平成２４年度秋期　情報セキュリティスペシャリスト　午後Ⅰ試験　解答速報

（株）アイテック　情報技術教育研究部　2012,10,24 発表

2012,10,25 修正（問 2 設問 2（4））

問１　インターネット Web サイトの刷新

【解答例】

［設問１］

a：エ　　b：ウ

［設問２］

会員登録をすれば，誰でもサービスを利用できる。

［設問３］

(1) c：会員サイト　　e：ブラウザ

(2) 会員が会員サイトにログイン済みで，クッキーの有効期限が切れてなく，かつログアウト前であるという条件

(3) d：JSONP 型データ

［設問４］

f：ログインした会員　　g：転送されない

問２　ログの管理

【解答例】

［設問１］

(1) 営業部が業務目的で利用する頻度と時間帯

(2) a：個人情報へのアクセスを試みた無権限者

(3) ログイン失敗

［設問２］

(1) 個人情報への不正アクセスの抑止

(2) モニタリング条件で抽出されない方法を用いて不正アクセスされること

(3) 有権限者が自身の利用者 ID を用いて，毎週，利用成功回数を超えない範囲内で個人情報にアクセスした場合

(4)b：　1 週間で 8,000 番台の機能の利用成功回数が 50 回以上

［設問３］

モニタリング結果のレビューを定期的に行い，レビュー結果と業務の変化を勘案して条件を適切に見直す。

問３　標的型攻撃メールへの対応

【解答例】

［設問１］

a：ウ　　b：ア

［設問２］

(1) c：オ　　d：イ

(2) □□. △△. ○○. ▽▽

［設問３］

(1) メールに書いてある社外サイトをたどった点

(2) システムの名称：ネットワーク型 IDS

設置場所：DMZ と社内 LAN

監視すべき事象：異常なトラフィックの発生

(3) PC からインターネット上の Web サイトへの直接通信は FW で遮断されている。

(4) PRX でユーザ認証を行い，認証に成功した場合にアクセスを許可する。

問４　情報セキュリティインシデント対応

【解答例】

［設問１］

16 時以降の時間帯で，Web サーバの使用率が高くなっていれば攻撃を受けている可能性が高いから。

［設問２］

(1) a：△△. 123. 123. 123

(2) 表 5 (3)，表 6 (1)

(3) HTTP リクエストが Web サーバで正常に処理されているから。

［設問３］

(1) b：送信元 IP アドレス　　c：HTTPS　　d：暗号化鍵

(2) Web サーバプログラムの同時セッション数が 50 になっている場合

(3) 機器①：ウ

設定内容①：X-Forwarded-For ヘッダを追加して Web サーバに送信する。

機器②：オ

設定内容②：X-Forwarded-For ヘッダの送信元 IP アドレスをログに出力する。

以上