TAC

令和6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】

問 1 （配点 50 点）

設問 1 （3 点）

a ： ステートレス

設問 2 （22 点：(1)3 点，(2)（データ）3 点，（内容）3 点，(3)5 点，(4)3 点，(5)5 点）

(1) b ： 500

(2) （データ） JWT のヘッダ内の"alg"の値

（内容） 許可された署名アルゴリズムであること

(3) 利用者 API の呼出しに対して，mid の値と JWT 内の利用者 ID の一致を確認する。

(4) c ： 共通モジュール P

(5) d ： otp による認証に一定回数失敗したらアカウントロックする機能

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

(1) テストサーバの index.html のダウンロードログを得られる仕組み

(2) e ： Header

f ： Header

(3) ¥W[jJ][nN][dD][iI]¥W

（別解） ¥W(j|J)(n|N)(d|D)(i|I)¥W

(4) （利点） 誤検知によって正常な通信が遮断されることを防げる。

（内容） 検知アラート発生時に，即座に攻撃か確認し対応する。

問 2 （配点 50 点）

設問 1 （16 点：(1)5 点，(2)5 点，(3)3 点×2）

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

(2) 単なるアクセスの集中を不正アクセスとして遮断する。

(3) b ： DNS-K

c ： DNS-F

設問 2 （15 点：(1)5 点×2，(2)5 点）

(1) d ： 攻撃者は入手した利用者 ID とパスワードを VPN-H に入力し，罠の Web サイトにセキュリティコード入力画面を表示する。

e ： その入力画面で，VPN-H から送信されたセキュリティコードを正規利用者に入力させられれば，攻撃者は入手したコードを VPN-H に入力して VPN 接続を確立する。

(2) 受信メール内の URL リンクから接続したサイトで認証情報を入力してはならない。

設問 3 （10 点：(1)5 点，(2)5 点）

（1） パケットの盗聴で入手した順番とポート番号で接続する。

（2） ワンタイムパスワードでの送信元認証の突破や盗聴パケットの再利用はできないから

設問 4 （9 点：(1)4 点，(2)5 点）

（1） コンテンツデリバリーネットワークサービス （CDN サービス）

（2） 取引先向け Web サーバには，取引専用 PC からの VPN 接続のみ許可されるから

問 3 （配点 50 点）

設問 1 （9 点：(1)3 点，(2)6 点）

（1） 9

（2） 管理者用の利用者アカウントの SESSIONID を窃取して管理者としてサイト X に接続し，会員管理機能を利用して利用者情報を取得する。

設問 2 （10 点：(1)6 点，(2)1 点×4）

（1） 攻撃者が予め取得した有効な csrf_token を含む悪意のある会員機能（編集）リクエストを行う罠サイトを用意し，サイト X 利用中の利用者にアクセスさせるように誘導して，そのリクエストを送信させる。

（2） a ： ×

b ： ×

c ： ○

d ： ×

設問 3 （10 点：(1)4 点，(2)6 点）

（1） 注文管理番号のランダムな英大文字列に対して総当たり攻撃する。

（2） リクエストで指定された注文管理番号に紐付いた利用者 ID がログイン中の利用者 ID と一致しない場合，エラーで中断する処理

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

（1） CMS の管理画面での管理ログインは GET メソッドでは許可されないから

（2） リクエストの page パラメータの値にクラウド W の IMDS のクレデンシャル情報を返す URL を設定する。

（3） IMDS のトークンを発行する URL に対して PUT メソッドでアクセスし，入手したトークンをリクエストヘッダに含めてクレデンシャル情報を返す URL にアクセスする。

（4） リクエストのパラメータの値に不正な URL が設定されていないか検証する。

問 4 （配点 50 点）

設問 1 （10 点：(1)3 点，(2)4 点，(3)3 点）

（1） a ： ア

（2） b ： personal

（3） c ： 4

設問 2 （40 点：(1)3 点，(2)4 点，(3)システム運用担当者（アクセスできてしまう情報）完答で 5 点，
（出力される場所）3 点，システム開発者（アクセスできてしまう情報）完答で 5 点，
（出力される場所）3 点，(4)4 点，(5)5 点，(6)4 点，(7)4 点）

（1） d ： 5

（2） e ： NoSuchAlgorithmException

(3) (システム運用担当者)

(アクセスできてしまう情報) パスワード, 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) パスワード, 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 : ユーザー登録処理を終了する。

(6) h : finally

(7) ア

以上