TAC

令和3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 Ⅰ】

問 1 （配点 50 点）

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

(1) S サービスの利用者認証の認証方式を多要素認証にできる。

(2) T サービスが停止すると，S サービスを利用することができない。

(3) a : ア　　b : イ　　c : ウ

(4) α：(え)

設問 2 （14 点：(1)2 点×2，(2)3 点×2，(2)2 点×2）

(1) d : ウ　　e : ア

(2) （ファイルのアップロード） 攻撃者
（ファイルのダウンロード） 攻撃者

(3) β : (い)　　γ : (か)

設問 3 （8 点：(1)2 点，(2)6 点）

(1) (エ)

(2) T サービスとの ID 連携改修後に，ID 連携を利用して新規に登録した S 会員

設問 4 （8 点）

T サービスで認証後に T サービスから取得した T-ID と，S サービスに登録済みの T-ID を比較し認証する。

問 2 （配点 50 点）

設問 1 （26 点：(1)5 点，(2)4 点，(3)2 点×2，(4)3 点，(5)3 点，(6)3 点，(7)2 点×2）

(1) 公開 Web サーバの名前解決ができずアクセスできない。

(2) DNS リフレクタ攻撃 （DNS リフレクション攻撃）

(3) a : ア　　b : イ

(4) c : A

(5) d : ランダム化

(6) e : DNSSEC

(7) f : オ　　g:カ　（f と g は順不同）

設問 2 （24 点：(1)6 点，(2)2 点×2，(3)2 点×4，(4)2 点×3）

(1) 権威 DNS サーバがサービス停止し，名前解決できなくなるリスク

(2) h : カ　　i : ク

(3) j : 拒否　　k : 許可　　l : 拒否　　m : 拒否

(4) n : オ　　o : ア　　p : カ　（n と p は順不同）

問 3 （配点 50 点）

設問 1 （8 点）

a ： 動作に不具合が生じないかどうか

設問 2 （4 点）

L2SW1

設問 3 （16 点：(1)4 点，(2)4 点，(3)8 点）

(1) b ： エ

(2) c ： イ

(3) ダイレクトブロードキャストの中継を許可するように設定する。

設問 4 （22 点：(1)5 点×2，(2)12 点）

(1) ((2)の活動に必要な情報） PC の IP アドレス
((4)の活動に必要な情報） PC の MAC アドレス

(2) エージェント機能によって，夜間に WoL の起動パケットの送信コマンドを実行した PC のすべての通信を遮断する。

【午　後　Ⅱ】

問 1 （配点 100 点）

設問 1 （34 点：(1)8 点，(2)8 点，(3)8 点，(4)5 点，(5)5 点）

（1） 流出した ID とパスワードが記録されたリストを入手し，それを用いて不正ログインを試みる攻撃

（2） 複数のオンラインサービスで同じ ID とパスワードを設定しない。

（3） 普段のプロバイダ，ブラウザ，接続元 IP アドレス等の情報を記録しておき，ログイン時に比較する。

（4） a ： タイムゾーン

（5） b ： 9

設問 2 （8 点）

マルウェアに感染した社内 LANPC から USB メモリを介して店舗管理システムにデータを渡す際に侵入する。

設問 3 （12 点：(1)3 点，(2)3 点×3）

（1） c ： オ

（2） d ： イ　　e ： カ　　f ： ウ

設問 4 （38 点：(1)6 点，(2)10 点，(3)8 点，(4)6 点，(5)8 点）

（1） 5 個

（2） “/etc/shadow”ファイルは管理者権限でしか参照できないため，脆弱性 M を持つ開発支援ツール J を使う一般利用者権限では参照できないから

（3） “/etc/hosts.allow”ファイルの設定で，SSH 接続の接続元制限を解除する。

（4） 24

（5） FW2 において，送信元 IP アドレスがＮ社及びＶ社以外のインターネットからのインバウンド通信を拒否する。

設問 5 （8 点）

複数の脆弱性を組み合わせることで悪用される可能性が高くなる。

問 2 （配点 100 点）

設問 1 （30 点：(1)4 点，(2)10 点，(3)8 点×2）

（1） オ

（2） 個人所有機器が大量に AP に同時接続される状況が生じ，UTM の DHCP サーバ機能で払い出す範囲の IP アドレスを使いきった。

（3） （稼働させたまま行う方法）

パケットキャプチャによって，DHCP 検出要求のブロードキャストに応答するサーバが UTM 以外にあるか調査する。

（停止させて行う方法）

調査用の無線端末で，DHCP による IP アドレス割当てを要求し，IP アドレスが取得できるかどうか確認する。

（別解） パケットキャプチャによって，DHCP 検出要求のブロードキャストに応答するサーバがあるか調査する。

設問 2 （8 点）

企画部部員全員のサービス R への過去の書込み内容や利用したファイル内容

設問 3 （12 点：(1)4 点×2，(2)4 点）

（1） a ： C-PC　　b ： AP

（2） c ： エ

設問 4 （24 点：(1)6 点，(2)4 点，(3)4 点，(4)（記号）4 点，（方法）6 点）

（1） 情報を収集し顧客への提案や企画の立案を行う業務

（2） 2

（3） 1

（4）（記号） ウ

（方法） C 社用のクライアント証明書がインストールされているか調べる。

設問 5 （10 点：(1)6 点，(2)4 点）

（1） ISMS クラウドセキュリティ認証

（別解） ・CS マーク（クラウドセキュリティ・マーク） など

・ISO/IEC 27001，ISO/IEC 27017 など

（2） d ： 4

設問 6 （16 点：(1)8 点，(2)8 点）

（1） クライアント証明書と秘密鍵のエクスポートを禁止する設定にする。

（2） P ソフトを，一般利用者権限では動作の停止やアンインストールができない設定にする。

以上