平成 29 年度 秋期 情報処理安全確保支援士

＜午後Ⅱ 解答・解説＞

＜問 1＞ IoT システムのセキュリティ対策

■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（24 字）

(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。(47 字)

(1) TCP ポートに SYN を送信し，応答結果からポートが開いているかどうか確認する検査はポートスキャンの一種である「SYN スキャン」(「TCP SYN スキャン」「ステルススキャン」と呼ばれる場合もある）である。

(2) SYN を送信したポートが開いている場合には，SYN と ACK のフラグが ON になった応答を受信することが期待される。一方，ポートが閉じている場合には，RST と ACK が ON になった応答を受信することが期待されるが，ネットワーク機器やセキュリティ対策製品の設定等により，応答が返らないことも考えられる。

(3) 表 3 の Z カメラのセキュリティ検査は，マルウェア M 又はその亜種に Z カメラが感染するおそれがあるかを調べるのを目的としており，項番 5 では，マルウェア M を想定したファイルを起動できたことを確認している。表 2 より，ダウンロードし，実行されたマルウェア M は項番 1～4 の動作を行うことがわかる。表 2 の項番 1 でマルウェア M は，HTTP を用いて C&C サーバと通信しているため，これをセキュリティ検査で調べるには，表 3 の項番 5 で起動したプロセスが，HTTP を用いてインターネット上のサーバと通信できるか確認する必要がある。

(4) 下線②の前の文にあるように，Z カメラの TCP ポート 2323 が開いていたのは，委託先が開発時に使ったデバッグ用プログラムとその起動スクリプトが，出荷版のファームウェアにそのまま残されていたことが原因である。また，問題文の〔Z クラウドの詳細〕の(5)に「Z クラウドから Z カメラへの各種操作コマンド及び設定情報の送信とファームウェアの配信は，Z カメラが定期的にカメラ IF にアクセスすることによって行われる」とある。これらの内容から，出荷時の Z カメラに対する対策は，問題個所を修正したファームウェアを Z カメラに配布することであることがわかる。具体的には，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 カメラに配布することである。

■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（27 字）

(1)

c：Z カメラと Z クラウド間の HTTPS 通信の内容を復号して確認できるか検査していることから，表 4 の項番 1 で想定している脅威は，中間者攻撃による暗号通信の盗聴である。

d：偽 Z クラウド上で稼働している偽カメラ IF に Z カメラを接続させて Z カメラが操作できるか検査していることから，表 4 の項番 2 で想定している脅威は，攻撃者による DNS キャッシュポイズニングを使った偽 Z クラウドへの誘導である。

(2) 問題文の〔Z クラウドの詳細〕の(5)に「Z カメラ及び Z アプリは Web サーバに HTTPS の POST メソッドを用いて通信する」とあることからわかるように，該当するのは HTTPS である。

(3) プライベート認証局のルート証明書を，テスト対象の Z カメラに信頼されたルート認証機関のものとして登録すると，プライベート認証局が発行したサーバ証明書の証明書パ

スの認証が成立することになる。そうなると，信頼されたルート証明機関以外が発行した証明書を使用した場合に，証明書パスの検証が正しく行われるかを確認できなくなってしまう。

■設問 3

(1) クライアント証明書を用いた端末認証を行う。(21 字)

(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。(36 字)

(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 (37 字)

(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 (42 字)

(6) 利用者番号の入力を求める。(13 字)

(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 (29 字)

(8) 脆弱性検査合格を受入条件とする。(16 字)

(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。(29 字)

(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。

(1) アクセス元の端末を制限する方法としては，IP アドレスによる端末認証，MAC アドレスによる端末認証，クライアント証明書による端末認証などが考えられる。図 1 の注記 2

を見ると，Z クラウドの管理者は，通常時は管理端末を用いて Z 社内又は委託先社内で運用管理作業を実施するほか，緊急時には貸与された管理用モバイル端末を用いて自宅で同作業を実施することもある。また，〔Z クラウドの詳細〕の(5)に「インターネットから Web サーバへの接続は HTTPS だけが許可されている」とある。これらの点から，Z システムに適した方式は，クライアント証明書を用いた端末認証である。

(2) 図 1 の注記 2 にあるように，Web サーバのコンテンツ，及び Web アプリケーションの変更は，Z クラウドの管理者だけが実施できる。その前提で，表 5 の脅威が Z クラウドの Web サーバ上にあるコンテンツの予期せぬ変更の原因となるかどうかを確認する。

