TAC

平成27年度秋期 情報処理技術者試験

情報セキュリティスペシャリスト 解答例

【午 後 Ⅰ】

問 1 （配点 50 点）

設問 1 （12 点：要素 3 点×2，理由 3 点×2）

（E システム）（要素） 可用性

（理由） 販売チャネルの大部分を担い，常時稼働が必要だから

（E システムの別解）（要素） 機密性

（理由） 購入者情報の漏えいは事業の継続や業績に悪影響する。

（F システム）（要素） 完全性

（理由） 投資家に対して，正確な財務情報開示の必要があるから

設問 2 （4 点）

a：公開ディレクトリ上

（別解） webapps/ROOT

設問 3 （22 点：(1)2 点×6，(2)2 点×2，(3)2 点，(4)4 点）

（1） b：ANY

c：遮断

d：COOKIE

e：遮断

f：Multipart

g：遮断

（b，d，f は順不同）

（2） イ，ウ

（3） エ

（4） 動作に必要な最小限の権限を付与するように見直す。

設問 4 （8 点：4 点×2）

① 攻撃のパターンにマッチする HTTP リクエストが遮断されること

② 攻撃のパターンにマッチしない HTTP リクエストが通過すること

設問 5 （4 点）

可用性を損なわずに，誤判定しやすい通信に関するログを蓄積・精査でき，設定改善に役立てられる。

問 2 （配点 50 点）

設問 1 （6 点）

a:Y 社の管理者

設問 2 （27 点:(1)委託用特権 ID 5 点，理由 6 点，(2)5 点×2，(3)6 点）

（1）（委託用特権 ID） DBMS 操作 ID

（理由） 作業者と各業務アプリが DBMS 操作 ID を共用しているから

（2） b:FW1

c:管理用サーバ

（3） 作業対象サーバでの操作履歴は書き換え困難な管理用サーバに保存されるから

設問 3 （17 点:(1)6 点，(2)5 点，(3)6 点）

（1） 個人 ID が付与された本人以外の者に使われない管理が徹底されていること

（2） 抑止効果

（3） 管理用サーバ及びプログラム K の Y 社資産だけを資産管理の対象とすればよいから

問 3 （配点 50 点）

設問 1 （9 点:3 点×3）

a:WebAP サーバ 2

b:WebAP サーバ 1

c:Web サーバ

設問 2 （17 点:(1)2 点×4，(2)9 点）

（1） d:2

e:404

f:14

g:200

（2） 僅か数秒内の管理画面へのログイン試行が，8 回連続して失敗した直後に成功した様子をログのステータスコードから読み取れるから

設問 3 （12 点:(1)2 点×2，(2)項番 2 点，サービス 3 点×2）

（1） 3，4

（2）（項番） 5

（サービス） ① ファイル共有

② リモートデスクトップ

設問 4 （12 点:(a)6 点，(b)6 点）

（a） インターネットからサーブレットコンテナの管理画面にアクセスしログイン試行する攻撃

（b） サーバ OS の仕様を利用して，他のサーバに自動ログインして侵入範囲を広げる攻撃

【午　後　Ⅱ】

問 1 （配点 100 点）

設問 1 （16 点：(1)(a)3 点，(b)3 点，(c)3 点，(2)構成要素 3 点，通信 4 点）

（1） （a） 1，2，3

（b） 1，3，7，8，9

（c） 1，10，11

（2） （構成要素） TC サーバ

（通信） 2，3，10，11

設問 2 （48 点：(1)6 点×2，(2)12 点，(3)3 点，(4)3 点，(5)送信元 3 点×2，宛先 3 点×2，プロトコル 3 点×2）

（1） ① 受信メールの添付ファイルが暗号化されていた場合

② HTTPS 通信で添付ファイルをダウンロードした場合

（②の別解） ダウンロードしたファイルが暗号化されていた場合

（2） Web ブラウザ終了で仮想 IP アドレスが解放され，それを再利用した別のクライアントプロセスが利用者認証を受けずに Web アクセスができる可能性があるから

（3） IA 用 TC サーバ

（4） OA 用 TC サーバ

（5） （Web サイトのファイルを閲覧した場合）

（送信元） IA 用 TC サーバ

（宛先） ファイルサーバ又はグループウェアサーバ

（プロトコル） Windows ファイル共有プロトコル又はグループウェア独自プロトコル

（受信メールの添付ファイルを開いた場合）

（送信元） OA 用 TC サーバ

（宛先） 認証プロキシサーバ

（プロトコル） HTTP 及び HTTPS

設問 3 （12 点：(1)4 点，(2)4 点×2）

（1） b，c，f，g

（2） （Web サイトのファイルを閲覧した場合） 海外支店 X 用 TC サーバ

（受信メールの添付ファイルを開いた場合） 海外支店 X 用 TC サーバ

設問 4 （15 点：(1)10 点，(2)5 点）

（1） 476 ［M ビット／秒］

（2） ア，ウ，オ，キ，ク

設問 5 （9 点）

セキュリティ管理状況の公正かつ客観的な監査を行えない。

（注）問 1 の配点では，記号列挙の設問はすべて正解のときのみ得点できるものとする。

問 2 （配点 100 点）

設問 1 （11 点：(1)6 点，(2)5 点）

（1） 同期アプリの同期機能によって，感染ファイルが利用者の PC に自動的にコピーされる。

（2） マルウェアを検知した場合にバックアップファイルを削除する。

（別解） 同期ディスクのファイルの更新時にマルウェアスキャンを行う。

設問 2 （14 点：(1)2 点×4，(2)3 点×2）

（1） a：ク

d：ア

e：オ

f：キ

（2） b：営業秘密

c：公然と知られていないこと

設問 3 （26 点：(1)3 点×2，(2)6 点，(3)2 点×5，(4)2 点×2）

（1） g：OS

h：暗号化

（2） 同じ平文ブロックは同じ暗号文ブロックに暗号化されるので，それを足掛かりに解読されやすい。

（3） i：1

j：24

k：1

l：1

m：5

（4） n：CBC モード

o：OFB モード

設問 4 （27 点：(1)5 点，(2)6 点，(3)3 点×2，(4)2 点×5）

（1） サーバごとに生成した暗号鍵を Q サービス内で管理する仕様

（2） ある鍵が漏れても，他の鍵に対応するフォルダのファイルは復号できない。

（3） ① 暗号化対象ファイルのファイル名

② 暗号化対象ファイルのパス名

（4） p：9

q：62

r：2

s：31

t：8.9

設問 5 （16 点：(1)6 点，(2)場合 5 点，修正内容 5 点）

（1） 暗号化ファイルが登録・更新された場合，復号した上でマルウェアスキャンを行ってから，同期処理を行う。

（2） （場合） 同期用 FS が平文ファイルを検知前に Q サービスにバックアップされた場合

（修正内容） 同期用 FS が該当ファイルを暗号化時にバックアップを削除する。

設問 6 （6 点）

保護すべき情報の安全管理に必要な事項を事前に確認し，委託契約に盛り込む。

（別解） 委託先のセキュリティ対策の実施状況を定期的または不定期に確認する。

以上