令和５年度秋期　情報処理安全確保支援士　午後試験　解答速報

（株）アイテック　IT 人材教育研究部　2023.10.12 発表

問１　Web アプリケーションプログラムの開発

【解答例】

［設問１］

(1) イ

(2) レビューページに出力する要素にエスケープ処理を施す。

［設問２］

コメント記法を用いて，分割入力したスクリプトをレビューの表示時に一つのスクリプトとして形成させる。

［設問３］

(1) 読み込んだ cookie の内容をアイコン画像のファイルコンテンツとして，取得したトークンの値と合わせてアップロードする。

(2) レビューページに表示されるアイコン画像ファイルをダウンロードし，ファイル内の文字列から抽出する。

(3) 当該 cookie が払い出された会員になりすまして EC サイトを利用する。

［設問４］

Same Origin Policy の制限でレスポンスの内容を取得できない。

問２　セキュリティ対策の見直し

【解答例】

［設問１］

(1) a：利用者 ID　　b：パスワード　（順不同）

(2) c：このサーバ証明書の発行元は，信頼された認証局として登録されていない。
　　d：このサーバ証明書のサブジェクト代替名は，接続先の FQDN と一致しない。
　　（順不同）

(3) スキームを https:に変更してアクセスするので，接続先のサーバからサーバ証明書を受け取り，それを検証する。

［設問２］

(1) 外部の共有者のメールアドレスとして，従業員自身のメールアドレスを入力する。

(2) e：MAC アドレス

［設問３］

(1) RADIUS

(2) f：秘密鍵

(3) g：従業員がエクスポートできないように

(4) 秘密鍵は TPM の内部で生成され，外部から読み出すことができないから。

(5) フィルタリング設定の項番 1 の NAT について，送信元 IP アドレスを a1.b1.c1.d1 とは別のグローバル IP アドレスに変換する。

(6) h：DNS

(7) 表 3：1
表 4：1，4

問３　継続的インテグレーションサービスのセキュリティ

【解答例】

［設問１］

ウ，エ

［設問２］

(1) U さんが偽サイトに入力した認証情報と TOTP をそのまま用いて，クラウド管理サイトにログインする。

(2) ア

(3) イ

(4) フロントエンドの API を用いて取得後，被害バックエンドに送信する。

(5) 利用者がアクセスしたサイトと正規サイトのオリジンが一致することを検証する。

(6) ア

［設問３］

(1) P アプリを装った，コード署名付きの不正アプリを J ストアにアップロードする。

(2) J 社の Web サイトから削除する。

(3) オペレータの認証が行われる。

(4) 影響：P アプリが起動されなくなる。
対応：P アプリをアップデートする。

問４　リスクアセスメント

【解答例】

［設問１］

ア：8，10，11，12，13

イ：大

ウ：C

エ：G 百貨店で，S サービスの設定を変更し，貸与アカウントについて W 社の本社事務所の IP アドレスからのログインだけを許可する。

［設問２］

(1) あ：G 百貨店から W 社への特別な連絡事項を装うメールによって，配送管理用 PC に二重脅迫型ランサムウェアを送り込む。

(2) い：二重脅迫型ランサムウェアが，配送管理用 PC において一括出力機能を利用して書き出された Z 情報のファイルを取得し，W 社外に送信する。身代金の支払いに応じない場合，さらなる脅迫のために，窃取された Z 情報がリークサイト上に公開される。

う：2，3，4，5，6，9，10

え：大

お：低

か：C

き：リスク番号 1-4 の管理策に加えて，標的型攻撃に関する訓練を定期的に実施する。

［設問３］

a：4，5，6，10，12，13

b：2，3，4，6

以上