A1：利用者アカウントでは Web サーバのコンテンツを変更できないため，該当しない。
A2：管理者アカウントであれば Web サーバのコンテンツを変更できるため，該当する。
B1：DDoS 攻撃は Web サーバのコンテンツ変更とは関係ないため，該当しない。
C1：Web アプリケーションサーバと Web サーバは別個に存在するため，該当しない。
C2：こうした攻撃により管理者権限を奪われる可能性があるため，該当する。
D1：内部者であれば管理者アカウントで Web サーバにアクセス可能であるため，該当する。
D2：D1 に同じ。

したがって，Z クラウドの Web サーバ上にあるコンテンツの予期せぬ変更の原因として考えられるのは，A2, C2, D1, D2 である。

(3) ブルートフォース攻撃は，ユーザ ID を固定して何通りものパスワードの組合せを試行する手法である。これに対し，リバースブルートフォース攻撃は，パスワードを固定して何通りものユーザ ID の組合せを試行する手法である。

(4) ログイン制限は，同じ利用者 ID に対して連続してログインの試行が行われ，認証が失敗する場合には有効な対策となる。しかし，リバースブルートフォース攻撃やリスト型攻撃では，同じ利用者 ID に対して 1 回程度のログイン試行しか行われないため，ログイン制限では防ぐのが難しい。

(5) リスト型攻撃は，何らかの原因で会員制 Web サイト等から漏えいした情報に基づいて行われている。電話番号や電子メールアドレスについては漏えいした情報に含まれている可能性があるため，その場合にはそれらを認証情報として追加したとしても防ぐことができない。

(6) 問題文の〔Z クラウドの詳細〕の(2)に「登録時には自動的に 10 進数 12 桁の利用者番号が付与される。利用者番号は，Web IF の利用者登録画面上に表示される。また，利用者登録完了書に記載され，登録した住所に郵送される」とある。また，〔Z クラウドの詳細〕の(3)に「譲渡や転売などの理由で，登録済みの Z カメラが他の利用者によって登録された場合，Z カメラの利用者を変更するとともに，変更されたことを元の利用者に電子メールを送って通知する」とある。こうしたことから，Z クラウドと各利用者だけが知っていて，利用者以外が入手するのが困難な情報として利用者番号の入力を求めるのが適切である。

(7) 問題文の〔Z アプリの詳細〕の(2)「2 回目以降の利用者認証」に「前回認証成功以降に利用者情報の変更がなかった場合，UUID を用いて認証される」とある。つまり，2 回目以降は利用者情報の変更がない限り，利用者 ID とパスワードの入力は省略されるため，認証の失敗は発生しにくい。リバースブルートフォース攻撃やリスト型攻撃では，多くの利用者で認証失敗が発生する可能性が高いため，全利用者の単位時間当たりの認証失敗回数をしきい値として設定しておき，それを超えた場合に平常時とは異なる状況が発生していると判断するのが有効である。

(8) Web アプリケーションプログラムの納品時に脆弱性検査を実施するのであるから，開発委託先との契約には，脆弱性検査合格を受入条件として盛り込むべきである。

(9) 脆弱性を突いた攻撃が頻繁に発生する昨今の状況を踏まえると，年に 1 回の脆弱性検査や定期メンテナンス時の対応では不十分である。とはいえ，構成管理を導入していなければ，重大な脆弱性が新たに発見された場合に Z 社のシステムに影響するかを短時間で判断するのは困難である。そのため，D 社は構成管理を導入した脆弱性対応の仕組みを構築する必要があると指摘したと考えられる。

(10) Z クラウドの管理者に見られないことを重視した場合，共通鍵の生成は Z クラウドではなく，モバイル端末内の Z アプリで行うべきである。

次に動画の暗号化であるが，問題文の〔Z カメラの詳細〕に「撮影した動画は Z クラウドに送信され，大容量ストレージに保管される」「バッファ用の小規模ストレージがあるが，Z クラウドに送信した動画はそこから速やかに消去される」とあることから，この小規模ストレージを活用し，Z カメラで動画の暗号化を行うべきである。また，暗号化された動画の復号についてはモバイル端末内の Z アプリで行うべきである。

