平成３１年度春期　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　2019.4.24 発表

問１　マルウェア感染と対策

【解答例】

［設問１］

a：FW1　　b：プロキシサーバ

［設問２］

内容：削除されたものを含む全てのファイル

手段：セクタをスキャンして削除ファイルを復元する。

［設問３］

(1) WPA2 を用いても，MAC ヘッダは暗号化されないから。

(2) 攻撃者の無線 LAN 端末の MAC アドレスを，傍受した登録済み MAC アドレスに書き換える。

［設問４］

(1) 同一端末間のパケットの IP ヘッダは，同じ情報ブロックになることが多い。

(2) c：同一の暗号ブロック

d：平文ブロック

e：暗号化処理されたカウンタ値

［設問５］

(1) f：ログとして記録する

(2) g：カ　　h：オ

(3) 次のうち，2 点が指摘されていればよい。

・内部メールサーバを経由し外部メールサーバから SMTP で送信する。

・プロキシサーバに接続しプロキシサーバから FTP で送信する。

・プロキシサーバを経由し外部メールサーバから SMTP で送信する。

［設問６］

(1) i：信頼されたルート CA のディジタル証明書

(2) j：利用者が TLS クライアント認証処理を行う外部 Web サーバにアクセスする。

(3) k：FW1 がディジタル証明書をもっていないルート CA によって発行されたサーバ証明書を使用する外部 Web サーバにアクセスする。

問２　情報セキュリティ対策の強化

【解答例】

［設問１］

a：秘密管理　　b：有用　　c：非公知

［設問２］

(1) d：オープンリレー

(2) x1.y1.z1.16/29

［設問３］

(1) e：x1.y1.z1.18

(2) f：NTP

(3) g：ア

(4) h：CRYPTREC

［設問４］

i：エ

［設問５］

(1) サーバのログには，DPC，日時及び利用者 ID を特定する情報が含まれるが，操作者を特定する情報がないから。

(2) 当該アクセスの時間帯にはメンバの 3 人とも B 社で打合せをしており，K さんの DPC を操作し得ないから。

(3) パスワードの変更

(4) 侵入したマルウェアの活動に伴う被害や影響の有無と範囲を調査するため。

(5) 平常時には利用者が圧縮ファイルを展開したタイミングでリアルタイムスキャンが実行されるから。

［設問６］

(1) アクセス制限機能に関して，アクセスを許可する IP アドレスを設計部と製造部の LAN に制限する。

(2) 初期パスワードについては，初回のログイン時に変更を強制する設定にする。

［設問７］

j：リアルタイムで通知

以上