平成 26 年度 秋期 情報セキュリティスペシャリスト

＜午後 I　解答･解説＞

＜問1＞ スマートフォン

■設問 1

〔試験センターによる解答例〕

a：セキュリティパッチ（9 字）

b：ヒープ（3 字）

d：return-to-libc（14 字）

a：OS やライブラリのセキュリティホールに対処するために適用するのは**セキュリティパッチ**である。

b：バッファオーバフロー攻撃として，問題文にあるスタックバッファオーバフロー攻撃，静的メモリ領域を対象とした攻撃のほか，メモリの**ヒープ領域**を対象としたヒープバッファオーバフロー攻撃がある。ヒープ領域は，malloc 関数，new 演算子（C++言語の場合）によって動的に確保され，プログラムが永続的に使用するデータを格納するために用いられる。

d：このような攻撃は「**return-to-libc 攻撃**」と呼ばれる。攻撃者は，スタックバッファオーバフロー攻撃と同様の手法を用いて，メモリ上にロードされた libc 共有ライブラリ内の特定の関数（OS の任意のコマンドを実行する system()関数など）を呼び出すようにリターンアドレスと引数を書き換える。この攻撃はスタック領域のコードを実行するわけではないため，データ実行防止機能が実装されていたとしても防ぐことができない。

■設問 2

〔試験センターによる解答例〕

(1) スタック領域

(2) c：エ

(3) 攻撃を成功させるためのジャンプ先アドレスの特定（23 字）

(1) スタックバッファオーバフロー攻撃は，スタック領域に挿入したインジェクションベクタの shell コードを実行させる手法である。これを防止するのであるから，データ実行防止機能を**スタック領域**に適用する必要がある。

(2) リトルエンディアンとは，複数バイトの 2 進数をメモリに配置する際に，最下位のバイトから順番に並べる方式である。これとは逆に最上位のバイトから順番に並べる方式をビッグエンディアンという。
図 2 より，shell コードの前にはリターンアドレス X が入ることが分かる。shell コードを実行されるためには，shell コードの先頭アドレスである"c8048026"をリターンアドレス X に入れる必要があるが，バイトオーダはリトルエンディアンであるため，**"268004c8"**となる。

(3) アドレス空間配置ランダム化（Address Space Layout Randomization : ASLR）とは，アドレス空間における実行ファイル，ライブラリ，スタック，ヒープ等の配置をランダムにする技術である。これにより，**スタックバッファオーバフロー攻撃を成功させるためにジャンプ先アドレス（リターンアドレス）が特定される**ことを抑制する。

■設問３

〔試験センターによる解答例〕

(1) インジェクションベクタを検知・破棄する。(20 字)

(2) ルート特権があること (10 字)

(1) IPS（Intrusion Prevention System）や WAF（Web Application Firewall）は，あらかじめ設定された攻撃パターン（シグネチャ）に基づいて通信データに含まれる**インジェクションベクタを検知・破棄する**ことでバッファオーバフロー攻撃を防止する。

(2) インジェクションベクタの shell コードは，攻撃の対象となったプログラム（Vuln）と同じ権限で実行される。したがって，あらゆる命令を shell コードで実行するためには，Vuln が**ルート特権で動作している**必要がある。

■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

のアクセスだけを許可する」ことになっている。しかし，図 1 の(5)-2 にあるとおり，発行された証明書は代理店の担当者が端末にインストールする手順となっているため，仮に当該担当者が代理店の管轄下にない端末に証明書をインストールすれば，その端末から Q システムにアクセスできる可能性がある。この問題に対して代理店側でとる対策であり，代理店の代表者は不適切な行為をしないことが前提であることから，「**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**」ことが解答として導き出せる。

