令和６年度春期　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　2024.4.24 発表

問１　API セキュリティ

【解答例】

［設問１］

a：ステートレス

［設問２］

(1) b：500

(2) データ：JWT のヘッダ及びペイロード

内容　：指定されたアルゴリズムによる署名の検証

(3) パラメータ mid と JWT のペイロード中の利用者 ID の一致を確認する処理

(4) c：サービス L

(5) d：連続の検証失敗がしきい値を超えた場合のアカウントロック

［設問３］

(1) S システムから GET リクエストを受信したことを検出する仕組み

(2) e：Header　　f：Header

(3) ¥Wj|Jn|Nd|Di|I¥W

(4) 利点：過検知による正常なリクエストの遮断を防ぐ。

内容：アラート受信時の対応手順と体制を準備する。

問２　サイバー攻撃への対策

【解答例】

［設問１］

(1) a：公開 Web サーバ，取引先向け Web サーバを攻撃対象に，HTTP GET リクエストを大量に送り付ける。

(2) 攻撃ではない正常な通信を異常として検知する。

(3) b：DNS-K　　c：DNS-F

［設問２］

(1) d：攻撃者が，VPN クライアントソフトウェアを導入した PC で VPN-H に接続し，窃取した正規利用者の利用者 ID とパスワードを VPN ダイアログに入力する。

e：攻撃者が，正規利用者に罠の Web サイトのセキュリティコード入力画面に入力させたセキュリティコードを窃取し，VPN-H のセキュリティコード入力画面に入

力する。

(2) 受信したメールに記載されている Web サイトへの URL リンクをクリックして表示された画面では，秘密にすべきパスワードなどの認証情報を入力しないこと

［設問３］

(1) 接続が許可されるまでのポートへの通信要求を順番に試す。

(2) SPA パケットは再使用すると破棄され，盗聴による偽造もできないから。

［設問４］

(1) クラウド型の DDoS 対策サービス

(2) 取引専用 PC 以外からの通信パケットは取引先向け Web サーバに到達しないから。

問３　Web セキュリティ

【解答例】

［設問１］

(1) 9

(2) 問合せ機能の name パラメータとして画面の出力情報を読み取り，外部へ送信するスクリプトを DB サーバに格納させる。次に，D 社管理者が問合せ管理機能を使用した際にスクリプトを実行させて取得する。

［設問２］

(1) 攻撃者が会員機能（編集）で取得した csrf_token の値を含む，会員機能（編集）のリクエストを送信するスクリプトを攻撃サイトに用意する。次に，攻撃サイトに誘導した利用者にスクリプトを実行させる。

(2) a：×　　b：×　　c：○　　d：×

［設問３］

(1) 注文管理番号の英大文字 6 桁を改変する総当たり攻撃

(2) 注文管理番号の値から特定される利用者と，セッションオブジェクトから特定される利用者が一致することを確認する処理

［設問４］

(1) サーバ側から送信されるリクエストのメソッドが決定済みだから。

(2) パラメータの値を，IMDS のクレデンシャル情報を返す URL に変更する。

(3) Web サーバ Y からトークンを発行する URL へ PUT メソッドでアクセスさせる。次に，Web サーバ Y からクレデンシャル情報を返す URL へ，入手したトークンをヘッダに含むリクエストでアクセスさせる。

(4) サイト P へアクセスする URL の FQDN を固定とする処理

問４　Web アプリケーションプログラム

【解答例】

［設問１］

(1) a：ア

(2) b：personal

(3) c：4

［設問２］

(1) d：5

(2) e：チェック例外

(3) システム運用担当者

アクセスできてしまう情報：氏名，住所，電話番号，メールアドレス

出力される場所：エ

システム開発者

アクセスできてしまう情報：氏名，住所，電話番号，メールアドレス

出力される場所：オ

(4) f：SHA-256

(5) g：プログラムを異常終了させる。

(6) h：finally

(7) ア

以上