# 平成 29 年度　秋期　情報処理安全確保支援士試験　解答例

午後 II 試験

問 1

| 出題趣旨 |
|---|
| 昨今，Mirai ボットネットに代表される，今までに類を見ないほど大量の IoT 機器から成るボットネットによる，DDoS 攻撃が発生している。ネットワークカメラやインターネットルータ，ネットワークストレージなどのメーカが，これらへの対策として販売停止，あるいはファームウェア更新を実施する必要に追われたのは記憶に新しい。IoT マルウェアの感染手法は IT システムにおいては古典的であるとも言えるが，IT システムにおいては常識になっているセキュリティ対策が，IoT 機器では実施されていないことが多いという点と，IoT 機器の脆弱性が悪用されて，大規模な攻撃が発生したという点で，注目に値する。<br>本問では，IoT システムについて，ネットワークカメラを使ったビデオ監視システムを題材に，セキュリティ検査を実施し，セキュリティ対策を立案する能力を問う。 |

| 設問 | | 解答例・解答の要点 | | 備考 |
|---|---|---|---|---|
| 設問 1 | (1) | a | SYN スキャン | |
| | (2) | 開いている場合 | カ | |
| | | 閉じている場合 | エ，ク | |
| | (3) | b | HTTP を用いて，インターネット上のサーバと通信 | |
| | (4) | デバッグ用プログラムとその起動スクリプトを削除したファームウェアを作成し，Z カメラに配布する。 | | |
| 設問 2 | (1) | c | カ | |
| | | d | ア | |
| | (2) | e | HTTPS | |
| | (3) | 証明書パスの検証が行われているかを確認できなくなるから | | |
| 設問 3 | (1) | クライアント証明書を用いた端末認証を行う。 | | |
| | (2) | f | A2，C2，D1，D2 | |
| | (3) | 利用者 ID を変更しながら，よく用いられるパスワードでログインを試行する。 | | |
| | (4) | 一つの利用者 ID でのログイン試行が 1 回ないしは少ない回数しか行われないから | | |
| | (5) | ほかの Web サイトから漏えいした情報に電話番号や電子メールアドレスが含まれていた場合 | | |
| | (6) | 利用者番号の入力を求める。 | | |
| | (7) | 全利用者の単位時間当たりの認証失敗数がしきい値を超えた場合 | | |
| | (8) | 脆弱性検査合格を受入条件とする。 | | |
| | (9) | 脆弱性が Z 社のシステムに影響するかを短時間で判断できない。 | | |
| | (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 | Bluetooth 経由で受け渡す。 | |

問２

| 出題趣旨 |
|---|
| 2005 年の個人情報保護法施行以降，個人情報を暗号化して保存することが求められるようになった。DBMS 製品においてもデータ暗号化の機能が備わってきており，重要なデータを暗号化してデータベースに保管するシステムが増えてきている。<br>データベース暗号化及び暗号鍵の管理においては，やみくもにデータ暗号化や鍵管理機能を実装するのではなく，想定するリスクと残存リスクを明確にし，目的に沿って設計・実装することが重要である。鍵管理においては，暗号化に使用する鍵を安全に管理するための手段として，ハードウェア暗号モジュールが用いられてきた。<br>本問では，データ暗号化を題材に，暗号方式及びハードウェア暗号モジュールに関する基本的な知識並びに目的に沿ったデータ暗号方式の設計能力を問う。 |

| 設問 | | 解答例・解答の要点 | | 備考 |
|---|---|---|---|---|
| 設問１ | (1) | a | FISC | |
| | | b | CRYPTREC | |
| | (2) | 162 | | |
| | (3) | オペレータ及びシステム管理者が，暗号化された契約情報を暗号化・復号に用いられる鍵を用いて復号し，取得するリスク | | |
| 設問２ | (1) | c | FIPS | |
| | (2) | 単独の鍵管理者ではマスタ鍵を復元できない。 | | |
| | (3) | 場合 | 製品 H を交換した場合 | |
| | | 目的 | マスタ鍵を復元するため | |
| | (4) | 耐タンパ性 | | |
| | (5) | 事象 | 静電気の放電による規定の範囲を超える電源電圧の発生 | |
| | | 機能 | 事象をセンサが検知し，製品 H 自身を使用不能で戻せない状態にする。 | |
| 設問３ | (1) | エラーとなる手順 | (v) | |
| | | API-X のコマンド | 暗号化(DBαの DB データ鍵，DBαの DB マスタ鍵 ID) | |
| | | API-X のエラーの原因 | DBαの DB マスタ鍵が鍵ストアファイル 2 に存在しないこと | |
| | (2) | 複数の H クライアントが送信したデータ鍵 ID が重複した場合 | | |
| 設問４ | (1) | 業務担当者及び契約者が業務アプリケーションを利用して持ち出すリスク | | |
| | (2) | オペレータ及びシステム管理者が，メモリダンプから平文の契約情報を読み出し，持ち出すリスク | | |