TAC

令和7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　サプライチェーンのリスク対策（配点 50 点）

設問 1（8 点:(1)4 点, (2)4 点）

(1) 企画・設計など開発の初期段階からセキュリティを考慮して対策を組み込む考え方

(2) 再委託の際には業務委託先が同等のセキュリティ管理に関する要件を再委託先との契約に含め責任を負うこと

設問 2（13 点:(1)4 点, (2)4 点, (3)(項番)と(修正内容)ともに正解で 5 点）

(1) スクリプト P は, L 社が自社で管理運用するサーバ内に配置する。

(2) 古い Web ブラウザ対応のコードを削除し, 当該ブラウザでのアクセスを拒否する。

(3)（項番）1

（修正内容）システムで利用する外部のスクリプトやライブラリを, 一覧化すべき情報資産に加える。

設問 3（17 点:(1)2 点×4, (2)3 点×3）

(1) ア : 10　　イ : 4　　ウ : 5　　エ : 11

(2) a : 踏み台サーバへのログインは, 会社ごとに発行した共用アカウントで行われている。

b : 問題なし。

c : インシデント対応手順書は存在するが, 発生時の連絡フロー以外確認できていない。

設問 4（4 点）

構成要素のバージョンや依存関係が明確化し, 脆弱性の影響範囲を迅速に把握できるから

設問 5（8 点:(1)2 点, (2)3 点×2）

(1) d : 踏み台サーバ

(2)（あ）早期に脆弱性を発見し, 端末上で開発者が迅速に修正できる。

（い）複数の開発者による変更によって生じ得る脆弱性を全体的な検査で発見できる。

問 2　脆弱性管理（配点 50 点）

設問 1（5 点:1 点×5）

a : ア　　b : ア　　c : ア　　d : ア　　e : イ

設問 2（6 点:3 点×2）

f : 新規の脆弱性が発見されたこと

g : 診断ツール／脆弱性定義が更新されたこと（f と g は順不同）

設問 3（9 点:(1)2 点, (2)4 点, (3)3 点）

(1) ウ

(2) OpenSSH の認証試行のログを監視し, 認証タイムアウトのメッセージ出力が短時間に多数検知された場合にアラートをあげる。

(3) クライアント証明書による端末認証

設問 4 （10 点：(1)(WA-1)4 点，(WB-1)4 点，(2)2 点）

(1) （WA-1） リクエスト中のパラメータ item の値を変更するだけで容易に攻撃が成立する。

（WB-1） 管理者用アカウントでのみ確認できる管理者用画面の URL 取得が攻撃成立の条件となる。

(2) 3

設問 5 （12 点：(1)(現状値)3 点，(EPSS 値)3 点，(2)3 点，(3)3 点）

(1) （現状値） 利用者側が各環境に応じた脅威情報を収集し，評価値を自ら算出する必要があるから

（EPSS 値） 外部機関が統計的に算出して提供する評価値であり，利用者側で評価する必要がないから

(2) I ： EPSS 値更新のモニタリング

(3) P 社は脆弱性が実際に悪用できることを確認した上で報告するから

設問 6 （8 点：1 点×8）

m ： A　　n ： A　　o ： C　　p ： A　　q ： B　　r ： B　　s ： A　　t ： S

問 3 スマートフォン用アプリケーションプログラムの開発 （配点 50 点）

設問 1 （22 点：(1)6 点，(2)6 点，(3)6 点，(4)4 点）

(1) HTTP リクエストの Authorization ヘッダー中のアクセスキーを取得する。

(2) F アプリを解析し，リソースとして保存されている暗号化されたアクセスキーと，コード中に定数として定義されている共通鍵と初期ベクトルを取得し，復号してアクセスキーを取得する。

(3) アクセスキーを Authorization ヘッダーに指定し，ストレージ名と連番の写真ファイル名を順に変化させた GET リクエストを C サービスに繰り返し行う。

(4) https://www.a-sha.co.jp.k-sha.co.jp　（注:“https://”の部分は解答用紙に印字）

設問 2 （17 点：(1)3 点，(2)1 点×8，(3)6 点）

(1) www.a-sha.co.jp

(2) a ： オ　　b ： ケ　　c ： ウ　　d ： コ　　e ： ア　　f ： イ　　g ： カ　　h ： キ

(3) 通信解析ツールのプライベート認証局のルート証明書をインストールし，信頼する証明書として設定する。

設問 3 （3 点）

i ： (い)

設問 4 （8 点：(1)3 点，(2)5 点）

(1) アプリ画面に接続先 URL が表示されない。

(2) F アプリ内で URL に含まれるドメイン部分をチェックし，許可されたドメイン以外へのアクセスを禁止する。

問 4 IT 資産管理及び脆弱性管理 （配点 50 点）

設問 1 （5 点：(サーバ名)2 点，(変更内容)3 点）

（サーバ名） 権威 DNS サーバ

（変更内容） 使用していないサブドメインの DNS レコードを削除する。

設問 2 （16 点：(1)3 点×2，(2)2 点，(3)1 点×3，(4)1 点×5）

(1) a ： 他社データセンターを契約して利用している

b ： レンタルサービスを契約して利用している　（a と b は順不同）

(2) c ： WHOIS

(3) あ ： Z　　い ： X　　う ： Y

(4) d ： オ　　e ： ア　　f ： イ　　g ： ク　　h ： キ

設問 3 （12 点 ：(1)3 点, (2)3 点, (3)(する場合)3 点, (しない場合)3 点）

(1) 対象 GIP に対してポートスキャンを行い, 稼働サービスへのアクセスを試行する。

(2) Z サービスによる検索で得た応答メッセージ情報から利用 OS や SW の状況を確認する。

（別解） 対象資産に脆弱性スキャナーを使用して OS や SW のバージョンと脆弱性を確認する。

(3)（する場合） OS と SW のバージョンを最新にし, パッチを適用して脆弱性を解消する。

（しない場合） サーバを停止し, ドメイン登録の抹消や関連 DNS レコードの削除を行う。

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

(1) 4.0

(2) ウ

(3) 実際に悪用が確認されている。

(4)（項番 1） 一元管理した SW の脆弱性情報を情シ部がツールで自動収集し, 対策の優先度などの判断ルールに基づき脆弱性の重要度を判定する。

（項番 2） 情シ部が修正すべき脆弱性を選別し, 該当管理部門に通知して, 完了報告の義務を課す。

以上