(2) 図 2 の項番 1 の(1)にあるように，証明書の利用を停止する場合には，当該証明書の利用者である担当者が受付サーバにログインし，申請する手順となっている。しかし，利用者が端末を紛失した場合などは，担当者は受付サーバにログインすることができなくなるため，利用停止の申請ができないという問題が生じる。表 3 の(2)は，役割と権限を見直すことでこの問題を解決する案である。担当者が不在の場合でも証明書の利用停止が可能であるが，その反面，代表者の役割が拡大し，権限が集中することから，［ i ］の解答として「**担当者の証明書を停止する権限を代表者に付与する**」ことが導き出せる。

(3) R 主任の指摘は，利用停止された証明書の取扱いを担当者が誤った場合などに，本来発行されるべきでない証明書が発行される可能性があるということである。利用停止された証明書については，識別番号が受付拒否リストに登録されている。ところが，図 2 の項番 2 の証明書の更新手順を見ると，更新する証明書の識別番号が受付拒否リストに登録されているかどうかについては確認していない。そのため，R 主任が指摘した問題が発生する可能性がある。これを防ぐために登録サーバに追加すべき処理は，「**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**」ことである。

＜問3＞ マルウェア感染への対応

■設問 1

〔試験センターによる解答例〕

(1) メールサーバ Z から営業部員宛てに送られるメール（23 字）

(2) 送信元メールサーバの IP アドレスのホワイトリストにメールサーバ Z の IP アドレスを追加する。(45 字)

(1) 問題文にあるように，SaaS 型クラウドサービスであるサービス X 内のメールサーバ Z は，製品紹介のメールの写しを M 社営業部員全員に送信しており，その際には送信者メールアドレスとして M 社のメールアドレスを使っている。そのため，外部メールサーバの送信ドメイン名のブラックリストに M 社のドメイン名を指定すると，上記の M 社**営業部員宛てに送られるメール**が届かなくなる。

(2) 表 1 にあるように, 外部メールサーバのメールフィルタリング機能のホワイトリスト及びブラックリストには，送信元メールサーバの IP アドレスのリスト及びドメイン名のリストがあり，両方のリストにマッチした場合はホワイトリストを優先する仕組みとなっている。この機能を活用し，メールサーバ Z から M 社営業部員宛てに送られるメールが届くようにするためには，**送信元メールサーバの IP アドレスのホワイトリストにメールサーバ Z の IP アドレスを追加**すればよい。

■設問２

〔試験センターによる解答例〕

(1) FW のフィルタリングルールで遮断しているから（22 字）

(2) 顧客管理（4 字）

(3)

メソッド	ポート番号	動作
CONNECT	2560	許可

(1) 図 2 にあるように，マルウェア Y には 2 通りの方法で C&C サーバとの通信を試みる。そのうち一つ目はプロキシサーバを経由せずに，TCP ポート番号 8050 を使用してアクセスする方法であるが，これは既に防ぐことができていると S さんは話している。
M 社のネットワークでは，FW と L3SW でアクセス制御を行っているため，これらのフィルタリングルールを確認する。すると，表 2 の FW のフィルタリングルールでインターネットへの通信は送信元がプロキシサーバに制限されているため，マルウェア Y が PC やサーバに感染したとしても，プロキシサーバを経由しないでインターネット上の C&C サーバと通信することはできない。一方，L3SW のフィルタリングルールでは，項番 5, 6 で開発サーバセグメントと全セグメント間の通信は拒否されているものの，項番 7 で開発サーバセグメント以外のセグメントから全セグメントへの通信が許可されているため，プロキシサーバを経由しないマルウェア Y の通信を防ぐことはできない。

(2) 問題文にあるように，営業部ではサービス X を利用して顧客管理を行っており，サービス X には，ポート番号 2560 番宛てに営業部の PC から HTTP の CONNECT メソッドを使用してプロキシサーバ経由でアクセスしている。しかし，表 4 のプロキシサーバのアクセス制御ルールでは，CONNECT メソッドはポート番号 443 番宛てのみ許可されているため，ポート番号 2560 番宛ての CONNECT メソッドは遮断されてしまう。そのため，このままの設定では営業部の**顧客管理**に支障が出ることになる。

