令和元年度秋期　情報処理安全確保支援士　午後Ⅱ試験　解答速報

（株）アイテック　IT 人材教育研究部　2019.10.23 発表

問１　ソフトウェア開発におけるセキュリティ対策

【解答例】

［設問１］

(1) S 社開発用 LAN の PC からサーバ A のポート 6379/tcp へ接続し，遠隔コマンド実行機能を用いて暗号資産の採掘用プログラムを停止させる。

(2) α：カ　　β：ク　　γ：ア

(3) 会員情報を保持する DBMS-R への S 社の PC 以外からのアクセスは，マルウェア X によるアクセス 1 回だけであり，かつ，マルウェア X は採掘演算結果だけを外部の特定のサーバに送信するだけだから

［設問２］

(1) 対策 1：(イ)　　対策 2：(イ)，(ウ)　　対策 3：(ア)，(エ)
対策 4：(ア)，(ウ)，(エ)，(オ)

(2) あ：22/tcp　　い：6379/tcp　　う：a2.b2.c2.d2

(3) a：curl　　b：iptables

(4) え：オ　　お：カ　　か：キ

［設問３］

(1) ア，イ，ウ

(2) S システムの実行環境の構成要素に関して，名称，バージョン，脆弱性情報の収集方法などの構成管理情報を棚卸しする。

(3) き：ア　　く：ウ

(4) け：レビュー　　こ：メンバ

［設問４］

c：オ　　d：ア　　e：エ　　f：カ　　g：キ　　h：ウ

問２　工場のセキュリティ

【解答例】

［設問１］

(1) マルウェアによる通信時に，標準 PC における通常の HTTP リクエストと同じ値が設定されるケース

(2) a：エ

(3) b：ア

(4) c：サイト U

［設問２］

(1) d：カ　　e：キ　　f：オ

(2) 活動 1：1　　活動 2：7　　活動 3：3

［設問３］

g：無線電波を傍受

h：機器の MAC アドレス

［設問４］

(1) 攻撃者のサーバからの指示による動作の封じ込め

(2) l：イ　　j：ウ　　k：ア

(3) マルウェア対策ソフトで USB メモリをスキャンする。

［設問５］

(1) 事務 LAN 用：(い)　　センサ NET 用：(か)

(2) AP への不正接続が発生しても，分離された F-NET の FA 端末には攻撃が及ばないので生産設備が停止するリスクが小さい。

［設問６］

(1) イ

(2) ① 当該ソフトウェアを停止する。

② 業務サーバを A-NET から切り離す。

［設問７］

(1) 図 4　工場 LAN：エ　　標準 PC：エ　　FA 端末：ア

図 5　事務 LAN：エ　　F-NET：ア　　センサ NET：ア　　標準 PC：エ　　FA 端末：ア

(2) ① 接続についてのリスクアセスメントの結果

② 接続についてのリスク対応及び措置の内容

以上