共通鍵を安全に共有するには，Z アプリと Z カメラ間での安全に通信を行う必要があるが，Z クラウドの管理者に見られないことを重視するのであるから，Z クラウドは経由せずに，Bluetooth 経由で受け渡すべきである。

＜問 2＞　データ暗号化の設計

■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（55 字）**

(1)

a：金融機関などがよりどころとすべき共通の安全対策基準を発行しているのは FISC（The Center for Financial Industry Information Systems：金融情報システムセンター）である。FISC は，金融情報システムに関連する諸問題（技術，利活用，管理態勢，脅威と防衛策等）の国内外における現状，課題，将来への発展性とそのための方策等についての調査研究を活動の基本としている。

b：電子政府における調達のために参照すべき暗号のリストは，CRYPTREC 暗号リストである。CRYPTREC（Cryptography Research and Evaluation Committees）とは，電子政府推奨暗号の安全性を評価・監視し，暗号技術の適切な実装法・運用法を調査・検討するプロジェクトである。

(2) 2017 年製の PC で，1998 年と同じ 40 日間，鍵空間の 80%を探索するのに必要な台数を試算するのであるから，単純に MIPS 値と台数の比を計算すれば良い。

2017 年製の PC の台数を x とすれば，次の式で求めることができる。

$$133{,}920x = 540 \times 40{,}000$$

$$x = \frac{540 \times 40{,}000}{133{,}920} = \frac{540 \times 40{,}000}{540 \times 248} = \frac{40{,}000}{248} = 161.29..$$

したがって，必要な PC は 162 台である。

(3) 問題文の〔K1 システムの現在の運用〕の(3)にあるように，オペレータとシステム管理

者には，DBMS と Web アプリケーションサーバソフトウェアとを除くミドルウェア及び OS 上の全ての操作権限が付与されている。

また，〔K1 システムの現在の運用〕の(4)にあるように，契約情報は，業務アプリケーションが共通鍵暗号方式で暗号化し，DB サーバに保管されている。

そして，Y 社による指摘 2 は，契約情報の暗号化及び復号に用いる鍵が平文でファイルに保管されており，オペレータ及びシステム管理者に当該ファイルのアクセス権が付与されている，という内容である。

これらのことから，オペレータ及びシステム管理者が，暗号化され，DB サーバに保管されている契約情報を，平文でファイルに保管された暗号化・復号に用いられる鍵を用いて復号し，取得するリスクが発生する。

■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。(21 字)

(3) 場合：製品 H を交換した場合（10 字）
目的：マスタ鍵を復元するため（11 字）

(4) 耐タンパ性（5 字）

(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（25 字）
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。(32 字)

(1) 空欄に該当するのは FIPS（Federal Information Processing Standardization：連邦情報処理規格）である。FIPS 140-2 は，米国連邦政府の省庁等各機関が利用する暗号モジュールに関するセキュリティ要件を規定した文書である。

(2) 1 人の鍵管理者が三つの部分鍵を入力し，3 枚の IC カードに保管して管理していたとすれば，その鍵管理者に悪意があればマスタ鍵を復元し，不正に使用することも可能である。一方，製品 H の仕様 1 では，3 人の鍵管理者が各々6 桁の PIN を入力した上で三つの部分鍵を別々の IC カードに保管し，当該 IC カード自体も別々に保管することになっている。また，IC カードから部分鍵を良い出す際には PIN の入力が必要になる。このよ

うな仕様であれば，鍵管理者の一人に悪意があったとしても，マスタ鍵を復元することはできない。

(3) 製品 H の仕様 1 にあるように，マスタ鍵は，3 つの部分鍵の排他的論理和によって生成され，製品 H のメモリ内に保持される，製品 H に故障や不具合が発生して交換した場合にはメモリ内のマスタ鍵を再生成する必要があり，その際に部分鍵が必要となる。

(4) 下線①のような暗号モジュールの性質を耐タンパ（tamper）性という。tamper とは，「許可なく変更する，改ざんする」といった意味で，耐タンパ性が高いほどセキュリティレベルは高くなる。暗号モジュールに保存された重要データを外部から無理やり取り出そうとしたり，盗み読もうとしたりする行為への耐性が耐タンパ性である。

