**■設問 4**

**〔試験センターによる解答例〕**

**(1) あるアプリから，ほかのアプリのデータへのアクセスを禁止するという仕様（34 字）**

**(2) ルート特権化するマルウェアに感染したとき（20 字）**

**(3) M システムを使って確認する。(14 字)**

(1) ルート特権化されていないスマホであれば，OS のファイルシステムに実装されているアクセス制御の仕組みにより，**あるアプリからほかのアプリのデータにアクセスすることを禁止する**仕様となっている。そうすることで，データが不正な読出しを防いでいる。

(2) 問題文に，マルウェアの侵入によってルート特権が取得される旨の記述があることから分かるように，従業員がスマホ利用規程を守ったとしても，**ルート特権化するマルウェアに感染した**場合には，意図しないルート特権化が起こり得る。

(3) 問題文の冒頭に「スマホを遠隔で管理するシステム（以下，M システムという）を追加で導入し，スマホの OS やアプリのバージョンなどの構成情報の管理や，スマホの紛失時のデータ消去などのセキュリティ対策を実現した」とあることから分かるように，**M システムを使用**すればスマホの OS のバージョンを確認することができる。

## ＜問2＞ 代理店販売支援システム

**■設問 1**

**〔試験センターによる解答例〕**

**(1) a：15,360**

**b：512**

**(2) カ，キ**

**(3) c：112**

**要件：利用期間は 2025 年 8 月までである。(18 字)**

(1) a : AES（Advanced Encryption Standard）は，米国政府標準の共通鍵暗号方式である。一方，RSA は標準的な公開鍵暗号方式であり，桁数の大きな整数の素因数分解が困難

であることを安全性の根拠にしている。表 2 より，256 ビットの共通鍵暗号方式と同等のセキュリティ強度をもつ素因数分解問題に基づくアルゴリズム（RSA アルゴリズム）の鍵長は，**15,360** ビットであることが分かる。

b：上記と同様に，表 2 より，256 ビットの共通鍵暗号方式と同等のセキュリティ強度をもつハッシュ関数（ハッシュ値）のビット数は，512 ビットであることが分かる。

(2)解答群の中で，ハッシュ関数は以下の四つである（括弧内はハッシュ値のビット数）。

ウ：MD5（128 ビット）
オ：SHA-1（160 ビット）
カ：SHA-256（256 ビット）
キ：SHA-512（512 ビット）

表 2 より，鍵長 3,072 ビットの RSA アルゴリズムと同等のセキュリティ強度をもつハッシュ関数のビット数は 256 ビットであることが分かる。したがって，上記と同等又はそれ以上のセキュリティ強度をもつと考えられるハッシュ関数は，カの **SHA-256** とキの **SHA-512** である。

(3)〔Q システムの設計方針〕より，Q システムは 2015 年 9 月から 10 年間，つまり，**2025 年 8 月までの稼働**を想定していることが分かる。したがって，表 2 で利用終了時期の目安が 2030 年となっている **112** ビット安全性と同等，又はそれ以上のセキュリティ強度をもつ暗号アルゴリズムを採用すべきである。

**■設問 2**

**〔試験センターによる解答例〕**

**(1) 端末に発行された証明書の利用停止を申請する。(22 字)**

**(2) d：公開鍵（3 字）**

**e：シリアル番号（6 字）**

**f：受付拒否リスト（7 字）**

**g：入力された利用者 ID（10 字）**

**h：利用者 ID（5 字）**

(1) Q システムにアクセスしていた端末を交換及び廃棄する場合には，当該端末用に発行された証明書が不正に利用されることのないよう，**利用を停止するための手続き**が必要と

なる。詳細な手順は図 2 に示されており，代理店が行うのは項番 1 の(1)であるが，これは利用停止処理ではなく，あくまでも利用停止の申請であることに注意する。利用停止の処理は項番 1 の(2)であり，項番 1 の(1)の申請を受けて L 社側で実施する。

(2)

d：ディジタル証明書は，「公開鍵証明書」とも呼ばれるように，発行する際に利用者の公開鍵を登録する。したがって，図 1 の(4)では，担当者は端末で自身の公開鍵，秘密鍵の鍵ペアを生成した後，**公開鍵**を送信する。

e：証明書の利用を停止するために入力するものであるから，証明書を一意に識別できる情報であることが分かる。図 1 の注記に「証明書には，証明書のシリアル番号，利用者 ID，公開鍵，識別番号などを登録する」とあることから，［ e ］には「**シリアル番号**」が該当する。

f：受付サーバにおける担当者及び代表者のログイン処理時の検証項目として，証明書が失効状態にないことを確認する必要があり，［ f ］の項目ではそれを行っている。失効状態にある証明書は，識別番号が CRL（Certificate Revocation List）と呼ばれるリストに登録されているため，そこに登録されていないことを確認する。本問では，CRL を図 2 の項番 1 の(2)で「**受付拒否リスト**」と表記しているため，これを解答する。

g，h：まず，図 1 の注記より，証明書にはシリアル番号，利用者 ID，公開鍵，識別番号などが含まれていることから，［ h ］には，これらの項目のうちいずれかが該当することが分かる。表 1 の「利用者の認証」及び図 2 の項番 3 の一つ目にあるように，ログイン処理時には，利用者は利用者 ID とパスワードを入力し，それが正しい組合せであることを確認している。
これらの情報から，［ g ］には「**入力された利用者 ID**」，［ h ］には「**利用者 ID**」という解答が導き出せる。こうすることで，第三者がなりすまして（他人の証明を利用して）ログインしていないかどうかを検証することができる。

**■設問３**

**〔試験センターによる解答例〕**

**(1) 代理店の管轄下の端末に証明書がインストールされていることを代表者が確認する。(38 字)**

**(2) i：担当者の証明書を停止する権限を代表者に付与する (23 字)**

**(3) 受付拒否リストに識別番号が登録されている証明書は更新を拒否する。(32 字)**

(1) 表 1 にあるように，"端末の限定"の設計方針により，「代理店の管轄下にある端末から