

平成31年度春期 情報処理安全確保支援士 午後I試験 解答速報

(株) アイテック IT人材教育研究部 2019.4.23 発表

問1 Webサイトのセキュリティ

【解答例】

[設問1]

- (1) a : Same Origin (又は, 同一生成元, 又は, 同一源泉)
- (2) b : イ c : キ d : ク (b~d は, 順不同)
- (3) Web サイト B にログインする。

[設問2]

e : (v)

[設問3]

- (1) f : `https://site-a.m-sha.co.jp`
- (2) g : プリフライトリクエスト中の Origin ヘッダフィールド
- (3) h : Origin ヘッダフィールドの値  
i : 許可するオリジンのリスト  
j : 一致

問2 クラウドサービスのセキュリティ

【解答例】

[設問1]

- (1) ホテル Wi-Fi の SSID 及び事前共有鍵と DNS サーバ情報
- (2) a : メールサービス P  
b : 攻撃者が用意した Web サーバ
- (3) HTTP でアクセスしたから。

[設問2]

- (1) Web ブラウザと正規サイトとの間の通信を中継して, 情報を窃取する。
- (2) c : ウ d : ア e : エ f : イ
- (3) IDaaS の認証サーバ X では, 署名 M 中のオリジン b の正当性を検証するから。

### 問3 IoT機器の開発

**【解答例】**

[設問1]

エ

[設問2]

- (1) ゲームプログラム ID
- (2) 管理者が一つの共通鍵をゲームプログラムに設定する。
- (3) 仕様：MACの生成と検証に共通鍵を用いる。  
範囲：同じゲームプログラム開発会社が稼働させているゲームプログラム
- (4) a：オ b：エ c：カ
- (5) ゲーム機VのSSDを取り外してPCに直結させる。
- (6) 耐タンパ性

[設問3]

ハッシュ値リストをTPMに格納する。

以上

