平成 30 年度　秋期　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，ソフトウェア開発の現場で採用されている，メモリ破壊攻撃に対する対策技術について出題した。

設問 1 は，メモリ破壊攻撃自体の仕組みについて問う問題であった。これは，バッファオーバーフローなどのメモリ破壊攻撃についての動作の概要を問う問題である。基本については理解されているようだったが，(2)と(3)についての正答率は低かった。受験者は，メモリ破壊攻撃の具体的な動きについての理解を確認されたい。

設問 2 は，メモリ破壊攻撃に対する対策技術についての問題であった。本文中の説明を理解すれば解ける問題であったので，正答率は高かった。

設問 3 は，メモリ破壊攻撃に対する対策技術の制約についての問題であった。おおむね正答率は低かった。(1)は Automatic Fortification の仕組みを理解した上で，Automatic Fortification が対処できない箇所をソースコードから見つける問題であった。なぜ対処できないのかの理由を正しく理解していない解答が多かった。(2)は，SSP はコンパイラに依存するので，脆弱性があるコードに SSP が適用されない場合，脆弱性が防げないことに気付いてほしかった。

問 2

問 2 では，セキュリティインシデント対応について出題した。

設問 1 は，ミラーポートを使ったネットワークのパケット取得について問う問題であった。正答率は高かったが，STIX を答える問題については，正答率が低かった。

設問 2(2)は，本問で扱ったワームのスキャンの特徴の場合，IP アドレス別件数の上位に登場しない理由を問う問題であった。(a)のスキャンの場合，感染した PC と同一セグメントの範囲をスキャンするため，ネットワークの構成上，NSM ではパケットを取得できないということを正しく理解していない解答が多かった。

設問 4(2)は，有線 LAN の L2SW に接続された PC 同士のワーム感染を防ぐ対策について問う問題であったが，正答率は低かった。L2SW に接続された PC 同士が直接通信を行うというワームの特性を踏まえて，VLAN によるセグメントの分離といったネットワークのレイヤでの対策が立案できるようになることを期待したい。

問 3

問 3 では，ソフトウェアの脆弱性対策について出題した。全体として，正答率は高かった。

設問 2 は，基本評価基準，現状評価基準，環境評価基準の三つの基準で脆弱性の深刻さを評価する CVSS の名称を問う問題であったが，正答率は低かった。基礎的な知識であり，正確に覚えてほしい。

設問 3 は，セキュリティインシデント発生後の被害拡大防止のために必要な措置を問う問題であったが，正答率は高かった。

設問 4 は，攻撃が拡散したかを調査する方法を問う問題であったが，正答率は高かった。ただし，攻撃内容とかけ離れた解答も散見された。攻撃内容から，何を調査すべきかをよく見極めて解答してほしい。

設問 5 は，WAF に関する対策を問う問題であったが，(3)は正答率が低かった。クラウド型 WAF サービスを使用する上での留意点をよく理解してほしかった。WAF の理解を手助けする資料として，IPA が“Web Application Firewall 読本”を公開しているので，学習の参考にしてほしい。