した上で解答してほしかった。

設問 4 では，利用権限の付与における最小権限の原則に関して問うたが，おおむね理解されていた。

IT の進化に伴い，企業においても様々な IT サービスの利用が進んでいるが，情報セキュリティリーダには，そうしたサービスを新たに利用する際のリスクを適切に評価し，対応する能力を期待したい。

問 3

問 3 では，自己点検と個人所有のスマートフォンの業務利用を題材にして，情報セキュリティを維持するための，管理策の実施状況及び有効性の評価，自己点検の改善，脆弱性情報の見方，並びに情報セキュリティリスクアセスメントについて出題した。

設問 3 の(1)～(3)では，脆弱性評価基準（CVSS）に関して問うたが，(2)及び(3)の正答率が低く，あまり理解されていなかった。脆弱性情報は情報セキュリティの維持にとって重要な情報であるので，日頃から見方を確認しておいてほしい。(4)では，IT 資産管理ツールについて問うたが，正答率が低く，ソフトウェア構成管理ツールと混同した解答が見受けられた。

設問 6 の(1)では，チャットアプリの利用におけるリスクを問うたが，正答率が低かった。写真の位置情報によって撮影場所が特定されるリスクも重要であるが，本文中のチャットアプリの機能をよく確認して解答してほしい。

情報セキュリティ管理策が，現場では実施されなかったり，業務や情報システムの変化に対応できていなかったりして，情報セキュリティ事故が発生してしまうケースがある。情報セキュリティリーダは，導入した管理策が実施されているか，またそれが有効であるかを評価し，情報セキュリティの維持と改善に努めてほしい。