TAC

平成29年度春期情報処理安全確保支援士試験

情報処理安全確保支援士　解答例

【午　後　Ⅰ】

問 1 （配点 50 点）

設問 1 （28 点：(1) 4 点×3, (2) 4 点, (3) 4 点×3）

(1) a ：（カ）

b ：（オ）

c ：（エ）

(2) d ： 5

(3)（送信元）カ

（宛先）ケ

（サービス）キ

設問 2 （8 点：4 点×2）

（攻撃名） 中間者攻撃

（機器名） CRM サーバ

設問 3 （14 点：(1) 6 点, (2) 4 点×2）

(1) 管理用 PC とサーバセグメント間の通信が PC セグメントに流れないから

(2)（SYN パケット）(C)(A)

（SYN-ACK パケット）(A)(B)

問 2 （配点 50 点）

設問 1 （12 点：6 点×2）

（L 氏に確認した内容） L 氏が今日サイトαにログインした時刻

（ログイン記録） L 氏の利用者 ID で今日ログインされた時刻

設問 2 （24 点：(1) 4 点, (2) 4 点, (3) 4 点×2, (4) 4 点×2）

(1) a ： クロスサイトリクエストフォージェリ

(2) b ： 3

(3) c ： 現在のパスワード

d ： 知り得ない

(4) e ： confirm

f ： submit

設問 3 （14 点：(1) 4 点, (2) 4 点, (3) 6 点）

(1) カ, キ

(2) g ： セッションハイジャック

(3) h ： スクリプトを実行する属性を無効化する

問 3（配点 50 点）

設問 1（4 点）

利用者 ID が F 社のもので，接続元 IP アドレスが F 社の IP アドレス以外

設問 2（32 点：(1) 3 点×4，(2) 3 点×2，(3) 3 点，(4) 3 点×2，(5) 5 点）

(1) a ： ウ

b ： エ

c ： ア

d ： イ

(2) e ： 処理 1

f ： 処理 4

(3) g ： ウ

(4) h ： IdP

i ： 改ざん

(5) 利用者端末の Web ブラウザ経由で認証情報をやりとりするから

設問 3（14 点：(番号 3 点，理由 4 点)×2）

（交通費精算サービス）（番号）(3)

（理由）社外から社内ネットワークへの通信はファイアウォールで禁止されているから

（グループウェアサービス）（番号）(1)

（理由）接続元 IP アドレスの制限機能でログインを社内からだけに制限しているから

【午　後　Ⅱ】

問 1 （配点 100 点）

設問 1 （15 点:(1) 5 点, (2) 5 点×2）

(1) ウ, エ

(2) a ： プロキシサーバ

b ： DHCP サーバ

設問 2 （17 点:(1) 5 点, (2) 5 点, (3) 7 点）

(1) 被疑サーバの FQDN

(2) 中継サーバ 1

(3) 宛先 IP アドレスを被疑サーバの IP アドレスから中継サーバ 1 の IP アドレスに書き換える設定

設問 3 （13 点:(1) 6 点, (2) 7 点）

(1) マルウェアが実行される時間が通常の時間より長いことを検知する方法

(2) ウイルススキャン時のマルウェアは暗号化済みコードになっているので, ウイルス定義ファイルのパターンと一致しないから

設問 4 （18 点:(1) 6 点, (2) 6 点, (3) 6 点）

(1) c ： プロキシサーバのブラックリスト

(2) d ： 脆弱性 K を含む公開された脆弱性修正プログラムを全て適用する

(3) e ： パスワードの変更

設問 5 （18 点:(1) 6 点, (2) 5 点, (3) 7 点）

(1) PDF 閲覧ソフトの脆弱性修正プログラムを適用しているか否か

(2) f ： パッチ配信サーバ

(3) PDF 閲覧ソフトの脆弱性修正プログラムが適用されておらず, 該当する PDF ファイルをダウンロードしている場合

設問 6 （19 点:(1) 6 点, (2) 6 点, (3) 7 点）

(1) 被疑 PC の HDD の複製を作成する作業

(2) 被疑 PC の利用者に脆弱性が修正された PC を貸与する。

(3) g ： 不審 PC に適用されている脆弱性修正プログラムや更新されているウイルス定義ファイル

問 2 （配点 100 点）

設問 1 （24 点:(1) 6 点, (2) 6 点×2, (3) 6 点）

(1) a ： SMTP over TLS

(2) b ： ウ

d ： ア

(3) c ： 内部メールサーバ

設問 2 （47 点:(1) e 6 点, f 7 点, (2) g 6 点, h 7 点, (3) 7 点×2, (4) 7 点）

(1) e ： プロキシサーバ

f ： ログに記録された URL がマルウェア X の C&C サーバの URL

(2) g ： 外部メールサーバ

h ： 内部メールサーバの調査の宛先メールアドレスと同じ

(3)（外部 DNS サーバの設定変更の内容）

内部 DNS サーバからの再帰的な DNS 問合せを拒否する。

（内部 DNS サーバの設定変更の内容）

内部 DNS サーバでの名前解決は社内専用のドメイン名に制限する。

(4) i : 社外のドメイン名の TXT レコードの DNS 問合せ

設問 3（15 点:(1) 7 点, (2) 8 点）

(1) ファイルを暗号化せずにアップロードする。

(2) サーバ及び PC をフルスキャンしたときのマルウェア検出結果を集中管理する機能

設問 4（6 点）

j : PC-LAN

設問 5（8 点）

ネットワーク型の侵入検知システムを導入し, サーバ間の通信を監視する。

以上