平成２１年度春期　情報セキュリティスペシャリスト　午後Ⅱ試験　解答速報

（株）アイテック　情報技術教育研究グループ　2009, 4, 21 発表

問１　公開鍵基盤の構築

【解答例】

［設問１］

a：1,024　　b：SHA-1　　c：ハッシュ値　　f：自己署名

［設問２］

問題：テレワーク PC が直接インターネット接続を行うと，ウイルス定義ファイルが配布されない。

対策：テレワーク PC については，ウイルス定義ファイルのベンダサイトに接続するように設定変更する。

［設問３］

①　テレワーク PC に格納された秘密鍵をコピーされないようにする。

②　秘密鍵を活性化するためのパスワードを設定する。

［設問４］

改ざんしたデータに対し署名アルゴリズムを適用してハッシュ値を求め，そのハッシュ値に対して推測した秘密鍵で暗号化する。　（2009/04/28 アイテック修正）

［設問５］

(1) 公開鍵証明書を偽造されると，不正アクセスが可能となり社内の機密情報などが漏えいする。

(2) d：(イ)　　e：(ケ)

(3) CA 運用担当者が鍵ペアを取り扱う際の規定を明確にする。

［設問６］

問題：受信したメールを復号できない。

理由：第三者は，A 社の自己署名証明書を入手できないから。

問２　インターネット販売を行う企業の情報セキュリティ管理

【解答例】

［設問１］

(1) a：情報セキュリティ委員会

(2) セキュリティ要件が提示されていなければ委託先の責任ではないので，その後の修正などの費用を P 社が負担する必要がある。

［設問２］

(1) b：事業継続　　c：NTP

(2) ウイルス対策ソフトにおける更新履歴の状況を確認する。

(3) ポートスキャンの結果，サーバで必要としないサービスから応答があった場合に不要と判断する。

(4) 地震などで P 社が被災した場合，バックアップ媒体も同一場所にあるため，事業の再開が難しくなる。

(5) 対象システムを熟知しているので，客観的なテストにならない。

［設問３］

(1) 個々の Web アプリケーションに対し，いろいろな攻撃パターンをすべて定義することは困難であるから。

(2) WAF の検知機能を回避する攻撃が発生し，Web アプリケーションに脆弱性がある場合には簡単に侵入されてしまう。

［設問４］

(1) d：エ

(2) e：チェックポイント経過後はトランザクションログを削除する。

［設問５］

観察事項として指摘された事項について，それらの改善状況に関する記録を残す。

（2009/04/28 アイテック修正）