TAC

平成28年度秋期 情報処理技術者試験

情報セキュリティスペシャリスト 解答例

【午 後 Ⅰ】

問 1 （配点 50 点）

設問 1 （8 点:4 点×2）

a : エ

b : ア

設問 2 （14 点:(1)4 点×2, (2)6 点）

(1) c : x1.x2.x3.x4

d : y1.y2.y3.y4

(2) 認証方式をパスワード認証方式から公開鍵認証方式に設定変更した。

設問 3 （28 点:(1)5 点, (2)5 点, (3)(イメージファイルの作成時)6 点, (イメージファイルの更新時)6 点, (4)6 点）

(1) e : 監視端末の IP アドレス以外は SSH サービスへのアクセスを遮断

(2) 同一モデル機器でなりすまし接続する。

(3) (イメージファイルの作成時) イメージファイルのハッシュ値を作成者の秘密鍵で暗号化して署名しておく。
(イメージファイルの更新時) 作成者の公開鍵で署名を復号し, イメージファイルのハッシュ値と照合する。

(4) ファームウェアの更新機能が更新用に保持する復号鍵を解析して入手する。

問 2 （配点 50 点）

設問 1 （12 点:3 点×4）

a : ア

b : イ

c : ウ

d : エ

設問 2 （12 点:(1)6 点, (2)6 点）

(1) 関数の呼び出し元へのリターンアドレス

(2) ア : sample2

設問 3 （12 点:(1)4 点, (2)4 点, (3)4 点）

(1) ウ

(2) 23

(3) オ

設問 4 （14 点:(1)8 点, (2)6 点）

(1) ヒープ領域の管理方法によっては, uid をあふれさせても pass を上書きしないから
(別解) メモリ空間中のデータ領域がランダムに配置される実行環境では攻撃が成立しないから

(2) データ領域で機械語コードを実行させる攻撃には該当しないから

問 3 （配点 50 点）

設問 1 （4 点:4 点）

a : エ

設問 2 （12 点:(1)3 点×2, (2)6 点）

(1) b : イ

c : オ

(2) 攻撃用プログラムのプログラム名やコード内容が変異する場合

設問 3 （10 点:(1)6 点, (2)4 点）

(1) プロキシ 2 のログでは, プロキシ 1 が送信元アドレスとなるから

(2) d : オ

設問 4 （24 点:(1)8 点, (2)(URL フィルタリング機能)8 点, (カテゴリ単位フィルタリング機能)8 点）

(1) プロキシ認証のためのユーザ ID や認証情報を, 盗聴やキーロガーなどの手段で不正に取得し, 再使用する。

(2) (URL フィルタリング機能) 業務に必要かつ安全であることを確認した URL をホワイトリストに登録する。
(カテゴリ単位フィルタリング機能) 業務に不要と思われるカテゴリを“遮断”に設定する。

【午　後　Ⅱ】

問 1 （配点 100 点）

設問 1 （36 点：(1)2 点×5，(2)6 点，(3)2 点×3，(4)6 点（全一致で得点），(5)2 点×4）

(1) a ： ウ
b ： オ
c ： ス
k ： エ
l ： イ

(2) 認証カードを他人に貸したり，認証カードの PIN を他人に開示する。

(3) d ： ウ
e ： カ
f ： ク

(4) ア，イ，エ，キ，ク，ケ

(5) g ： イ
h ： オ
i ： ア
j ： セ

設問 2 （26 点：(1)6 点×2，(2)2 点，(3)（改善すべき不備）8 点，（失効事由の値）2 点×2）

(1) ① いずれかの事業用システムを業務上利用する必要がある者であるか
② グループ従業員であれば，認証カードが既に発行済みであるか

(2) ア

(3) （改善すべき不備） 受付サーバで失効の申請を受け付けてから 1 営業日以内に失効情報が開示されていない。
（失効事由の値） ア，ウ

設問 3 （14 点：(1)6 点，(2)8 点）

(1) サーバ証明書の信頼性を PC が確認できず，警告が発せられる。

(2) D 社の認証局が不正操作され不正なサーバ証明書が発行された場合，それを信頼して接続してしまう。

設問 4 （24 点：(1)6 点，(2)6 点×2，(3)6 点）

(1) 認証されても，利用権限の認可はプロジェクトへの参加期間だけ有効となるから

(2) ① 認証カードの貸与対象者への配布と回収について，事業部門の管理工数が少ないから
② 認証カードの作成や失効などの管理について，システム部の管理工数が少ないから

(3) 認証カードは入退室に必須となり，現場事務所内での貸借の動機が薄れ，保管もできない。

問 2 （配点 100 点）

設問 1 （13 点：(1)3 点，(2)10 点）

(1) ウ

(2) 公表された脆弱性を持つソフトウェアのバージョンを導入している A 社の機器を迅速に特定するため

設問 2 （18 点：(1)3 点，(2)3 点，(3)6 点，(4)6 点）

(1) ウ

（2） ウ

（3） a ： HTTP リクエスト

（4） (){:;};/usr/bin/cat /etc/passwd

（別解） (){echo test;}; /usr/bin/cat /etc/passwd など

設問 3 （27 点：(1)5 点，(2)8 点，(3)3 点×2，(4)8 点）

（1） b ： パターンマッチング

（2） シグネチャ登録による対応では脆弱性対策による影響を検証する作業の必要がないから

（3） c ： ウ

d ： イ

（4） Web サーバの通信量の変動に応じ，サービス利用契約を随時変更し，WAF の通信量の上限を切り替えられる。

設問 4 （21 点：(1)6 点，(2)3 点×3，(3)6 点）

（1） f ： 社内 Web サーバの Web アプリの URL

（2） e ： オ

g ： ア

h ： キ

（3） HTTP リクエストを送信できるコマンド

設問 5 （21 点：(1)3 点，(2)3 点×2，(3)6 点×2）

（1） i ： 中

（2） ア，ク

（3） j ： 社外から不正アクセスされる

k ： 重要情報が社外に漏えいする

（注 ： j，k は順不同）

以上