令和元年度秋期　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　2019.10.23 発表

問１　電子メールのセキュリティ対策

【解答例】

［設問１］

a：MAIL（又は，MAIL FROM）

［設問２］

(1) b：×　c：×　d：×　e：×　f：×　g：○　h：×　i：×

(2) j：x1.y1.z1.1

(3) メール送信側の DNS サーバは，転送メールサーバの IP アドレスを登録していないから。

(4) メール本文及びメールヘッダの完全性

［設問３］

k：mail.x-sha.co.jp　l：x2.y2.z2.1　m：quarantine　n：r

［設問４］

N 社の取引先の PC をマルウェアに感染させ，正当な利用者のメールアドレスを用いてメールを送信する。

問２　セキュリティインシデント対応におけるサイバーセキュリティ情報の活用

【解答例】

［設問１］

(1) プロキシ認証に失敗したから。

(2) a：(b)

(3) ・グローバル IP アドレス M への HTTP 通信の成功
・パブリック DNS サービス L への DNS 通信の発生

(4) イ，ウ

［設問２］

(1) エ

(2) ウ

(3) 項番：3
送信元：DMZ　　宛先：インターネット　　サービス：DNS　　動作：許可

(4) b：権威 DNS サーバ
c：外部 DNS サーバ
d：再帰的クエリ

(5) e：同じドメイン名に対する連続的な DNS クエリの発生

問３　標的型攻撃への対応

【解答例】

［設問１］

(1) 不審 PC のメモリやストレージの状態を保全するため。

(2) ① ほかの PC やサーバへ感染拡大する。
② C&C サーバと通信して情報を送信する。

［設問２］

a：ウ　　b：イ　　c：オ　　d：ア

［設問３］

(1) e：C&C サーバのグローバル IP アドレスとの通信

(2) 攻撃の初期調査や探索活動フェーズにあり，C&C サーバへの通信開始前の状態

(3) マルウェア M のハッシュ値を用いて R ログを検索する。

以上