令和６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　2024.10.17 発表

問１　インシデントレスポンス

【解答例】

［設問１］

(1) a：PC-C

(2) b：filesv

(3) c：ad01¥user019

(4) d：無効化

(5) URL フィルタリング機能の管理者拒否リストに https://△△△.com/及び https://□□□.com/を設定する。

(6) 全てのホストを対象に https://△△△.com/，https://○○○.com/及び https://□□□.com/への通信有無を確認する。

(7) F ツールの出力ファイルの srv.csv について，タスク名 install の登録の有無を確認する。

(8) ①L 社内ホストの全てを対象として，F ツールの出力ファイルに記載される内容と同等の情報を自動的に収集及び一元管理する仕組み

②一元管理された情報から，特定のタスクの登録や実行，マルウェア対策ソフトの停止，RDP 接続などの指定条件に合致する内容を自動的に抽出する仕組み

［設問２］

e：仮想環境の設定により，仮想 PC からほかの仮想 PC への RDP 接続を禁止する。

f：通信の監視制御機能により，RAR 形式のファイルのアップロードを禁止する。

問２　ドメイン名変更

【解答例】

［設問１］

(1) a：A 社ドメイン名

(2) b：全て

［設問２］

c：SMTPS

［設問３］

(1) エ

(2) d：イ

［設問４］

(1) 顧客に提供しているプログラムを装ってマルウェアをダウンロードさせる。

(2) メール：システムの変更に伴うパスワードの再登録依頼と登録用 URL を通知する。

攻撃　：URL を罠サイト，並びに宛先メールアドレスを Z 社ドメインに変更したメールを送信する。

(3) e：ア

［設問５］

(1) SPF レコードの許可する IP アドレスに T サービスの IP アドレスを追加する。

(2) SPF　：エンベロープ FROM には Z 社ドメインが設定されるが，SPF レコードでは Y サービスの IP アドレスを許可していないから。

DKIM：DKIM レコードの h タグに Subject ヘッダーが含まれ，メールの通番情報の付加により署名検証に失敗するから。

問３　クレジットカード情報の漏えい

【解答例】

［設問１］

a：5

b：XSS　又は　クロスサイトスクリプティング

c：格納

d：2

e：SQL インジェクション

［設問２］

(1)

(2) パラメータ：order[Payment]

値：1

(3) 書き換えたフォームの要素を取得後，フォームの送信時にカード番号，有効期限の月/年，名義，セキュリティコードの値を変数に格納し，攻撃者のサーバの URL クエリ文字列に設定して GET メソッドで送信する。

［設問３］

(1) アクセスログに記録されたリクエスト行のクエリ文字列から取得する。

(2) f：配送先・支払方法選択画面へのアクセスのあったアカウント名

問４　セキュリティ診断

【解答例】

［設問１］

(1) a：（イ）

(2) b：https://test.△△△.jp/

(3) c：手順 6 のメール受信者が利用者 ID と PW を入力するログイン操作

(4) d：ログイン前の sessionID の値と異なる sessionID の値を新たに生成し，hidden フィールドにセットする。

(5) e：M サイトへの通信を HTTPS に限定できる。

f：Web ブラウザのコンテンツの処理を，Web アプリが指定した MIME タイプの範囲内の解釈に限定できる。

［設問２］

g：画面 09 で図 B の手順 1 と同様の方法により攻撃者のメールアドレスを To:ヘッダーに指定した会社名に変更する。

h：画面 07 まで遷移し，再設定した PW を入力して APIkey を取得する。

［設問３］

i：求職者情報を取得する機能について，対象の求職者 ID を当該求人企業宛てに問合せ又は応募があった求職者に限定する。

j：任意の求職者 ID を指定可能な仕様では，推測した求職者 ID の指定により利用契約の範囲を超えた求職者情報を取得できるから。

k：ログイン画面の認証機能について，PW 認証から，フィッシング耐性をもつ認証方式に移行する。

l：昨今の脅威動向と取り扱う個人情報の特性を考慮すると，十分な認証方式の導入によるリスクの低減が不可欠といえるから。