TAC

平成29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 （3 点）

イ

設問 2 （25 点：(1)3 点×2，(2)4 点，(3)（営業用 PC の設定）5 点，（ランサムウェア X の特徴）5 点，(4)5 点）

(1) a ： オ

b ： エ

(2) バックアップの終了の時刻

(3) （営業用 PC の設定） D サーバ上の共有フォルダが PC の D ドライブとして自動的に割り当てられる。

（ランサムウェア X の特徴） ネットワークドライブを含むアクセス可能なドライブを探し出す機能がある。

(4) D サーバと G サーバの共有フォルダのファイルの暗号化

設問 3 （16 点：(1)1 点×6，(2)5 点，(3)5 点）

(1) c ： 可

d ： 可

e ： 可

f ： 不可

g ： 可

h ： 不可

(2) 検体解析で公開鍵を入手しても，暗号化共通鍵は復号できないから

(3) 暗号化に使用したメモリ上の共通鍵がシャットダウンすると消去されるから

設問 4 （6 点）

ローカルディスク上のバックアップデータなど一般利用者権限で扱えない対象の暗号化

問 2 （配点 50 点）

設問 1 （18 点：(1)2 点×2，（必要な全てのコードの並び）全ての一致で 5 点，(2)2 点×3，(3)3 点）

(1) ア ： 9

イ ： 11

（必要な全てのコードの並び） カ，ア，イ，ウ

(2) 21，22，23

(3) ウ

設問 2 （12 点：(1)3 点×2，(2)6 点）

(1) a ： エ

b ： イ

(2) ドメイン名が w-system.a-sha.jp であるリダイレクト先のみ許可する。

(別解) リダイレクト先の URL を W システムの 8 ページのものに限定して許可する。

設問 3 (20 点:(1)6 点, (2)6 点, (3)8 点)

(1) 本番環境でのセキュリティ検査の実施を検査手順に追加する。

(2) XSS フィルタ機能が検査用文字列を無効にする場合があるから

(3) 新たに発見された脆弱性など, 未対応の脆弱性を悪用した Web アプリケーションへの攻撃を受けるリスク

問 3 (配点 50 点)

設問 1 (16 点:(1)2 点×4, (2)6 点, (3)2 点)

(1) a : コ

b : カ

c : オ

d : イ

(2) C 社の EC サイトのドメインへのアクセスを偽の EC サイトへ誘導する役割を果たす。

(3) エ

設問 2 (17 点:(1)3 点×2, (2)4 点×2, (3)3 点)

(1) ア : 利用

イ : 失効

(2) ① 影響を受ける EC サイトの対象サービス内容

② 影響を受ける EC サイトの利用時期の情報

(3) e : 新しい鍵ペア

設問 3 (17 点:(1)5 点, (2)2 点×2, (3)2 点, (4)6 点)

(1) SSL 3.0 を無効とする設定に変更する。

(2) ウ, オ

(3) エ

(4) 運営者の実在性確認に基づく EC サイトの信頼性は得られず, 偽サイト構築も容易だから

【午　後　Ⅱ】

問 1（配点 100 点）

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

（1） a ：ポートスキャン

（2）（開いている場合） カ

（閉じている場合） エ

（3） b ： HTTP を用いて C&C サーバと通信し，ボットとして活動

（4） デバッグ用プログラムとその起動スクリプトを除去したファームウェアをカメラ IF から Z カメラに配信できるようにしておく。

設問 2（15 点：(1)3 点×2，(2)3 点，(3)6 点）

（1） c ： カ

d ： ア

（2） e ： TLS

（3） サーバ証明書の違いによる動作の違いを検証できなくなるから

設問 3（64 点：(1)4 点，(2)5 点（全一致で得点），(3)6 点，(4)6 点，(5)6 点，(6)6 点，(7)6 点，(8)6 点，(9)6 点，(10)3 点，3 点，3 点，4 点）

（1） 管理用モバイル端末を Z アプリの UUID で認証する。

（別解） クライアント証明書で管理用端末の認証を行う。

（2） f ： A2，C1，C2，D1，D2

（3） パスワードを固定し，可能性のある利用者 ID について順々にログインを試みる。

（4） 認証に失敗しても，異なる利用者 ID に対してはログイン制限の仕組みが機能しないから

（5） 利用者 ID とパスワード以外の利用者情報も一緒に漏えいし，攻撃用リストとして作成され使用されている場合

（6） 登録時に付与された利用者番号も認証時に入力させる。

（7） 一定期間内の認証失敗の回数が事前に決めたしきい値を超えた場合

（8） セキュリティ要件の性能保証条項及び瑕疵担保責任条項

（9） 脆弱性を持つ構成要素がシステム基盤上に存在するかすぐに洗い出せず，対応が遅れる。

（10）（共通鍵の生成を行う Z システムの構成要素） Z アプリ

（動画の暗号化を行う Z システムの構成要素） Z カメラ

（動画の復号を行う Z システムの構成要素） Z アプリ

（共通鍵の安全な共有方法） Web サーバとの HTTPS 通信を介して受け渡す。

問 2（配点 100 点）

設問 1（21 点：(1)4 点×2，(2)5 点，(3)8 点）

（1） a ： FISC

b ： CRYPTREC

（2） 162 台

（3） オペレータ及びシステム管理者が，契約情報の復号に用いる鍵が保存されているファイルから復号鍵を取得し，契約情報を復号する。

設問 2 （41 点：(1)4 点，(2)6 点，(3)（場合）5 点，（目的）5 点，(4)5 点，(5)（事象）8 点，（機能）8 点）

（1） c ： FIPS

（2） 3 人いないとマスタ鍵が生成できず，不正が抑止できる。

（3）（場合） 故障などで製品 H を交換する場合

（別解） 製品 H の内蔵バッテリを交換する。

（目的） 同じマスタ鍵を再生成する。

（4） 耐タンパ性

（5）（事象） 製品 H の運搬中に生じた静電気によって，規定の範囲を超える電源電圧が発生する。

（機能） メモリ上のマスタ鍵をゼロ化し，製品を使用不能にして元に戻せない状態にする機能

設問 3 （22 点：(1)（手順）4 点，（API-X のコマンド）5 点，（API-X のエラーの原因）5 点，(2)8 点）

（1）（手順）（ v ）

（API-X のコマンド） 暗号化（DB データ鍵，DB マスタ鍵 ID）

（API-X のエラーの原因） DBαの DB マスタ鍵 ID とは異なる鍵 ID が表領域作成で使用されている。

（別解） 鍵ストアファイルにない DB マスタ鍵 ID で DB データ鍵の暗号化を試みた。

（2） データ鍵 ID を 0 から順番に採番した結果，偶然データ鍵 ID が同じ値になった場合

設問 4 （16 点：(1)8 点，(2)8 点）

（1） 業務アプリケーション管理者が業務アプリケーションを操作して契約情報を取得し漏えいするリスク

（別解） X 社従業員が業務アプリケーションを利用し，悪意をもって契約情報を取得して漏えいするリスク

（2） オペレータ及びシステム管理者がメモリダンプファイルから契約情報を復元して取得し漏えいするリスク

以上