TAC

令和4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　Ⅰ】

問 1 （配点 50 点）

設問 1 （15 点：(1)5 点，(2)5 点，(3)5 点）

(1) ア

(2) プレースホルダ

(3) a ： 改行コード

設問 2 （28 点：(1)10 点，(2)8 点，(3)5 点，(4)5 点）

(1) GET リクエストのクエリ文字列中のプロジェクト ID を書き換えて送信する。

(2) 利用者 ID に紐づけられたプロジェクト ID を取得するから

(3) b ： ウ

(4) c ： stmt

設問 3 （7 点）

d ： プロジェクト ID = ? AND 情報番号 = ?

問 2 （配点 50 点）

設問 1 （16 点：(1)2 点×2，(2)6 点，(3)6 点）

(1) a ： ア

b ： エ

(2) 外部から認証なしでルータの設定を変更されてしまう。

(3) 通常はアクセスできない/root ディレクトリ配下のファイルも暗号化されていたから

設問 2 （16 点：(1)5 点，(2)5 点，(3)2 点×3）

(1) c ： ディレクトリトラバーサル　　（別解）パストラバーサル

(2) d ： OS コマンドインジェクション

(3) e ： ア

f ： ウ

g ： イ

設問 3 （13 点：(1)6 点，(2)7 点）

(1) POST メソッドではパラメタが URL に含まれず，ログに残らないから

(2) sudo コマンド設定ファイルで tar コマンドの OS コマンド実行オプションまで指定し，その使用を禁じる。

設問 4 （5 点）

h ： noindex

問 3 （配点 50 点）

設問 1 （4 点:2 点×2）

a ： イ

b ： ア

設問 2 （34 点:(1)6 点×2, (2)4 点, (3)2 点×2, (4)6 点, (5)8 点）

(1) ① フィッシング等で不正入手した口座番号と暗証番号を用いる。

② 入手できた口座個人情報とそれに基づき推定した暗証番号を用いる。

（別解） ・ありがちな暗証番号に対し，口座番号を 4 回変える試行を繰り返す。

・口座番号と暗証番号の組合せを 4 回まで変える試行を繰り返す。

(2) c ： 写真

(3) d ： ウ

e ： イ

(4) f ： 署名用電子証明書の有効性

(5) g ： 一定時間内に当該数字を記した紙と一緒に容貌や本人確認書類を撮影

設問 3 （12 点:(1)6 点, (2)6 点）

(1) 他人がスマートフォンを勝手に使える場合

（別解） スマートフォンを放置または紛失した場合

(2) 重要な操作の前にスマートフォンによる生体認証を行う機能

【午　後　Ⅱ】

問 1 （配点 100 点）

設問 1 （12 点：(1)4 点，(2)8 点）

（1） ア

（2） 使用するライブラリのアップデートを常時確認し，最新版を用いる体制をとる。

設問 2 （10 点：5 点×2）

a ： 利用者　 b ： セッション （a と b は順不同）

設問 3 （26 点：(1)3 点×6，(2)4 点×2）

（1） c ： イ
d ： ア
e ： ア
f ： ア
g ： イ
h ： イ

（2） i ： エ
j ： イ

設問 4 （6 点）

topic パラメタの値を https://db-y.b-sha.co.jp/に変更した。

設問 5 （12 点：(1)6 点，(2)6 点）

（1） k ： V 氏が用意したサイト

（2） returnURL の値をサイト Z の URL に固定する。

設問 6 （34 点：(1)6 点×2，(2)6 点，(3)8 点，(4)8 点）

（1） ① セッション管理の脆弱性
② 認可・アクセス制御の脆弱性

（2） 改良フェーズの1か月の休止期間の時期

（3） 大規模な改修の際のテストと並行して専門技術者による脆弱性診断の実施を組み込む。

（4） 推測困難なトークンを生成して入力フォームに埋め込み，そのリクエスト処理時にトークンを照合し，正当性を検証する。

問 2 （配点 100 点）

設問 1 （23 点：(1)4 点，(2)4 点，(3)4 点，(4)6 点，(5)5 点）

（1） a ： キャッシュ

（2） b ： DDoS

（3） c ： Host

（4） Y-CDN-U-FQDN を名前解決した IP アドレスのサーバにコンテンツを配置している Web サイト

（5） d ： TLS の接続先サーバ名

設問 2 （12 点：(1)6 点，(2)6 点）

（1） ST は認証サーバの検証なしにアクセス対象サーバに送られるから

（2） ST に対する総当たり攻撃はオフラインで行われ，サーバとは通信しないから

設問 3 （19 点：(1)3 点，(2)3 点，(3)4 点，(4)3 点×3）

（1） e ： ウ

(2) f : ア
(3) g : 改ざん
(4) h : 1
i : 3
j : 4　(iとjは順不同)

設問4 (21点:(1)3点×3, (2)3点, (3)3点×2, (4)3点)

(1) k : ウ
l : イ
m : ア
(2) n : エ
(3) o : (2)
p : (6)
(4) q : ウ

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

(1) r : オ
s : エ
t : ウ
(2) u : (8)
(3) v : イ
(4) w : 認証要求
x : IDトークン

以上