令和３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　2021.10.13 発表

問１　協力会社とのファイルの受渡し

【解答例】

［設問１］

(1) a：<　　b：>

(2) c：エ

［設問２］

(1) URL の出力処理を http:や https:から始まる文字列だけを許可する方式で実装する。

(2) D システムとスキーム及び FQDN が一致する同一オリジンのスクリプトファイル

(3) スクリプト：HTML 中のインラインに記述されたスクリプト

呼出し方法：<script src="スクリプト URI"></script>の形で URI を指定して呼び出す。

［設問３］

(1) d：ウ　　e：ア

(2) G サービスの機能とは別に, U 社と協力会社がファイルの暗号化と復号を実施する。

［設問４］

(1) f : 同一利用者 ID によるログイン失敗

(2) 異なる IP アドレスの多数の端末からログイン試行を実行された場合

［設問５］

(1) g : 利用者認証のメッセージを中継

(2) h：生体認証

i：K サービス

j：アカウントを削除

k：アカウントを停止

(3) PC が認証器を兼ねるので, ファイル受渡し用 PC だけが G サービスにアクセス可能になるから。

問２　マルウェア感染への対処

【解答例】

［設問１］

(1) a：ア　　b：イ　　c：イ　　d：ウ

(2) e：CRYPTREC

［設問２］

(1) エ

(2) アクセス元を UTM のグローバル IP アドレスに限定していたこと

［設問３］

(1) C&C サーバの IP アドレス及び当該サーバに関する DNS レコードの変更

(2) FQDN ではなく，IP アドレスのリストを用いる通信を遮断できないから。

(3) f：イベントログの消去を示すログ

(4) 待機機能及び横展開機能だけを実行した場合

(5) UTM の IDS 機能によって，不審なインバウンド通信を早期に検知できるから。

［設問４］

(1) g：7 月 14 日

(2) h：IP リストに登録された IP アドレス

(3) 連携端末以外の端末から C&C サーバへの通信記録

(4) 連携端末を一時的にネットワークから切り離す対応

以上