(3) 上記(2)の問題を解決するには，ポート番号 2560 番宛ての CONNECT メソッドを許可するようにプロキシサーバのアクセス制御ルールに追加すればよい。これは，表 4 の項

番 1 とポート番号のみが異なるルールであるため，メソッドに"**CONNECT**"，ポート番号に"**2560**"，動作に"**許可**"と設定する。

■設問 3

〔試験センターによる解答例〕

(1) 利用者セグメント 2 から開発サーバセグメントへの通信を拒否にする。(32 字)

(2) a：運用サーバセグメントの管理に必要のないソフトウェアの利用 (28 字)

(1) 開発専用 PC を数十台開発サーバセグメント内に置き，ソフトウェアパッケージの開発を開発専用 PC 及び開発サーバだけで行うようにすれば，利用者セグメント 2 に接続された開発部の PC から開発サーバにアクセスする必要がなくなる。これにより，表 3 の項番 1 にある**「利用者セグメント 2 から開発サーバセグメントへの通信」を拒否にする**ことで，開発サーバがマルウェアからアクセスされるリスクを軽減することができる。

(2) 図 2 の項番 1 にあるように，PC がマルウェアに感染してしまうリスクとして，ブラウザ又は PDF 閲覧ソフトの脆弱性の悪用による感染，他の PC 等からネットワークを介して感染，といったものがある。これらのリスクを軽減するために運用管理専用 PC で禁止することを単純に挙げると，①ブラウザ又は PDF 閲覧ソフトの利用，②ネットワークの利用，となるが，業務上②の禁止は不可である。①の禁止も困難と考えられるが，マルウェアはブラウザや PDF 閲覧ソフトに限らず，様々なソフトウェアの脆弱性を悪用して感染するため，使用するソフトウェアを限定すれば，感染リスクを軽減することができる。運用管理専用 PC であれば，**運用サーバセグメントの管理に必要のないソフトウェアの利用**を禁止することが，マルウェア感染のリスクを軽減する策となる。

■設問 4

〔試験センターによる解答例〕

(1) b：7

c：69^i

d：14

e：95^i

(2) 同じパスワードでもソルトが異なるとハッシュ値が変わるから (28 字)

(1)

b：表 5 にあるように，L1 ハッシュでは，パスワードが 8 字以上の場合は前半 7 字と残り

に分割し，それぞれのハッシュ値を計算し，その 2 個の結果を結合して格納する。したがって，14 字までのパスワードを解析する場合には，まず前半 **7 字**までについて最大個のハッシュ値を求めれば，後半 7 字についても同じハッシュ値を使って解析することができる。

c：解析するパスワードの長さは 1～7 字の範囲であり，パスワードの文字種は 69 種類であるため，1 字のパスワードのハッシュ値は 69 個，2 字のパスワードのハッシュ値は69^2個，3 字のパスワードのハッシュ値は69^3個（以降の文字数も同様）となる。つまり，1～7 字の範囲のパスワードを解析するのに必要なハッシュ値の個数は，$69^1 + 69^2 + 69^3 + 69^4 + 69^5 + 69^6 + 69^7$ となる。これをΣを使って表すと，指数を i として，その最小値（i＝1）をΣの下，最大値（7）をΣの上，Σの右側には和を求める計算式である「$\mathbf{69^{\mathit{i}}}$」を記載する。

d，e：L2 ハッシュではパスワードの文字種は 95 種類であり，パスワードの文字列分割は行わない。そのため，**14 字**までのパスワードを解析する場合に必要となるハッシュ値の最大個数は，「$\mathbf{95^{\mathit{i}}}$」の計算式に 1 から 14 までを代入した総和となる。

(2) ソルトとは，パスワードからハッシュ値を求める際に，パスワードに付加する文字列のことである。ソルトには，ユーザごとにランダムな文字列であることと，ある程度の長さ（少なくとも 20 文字程度）であることが求められる。これらの要件を満たしたソルトを使用することにより，同じパスワードであってもハッシュ値が変わるため，ハッシュ値から元のパスワードを特定することが困難になる。