平成２９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　2017.4.18 発表

問１　マルウェアの解析

【解答例】

［設問１］

(1) ウ，エ

(2) a：プロキシサーバ　　b：DHCP サーバ

［設問２］

(1) 被疑サーバの FQDN

(2) 中継サーバ１

(3) hosts ファイルに被疑サーバの FQDN と中継サーバ１の IP アドレスを対応付けて設定する。

［設問３］

(1) マルウェアの実行時間を計測し，ブレークポイントによる中断などを検知する方法

(2) メモリにロードされたときにはマルウェア本体が暗号化されているので，ウイルス定義ファイルとは一致しないから。

［設問４］

(1) c：プロキシサーバのブラックリスト

(2) d：脆弱性 K に対する脆弱性修正プログラムを適用する

(3) e：パスワードの変更

［設問５］

(1) 最新の脆弱性修正プログラムが適用済みか否かという点

(2) f：パッチ配信サーバ

(3) PDF 閲覧ソフトの最新の脆弱性修正プログラムが未適用の状態で，Q 社の Web サイトを閲覧していた場合

［設問６］

(1) 被疑 PC の HDD の複製を作成する作業

(2) 業務を継続するための代替 PC を貸し出す対応

(3) プロセスを自動実行するスケジュール設定などを含む OS の設定ファイルの内容

問２　社内システムの情報セキュリティ対策強化

【解答例】

［設問１］

(1) a：SMTP over TLS

(2) b：ウ　　d：ア

(3) c：内部メールサーバ

［設問２］

(1) e：プロキシサーバ

f：送信元 IP アドレスが感染したサーバかつ URL が C&C サーバ

(2) g：外部メールサーバ

h：インターネットへ転送されて転送結果が正常終了

(3) 外部 DNS サーバの設定変更の内容：

TXT レコードの再帰的な DNS 問合せは外部メールサーバに限定する。

内部 DNS サーバの設定変更の内容：

TXT レコードの DNS 問合せは外部 DNS サーバに送らない。

(4) i：レコードタイプが TXT レコードの再帰的な DNS 問合せ

［設問３］

(1) ファイルを暗号化せずにアップロードする。

(2) ウイルス対策ソフトがマルウェアを検知した時点でリアルタイムに通知する機能

［設問４］

j：PC-LAN

［設問５］

ホスト型の IPS を導入してサーバの脆弱性を突く攻撃を遮断する。

以上