平成３０年度秋期　情報処理安全確保支援士　午後Ⅰ試験　解答速報

（株）アイテック　IT 人材教育研究部　2018.10.23 発表

問１　ソフトウェア開発

【解答例】

［設問１］

(1) a：キ　　b：カ　　c：ウ　　d：ア

(2) あ：㋒

(3) DEP によってスタック領域上の shell コードの実行を防止できるから。

［設問２］

(1) e：canary　　f：ASLR

(2) g：strcpy

［設問３］

(1) 行番号：16

排除できない理由：代入処理においてライブラリ関数が使われていないから。

(2) 問題：メモリ破壊攻撃が成立してしまう問題

開発環境：コンパイラの SSP が適用されない開発環境

問２　セキュリティインシデント対応

【解答例】

［設問１］

a：ウ　　b：ス　　c：セ　　d：エ　　e：コ

［設問２］

(1) SYN/ACK

(2) (a)：NSM センサが NF 情報として記録しないから。

(b)：同一 IP アドレスには１回しかスキャンしないから。

［設問３］

(1) (PC101)　PC104　PC105　PC132　(PC133)　PC145　PC204
(PC277)　PC298　(PC301)　(PC321)　PC335　(PC340)

(2) イ，オ，カ

［設問４］

(1) ① 最新のセキュリティ修正プログラムが適用されていること

② 最新のマルウェア定義ファイルに更新されていること

(2) PC を分離するように L2SW に VLAN を設定する。

問３　ソフトウェアの脆弱性対策

【解答例】

［設問１］

NTP サーバとの時刻同期

［設問２］

a：CVSS

［設問３］

E サーバを L2SW から切り離して，待機サーバを公開する。

［設問４］

調査すべき機器：ログ管理サーバ

調査すべき内容：外部メールサーバへの SSH コマンドによる接続の有無

［設問５］

(1) b：攻撃

(2) インターネットからの HTTPS 通信を終端して復号する機能

(3) c：外部 DNS サーバ

d：CNAME

以上