TAC

平成30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 （8 点:4 点×2）

a : カ

b : ウ

設問 2 （5 点）

0x785634120a

設問 3 （5 点）

c : （エ）

設問 4 （5 点）

d : 0x0b123400

設問 5 （5 点）

e : データ

設問 6 （7 点）

共有ライブラリ内のメモリアドレスはデータ実行防止の対象外で system 関数を実行できるから

設問 7 （5 点）

f : （ア）

設問 8 （5 点）

g : DisplayNote

設問 9 （5 点）

h : m_note = NULL;

問 2 （配点 50 点）

設問 1 （20 点:(1)5 点, (2)5 点×3）

（1） a : x1.y1.z1.4

（2） b : 迷惑メール対策サーバ

c : Web メールサーバ

d : 外部メールサーバ

設問 2 （18 点:(1)6 点, (2)6 点×2）

（1） e : インターネット上のドメイン名の名前解決を行う再帰問合せ

（2） ① マルウェアスキャンをすり抜けてメールを送信できてしまう。

② 業務上, 外部へメールを送信する必要がない者が外部へメールを送信できてしまう。

（別解） 送信者メールアドレスを詐称したメールを送信できてしまう。

設問 3 （12 点：(1)6 点，(2)6 点）

（1） 運用 PC の IP アドレスからの接続を拒否する設定を追加する。

（2） 運用 PC の IP アドレスから T 社標準ソフトの各ベンダのサイト以外の URL への接続を拒否する設定を追加する。

問 3 （配点 50 点）

設問 1 （8 点：(1)2 点×2，(2)2 点×2）

（1） a ： ウ

b ： エ

（2） c ： ア

d ： ウ　（c，d は順不同）

設問 2 （21 点：(1)4 点，(2)e～g 各 3 点，方法 4 点，(3)4 点）

（1） ファイル転送サーバから研究開発 PC への通信は全て FW2 で遮断されるから

（2） e ： アップロード用 URL

f ： 利用者 ID

g ： パスワード

（方法） 感染した事務 PC のブラウザ内に保存された情報を利用する。

（3） 研究開発員が，ファイル転送サーバに自分でアップロードした覚えのない不正なファイルがあれば気づくから

設問 3 （16 点：4 点×4）

h ： 高い

i ： 配信サーバが研究開発 PC と同一ネットワーク上にあるから

j ： 低い

k ： FW2 によって感染活動を遮断できるから

設問 4 （5 点）

l ： 上長によるアップロードの承認

【午　後　Ⅱ】

問 1 （配点 100 点）

設問 1 （30 点：(1)10 点，(2)10 点，(3)10 点）

（1） フラグメント識別子に記述した攻撃コードはサーバに送信されないから

（2） フラグメント識別子をそのまま出力する JavaScript の記述がないか分析する。

（3） R ポータルが JavaScript で Cookie の参照や更新を行う実装をしている場合

設問 2 （10 点）

全サーバのアクセスログ取得による利用者 ID 及び時刻と，踏み台サーバの操作記録機能によるデスクトップ画面の画像データと実行内容及び入力情報

設問 3 （30 点：(1)4 点×4，(2)10 点，(3)4 点）

（1） a ： WebAP サーバ

b ： DB サーバ

c ： ODBC

（ルール） 項番 9

（2） 人事総務課職員が踏み台サーバからリモートデスクトップ機能を使い共通管理者アカウントで DB サーバにアクセスする。

（3） d ： 2

設問 4 （30 点：(1)10 点，(2)10 点，(3)10 点）

（1） e ： コンテナサーバにアクセスする利用者人数

（2） f ： 協力者に CCI のメディアを渡し，PC に CC をインストール

（3） g ： DMZ 上の DRM サーバへのアクセスを製作パートナの IP アドレスからのみに制限する

問 2 （配点 100 点）

設問 1 （20 点：(1)7 点，(2)7 点，(3)6 点）

（1） 特定の文字列を含む HTTP リクエストを POST メソッドで送信した場合

（2） a ： Web サイト Y の全ファイルと比較

（3） 公開鍵認証方式

設問 2 （7 点）

b ： Web サイトで利用している全ての WF，プラットフォーム及び Web アプリの製品名とバージョン

設問 3 （20 点：5 点×4）

c ： ディレクトリ

d ： クロスサイト

e ： HTTP

f ： ジャッキング

設問 4 （39 点：(1)6 点×2，(2)6 点，(3)7 点，(4)7 点×2）

（1） g ： 30

h ： 0

（2） i ： イ

（3） j ： (う)で，code に限定商品のコードを指定して，“選択”ボタンをクリックする

（4） k ： Web サイトで利用する全種類の

l ： 許可されていない操作内容と想定される結果

設問 5 （7 点）

Web セキュリティガイドのレビューポイントに従って，レビューが実施済みであること

設問 6 （7 点）

検出された個々の脆弱性を作り込まないように，正しい実装方法を具体的に追加する。

以上