TAC

令和4年度秋期　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（26 点：(1)5 点，(2)4 点，(3)6 点，(4)6 点，(5)5 点）

(1) a ： DNS キャッシュポイズニング

(2) b ： エ

(3) 攻撃者の DNS 応答が正当な DNS 応答より先に到達すること

(4) サーバ証明書を検証し，正当性を確認できなかった場合はアクセスを行わない。

(5) c ： コード署名

設問 2（5 点）

d： POST リクエストのパラメータを検証せずにコマンド文字列を生成して

設問 3（11 点：(1)6 点，(2)5 点）

(1) 罠サイト中に図 6 のリクエストを行うフォームを偽装して埋め込み，利用者が閲覧した際に自動で送信する。

(2) e ： 推測が困難で毎回異なる

設問 4（8 点：4 点×2）

（脆弱性 A）ア

（脆弱性 B）オ

問 2（配点 50 点）

設問 1（3 点）

a ： a3.b3.c3.d3

設問 2（26 点：(1)6 点，(2)4 点×5）

(1) run プロセスの親プロセスが T ソフトの BSoftMain プロセスだから

(2) b ： 13:04:32

c ： 13:05:50

d ： a8.b8.c8.d8

e ： LDAP

f ： JExp

設問 3（12 点：(1)6 点，(2)6 点）

(1) ログ出力処理は認証前のアクセスでも行われ，攻撃文字列を含ませることができるから

(2) 会員サーバからインターネットへの LDAP 通信は FW で拒否されるから

設問 4（9 点：3 点×3）

g ： 予約サーバ

h ： SNS 投稿用のサーバ

i ： 全て

問 3（配点 50 点）

設問 1（20 点：(1)4 点，(2)6 点，(3)5 点，(4)5 点）

(1) a ： 376

(2) prog プロセスの実行ファイルをダウンロードして実行する。

(3) b ： 一時ディレクトリ内のファイル

(4) ゼロデイ攻撃

設問 2（12 点：(1)6 点，(2)6 点）

(1) ステータスが 404 Not Found であること

(2) ソースコードサーバからゲームイメージを再登録する。

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

(1) c ： a3.b3.c3.d3

(2) d ： エ

(3) 攻撃者のサーバの IP アドレスが変更された場合

(4) e ： オ

【午　後　Ⅱ】

問 1 （配点 100 点）

設問 1 （16 点：(1)4 点，(2)6 点，(3)6 点）

(1) エ

(2) C&C サーバの IP アドレス

(3) 検体γが通常の動作をする物理環境

設問 2 （12 点：3 点×4）

a ： ア

b ： ウ

c ： エ

d ： イ

設問 3 （33 点：(1)3 点，(2)3 点×4，(3)3 点×6）

(1) e ： 1

(2) f ： ア

g ： イ

h ： ウ

i ： ウ

(3) j ： ア

k ： ウ

l ： ウ

m ： イ

n ： ウ

o ： ア

設問 4 （25 点：(1)7 点，(2)7 点，(3)4 点，(4)7 点）

(1) ハッシュ関数を繰り返し適用する。

(2) 5 回連続してログインに失敗した利用者 ID によるログインを 10 分間ロックする機能

(3) p ： エ

(4) 数値 n の左に 0 を詰めて 5 桁で表したものを"Admin"の後ろに連結した文字列

設問 5 （14 点：(1)7 点，(2)7 点）

(1) 異なる IP アドレスに同じ MAC アドレスが対応付けられた状態

(2) q ： ログに出力する情報には認証情報を含めないこと

問 2 （配点 100 点）

設問 1 （12 点：6 点×2）

① ： メールフォルダ内の何らかのファイルが読み込まれた。

② ： 何らかのファイルが特定の URL にアップロードされた。

設問 2 （30 点：(1)5 点×5，(2)完答 5 点）

(1) a ： 15:03

b ： PC1

c ： file1.v

d ： file2.v

e ： PC2

(2) ア, ウ, エ, オ, キ

設問 3 (7 点)

何らかのファイルが読み込まれた後, 1 分以内に, 同じ種別の別ファイルの読込みとそのファイルへの書込みが順に行われた。

設問 4 (32 点:(1)4 点×2, (2)4 点, (3)4 点×2, (4)4 点×3)

(1) f ： 添付ファイルの名称

g ： 添付ファイルのサイズ

(2) h ： ファイルサイズ

(3) i ： アップロードされたファイルのサイズ

j ： アクセス先の URL

(4) k ： ファイルの圧縮

l ： ファイル名

m ： ファイルサイズ

設問 5 (7 点)

情報システム課が管理していない USB-ID の USB メモリが装着され, 何らかのファイルがその USB メモリに書き込まれた。

設問 6 (12 点:6 点×2)

n ： 取引先に通報窓口を公開し, 取引先が直接通報できるようにする。

o ： インシデント対応支援サービスによる調査の中間報告後に再度レベル判定を行い, 体制のとり方を見直す。

以上