平成２９年度秋期　情報処理安全確保支援士　午後Ⅱ試験　解答速報

（株）アイテック　IT 人材教育研究部　2017.10.18 発表

問１　IoT システムのセキュリティ対策

【解答例】

［設問１］

(1) a：TCP 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削除した修正版のファームウェアをカメラ IF から Z カメラへ配信する。

［設問２］

(1) c：カ　　d：ア

(2) e：HTTPS

(3) Z カメラには攻撃時に使われるルート証明書が未登録だから。

［設問３］

(1) クライアント証明書を対象の端末に導入する。

(2) f：A2，C1，C2，D1，D2

(3) 想定したパスワードを固定して，利用者 ID について全ての組合せを試行する。

(4) 試行する利用者 ID が毎回異なり，毎回の試行時にはログインを制限されないから。

(5) 他の Web サイトから利用者 ID とパスワードのリストに加えて電話番号などの利用者情報も漏えいした場合

(6) 利用者情報登録時に付与される利用者番号を用いる。

(7) Z クラウドへのログイン時に UUID を用いた認証が未実行又は失敗した場合

(8) 脆弱性を突いた攻撃に対するセキュリティ要求事項

(9) 脆弱性が報告された OS やミドルウェアなどに対する迅速な対応を実施できない。

(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 通信を用いて直接受け渡す。

問２　データ暗号化の設計

【解答例】

［設問１］

(1) a：FISC　　b：CRYPTREC

(2) 162 台

(3) オペレータとシステム管理者が OS を操作して DB のバックアップファイルを読み出し，平文で保管されている鍵で復号する。

［設問２］

(1) c：FIPS

(2) 鍵管理者による不正行為をできるだけ防止する。

(3) 場合：製品 H を交換した場合
目的：マスタ鍵をリカバリするため。

(4) 耐タンパ性

(5) 事象：製品 H の運搬時に静電気によるショートで規定の範囲を超える電源電圧が発生する。
機能：内蔵されているセンサが事象を検知して，メモリ上のマスタ鍵をゼロ化する機能

［設問３］

(1) 手順：(v)
API-X のコマンド：暗号化（DBαデータ鍵，DBαマスタ鍵 ID）
API-X のエラー原因：鍵ストアファイル 2 には DBαマスタ鍵 ID の鍵が存在しないから。

(2) 複数の業務システムの DB サーバの H クライアントが同じデータ鍵 ID を採番した場合

［設問４］

(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利用して契約情報を読み出すリスク

(2) オペレータとシステム管理者が OS の機能で出力したメモリダンプファイルから契約情報を読み出すリスク

以上