(5) 製品 H の仕様 5 にあるように，製品 H は，規定の範囲を超える電源電圧の発生やカバーのこじ開け等をセンサが検知すると，メモリ上に保持されているマスタ鍵をゼロ化するとともに，自身を使用不能で元に戻せない状態にする。つまり，製品 H の運搬時に必ず静電気防止シートで覆うように定めているのは，静電気の放電によって規定の範囲を超えた電源電圧をセンサが検知し，製品 H 自身を使用不能で元に戻せない状態にしてしまうことに配慮したものである。

■設問 3

(1) エラーとなる手順：（ｖ）
API-X のコマンド：暗号化（DBαのデータ鍵，DBαのマスタ鍵 ID）（25 字）
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（28 字）

(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（28 字）

(1) 問題文の K2 システムにおける DB 及び表領域の作成手順の(ⅲ）から順に確認する。

まず（ⅲ）では，製品 D1 上で DBα を作成するが，その際，DBα のマスタ鍵を生成するため，H クライアント 1 が H サーバ 1 に API-X の実行要求を出し，製品 H-1 で鍵が生成される。生成された DBα のマスタ鍵と DBα のマスタ鍵 ID は鍵ストアファイル 1 に保管される。

（ⅳ）では（ⅲ）と同様に DBβ を生成する。DBβ のマスタ鍵を生成するための API-X

の実行要求は，資源を純繰りに割り当てるラウンドロビン方式により，H クライアント 1 から H サーバ 2 に対して行われる。その結果，製品 H-2 で DBβのマスタ鍵が生成され，DBβのマスタ鍵 ID とともに鍵ストアファイル 2 に保管される。

続いて（ｖ）では，DBαに対応する表領域 1 を作成に際し，まずは乱数を生成するために API-X の実行要求を出す。ラウンドロビン方式により，この実行要求は H クライアント 1 から H サーバ 1 に対して行われる。生成された乱数は DBαのデータ鍵として製品 D1 のメモリ上に保持される。続いて DBαの DB マスタ鍵で暗号化するために API-X の実行要求を出す。ラウンドロビン方式により，この実行要求は H クライアント 1 から H サーバ 2 に対して行われ，製品 H-2 が DBαの DB マスタ鍵を鍵ストアファイル 2 から読み出そうとするが，鍵ストアファイル 2 には存在しないため，エラーが発生する。このときの API-X のコマンドは，図 3 にあるように「暗号化（DBαのデータ鍵, DBαのマスタ鍵 ID)」である。

(2) 問題文の〔暗号方式の検討〕の H クライアントと H サーバの仕様(1)にあるように，従来のデータ鍵 ID は，H クライアントの内部で 0 から順番に採番される。そのため，H クライアント ID をデータ鍵に付け加える機能がないと，複数の H クライアントが重複したデータ鍵 ID を送信する可能性があり，その際に DB 作成がエラーとなる。

■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（33 字）

(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（44 字）

まず，問題文に登場するアクターとして，業務担当者，契約者，オペレータ，システム管理者，業務アプリケーション管理者があり，各アクターの K2 システムの利用方法や権限等は次のようになっている。

業務担当者：

業務アプリケーションを利用して契約情報を管理する。

契約者：

PC の Web ブラウザ及びスマートフォンのアプリからインターネットを介して K2 システ

ム（業務アプリケーション）にアクセスし，契約情報の参照，被保険者情報の更新などを行う。

オペレータとシステム管理者：

DBMS, Web アプリケーションソフトウェアを除くミドルウェア及び OS 上の全ての操作権限が付与されている。

業務アプリケーション管理者：

DBMS, Web アプリケーションソフトウェア，業務アプリケーション，及び業務アプリケーションのログに関する全ての権限が付与されている。

対策 1 は，業務アプリケーションのログから不審なアクセスがないか監視することが目的であるため，「誰が」については日常的に業務アプリケーションを利用している「業務担当者と契約者」であり，「どのような方法で契約情報を取得するリスクか」については「業務アプリケーションを利用して契約情報を持ち出すリスク」である。

対策 2 は，メモリダンプファイルに対する操作履歴を対象としている。製品 D の仕様 D にあるように，ディスク上から読み込まれた暗号化データは DB データ鍵で復号されるため，メモリ内には平文の契約情報が存在することがわかる。したがって，「どのような方法で契約情報を取得するリスクか」については，「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」である。そして，「誰が」については，DBMS, Web アプリケーションソフトウェアを除くミドルウェア及び OS 上の全ての操作権限が付与されている「オペレータとシステム管理者」である。