TAC

平成26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 （12 点：4 点×3）

a：セキュリティパッチ

b：ヒープ

d：Return-to-libc

設問 2 （12 点：(1)4 点，(2)3 点，(3)5 点）

(1) スタック領域

(2) c：エ

(3) リターンアドレス格納位置を推測して不正に書き替える。

設問 3 （10 点：(1)5 点，(2)5 点）

(1) 設定したサイズ以上の HTTP リクエストを破棄する。

(2) プログラムがルート権限で動作している。

設問 4 （16 点：(1)6 点，(2)5 点，(3)5 点）

(1) 許可されていない一般利用者の権限ではアプリのデータを勝手に読み出しできない。

(2) 侵入したマルウェアによって勝手にルート特権化される。

(3) M システムの構成情報の管理機能で確認する。

問 2 （配点 50 点）

設問 1 （15 点：(1)2 点×2，(2)2 点×2，(3)(c)3 点，(要件)4 点）

(1) a：15,360

b：512

(2) 力，キ

(3) c：112

（要件） 2015 年 9 月から 10 年間稼働させる。

設問 2 （20 点：(1)5 点，(2)3 点×5）

(1) 対象端末の証明書を利用停止し，端末内データを完全に消去する。

(2) d：公開鍵

e：シリアル番号

f：受付拒否リスト

g：入力された利用者 ID

h：利用者 ID

設問 3 （15 点：(1)5 点，(2)5 点，(3)5 点）

（1） 代表者は担当者が代理店管轄下の登録端末に証明書をインストールしたことを確認する。

（2） i: 証明書の利用停止手順については，担当者ではなく代表者が行う。

（3） 提示された証明書の識別番号が受付拒否リストに登録されていないことを確認する。

問 3 （配点 50 点）

設問 1 （11 点：(1)5 点，(2)6 点）

（1） メールサーバ Z から M 社営業部員全員に自動送信されたメール

（2） 送信元メールサーバの IP アドレスのホワイトリストにメールサーバ Z の IP アドレスの許可指定を追加する。

設問 2 （15 点：(1)5 点，(2)4 点，(3)2 点×3）

（1） TCP ポート番号 8050 を使用した通信は FW で拒否されるから

（2） 顧客管理

（3） （メソッド） CONNECT

（ポート番号） 2560

（動作） 許可

設問 3 （10 点：(1)5 点，(2)5 点）

（1） L3SW のフィルタリングルールの項番 1 および項番 2 のルールを削除する。

（2） a：インターネットへのアクセスやメールの送受信

設問 4 （14 点：(1)2 点×4，(2)6 点）

（1） b: 7

c: 69[i]

d: 14

e: 95[i]

（2） ソルト値の違いにより同じパスワードでも異なるハッシュ値が生成されるから

【午　後　Ⅱ】

問 1 （配点 100 点）

設問 1 （18 点：(1)5 点×2，(2)8 点）

（1） a：認証 Cookie

b：アジアポータル

（2） 情報システム部に ID 登録を依頼した正社員及び契約社員の真正性を確認して承認する手順がない。

設問 2 （18 点：(1)6 点，(2)6 点，(3)6 点）

（1） 認証 Cookie を検証するためのエージェントを開発して組み込む。

（2） GDS と各地域の DS との間で信頼関係を結ぶ。

（3） 日本と欧米地域の ID 体系が同じで，重複している ID があること。

設問 3 （15 点：(1)6 点，(2)3 点×3）

（1） 人事システムからでは契約社員の情報が取得できない。

（2） ① 日本 DS

② 欧米 DS1

③ アジア DS

設問 4 （10 点：(地域)5 点，(サーバ名)5 点）

（地域） 日本

（サーバ名） 日本認証サーバ

設問 5 （24 点：(1)5 点×2，(2)6 点，(3)8 点）

（1） ① VPN パスワード

② OTP

（2） 日本 PC 専用に開発された IC カードリーダの動作検証

（3） 個人所有機器とシンクライアントサーバとの通信距離や経由回線の帯域逼迫によって，応答性能が確保できない。

設問 6 （15 点：(1)5 点，(2)((構成要素)と(設定内容)が共に正解で 5 点)×2）

（1） アジア地域

（2） ①（構成要素） アジア PC

（設定内容） SPNEGO の設定を行う。

②（構成要素） アジア認証サーバ

（設定内容） SPNEGO の設定を行う。

問 2 （配点 100 点）

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

（1） a：ウ

b：ク

（2） c：/GoodsDetail

d：goodsNo

（3） 攻撃が行われなかった残りの 3 画面の中にも脆弱性が存在する可能性があるから

（4） 攻撃の事実が判明した時点で直ちに A 社情報システム部に報告する。

設問 2 （22 点：(1)6 点，(2)8 点，(3)8 点）

（1） e：IPS， WAF などの外側

（2） f：それを利用した攻撃に用いるポートの通信がファイアウォールで遮断されている場合

（3） 脆弱性の修正に起因して新たな脆弱性が生じていないか確認する。

設問 3 （50 点：(1)4 点×2，(2)（診断方法）8 点，（理由）6 点，(3)（サイト）3 点×2，（変更内容）6 点，(4)4 点，(5)6 点，(6)6 点）

（1） g：#

h：</script>

（2） （診断方法） サーバ側で動的に生成される HTML のすべての要素に対して適切にエスケープ処理が施されているか確認する。

（理由） サーバ側の出力ではなく，ブラウザ上で不正なスクリプトが挿入されるから

（3） （サイト） サイト 5，サイト 6

（変更内容） “X-FRAME-OPTIONS”の DENY の指定を SAMEORIGIN の指定に変更する。

（4） i：ウ

（5） j：ブラウザが安全な HTTPS 通信で接続していることを示す表示を確認する。

（6） HSTS に対応していないブラウザを利用して HTTP でアクセスした場合

（別解） HTTP を使用して初めて Web サイトにアクセスする場合

以上