TAC

令和5年度秋期　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】

問 1（配点 50 点）

設問 1（10 点：(1)4 点，(2)6 点）

(1) イ

(2) 会員の投稿内容を HTML エスケープしてから画面出力する。

設問 2（8 点）

複数のレビューにスクリプトを分割し，投稿間の記述をコメントにして連続投稿し，一つのスクリプトにする。

設問 3（24 点：(1)8 点，(2)8 点，(3)8 点）

(1) 会員プロフィール設定ページにアクセスして取得したトークンを用いて，アイコン画像として cookie をアップロードする。

(2) 会員が投稿したレビューに表示されるアイコン画像をダウンロードし，テキストファイルとして読み込む。

(3) 取得したセッション ID の会員になりすまして商品の購入やレビューの投稿ができる。

設問 4（8 点）

同一生成元ポリシーにより，異なるオリジンのリソースへのアクセスを制限する。

問 2（配点 50 点）

設問 1（17 点：(1)2 点×2，(2)4 点×2，(3)5 点）

(1) a ： 利用者 ID

b ： パスワード

(2) c ： このサーバ証明書は，信頼された認証局から発行されたものではない。

d ： このサーバ証明書のドメイン名が，アクセス先のドメイン名と一致していない。

(3) https に変換して接続し，TLS ハンドシェイクでサーバ証明書のコモン名と B サービスの FQDN が一致するか検証する。

設問 2（7 点：(1)5 点，(2)2 点）

(1) 宛先に私用メールアドレスを指定して承認申請を行い，外部共有リンクを取得する。

(2) e ： MAC アドレス

設問 3（26 点：(1)2 点，(2)2 点，(3)4 点，(4)5 点，(5)5 点，(6)2 点，(7)完答 3 点×2）

(1) RADIUS

(2) f ： クライアントの秘密鍵

(3) g ： 漏えいしないように安全に管理

(4) クライアント証明書を個人所有 PC に格納して不正利用することを防止できるから

(5) 来客用無線 LAN からインターネットへの通信時の送信元 IP アドレスは，a1.b1.c1.d1 以外のグローバル IP アドレスに変換する。

(6) h ： DNS

(7)（表 3）1

（表 4）1, 4

問 3（配点 50 点）

設問 1（完答 4 点）

イ, ウ, エ

設問 2（21 点:(1)5 点, (2)2 点, (3)2 点, (4)5 点, (5)5 点, (6)2 点）

(1) U さんが偽サイトに入力した認証情報と TOTP を用いてクラウド管理サイトに直ちにログインする。

(2) ア

(3) イ

(4) フロントエンドから CI デーモンへの通信を監視しシークレットを窃取する。

(5) 認証要求に対する署名検証時に, オリジンが正規のオリジンと一致することを確認する。

(6) ア

設問 3（25 点:(1)5 点, (2)5 点, (3)5 点, (4)5 点×2）

(1) コード署名を付与した不正な P アプリを J ストアにアップロードして利用者に配布する。

(2) P 社の認証用 API キーを削除する。

(3) ID ベースの認証を行い, 不正使用を防ぐ。

(4)（影響）従来の P アプリが起動できなくなる。

（対応）P アプリを再インストールする。

問 4（配点 50 点）

設問 1（15 点:ア 完答 4 点, イ 3 点, ウ 3 点, エ 5 点）

ア : 1, 8, 10, 11, 12, 13

イ : (大) ・ 中 ・ 小

ウ : A ・ B ・ (C) ・ D

エ : G 百貨店で, S サービスのログインを許可するアクセス元 IP アドレスを, W 社など業務に S サービスの利用が必要な会社の IP アドレスのみに制限する。

設問 2（27 点:(1)4 点, (2)い 5 点, う 完答 4 点, え 3 点, お 3 点, か 3 点, き 5 点）

(1) あ : 配送に関する G 百貨店からのメールを装い, ランサムウェアを添付した標的型攻撃メールを W 社の配送管理課員宛てに送信する。

(2) い : 配送管理課員が添付ファイルを開き, 配送管理用 PC がランサムウェアに感染する。配送管理用 PC からアクセスできる S サービスの Z 情報が暗号化され, その前に窃取された Z 情報が W 社外の PC などに保存される。

う : 1, 2, 5, 9

え : (大) ・ 中 ・ 小

お : 高 ・ 中 ・ (低)

か : A ・ B ・ (C) ・ D

き : W 社で, メール SaaS の迷惑メールのブロックオプションを有効にし, 標的型攻撃に対する訓練を実施する。

設問 3（8 点:完答 4 点×2）

a : 1, 5, 10, 12

b : 1, 2, 3, 12

以上