平成 29 年度 秋期 情報処理安全確保支援士

＜午後Ⅰ解答・解説＞

＜問 1＞ ランサムウェアへの対策

■設問 1

［試験センターによる解答例］

イ

表 1 のセキュリティインシデントのタイムラインを見ると，No.7, No.8 に「ファイルが暗号化された」ことが事象として記載されている。ファイルが暗号化された時刻は更新日時により確認できる。

■設問 2

［試験センターによる解答例］

(1) a：オ
　b：エ

(2) バックアップ終了時刻（10 字）

(3) 営業用 PC の設定：D サーバ上の共有フォルダをネットワークドライブとして割り当てる。（32 字）

ランサムウェア X の特徴：ネットワークドライブ上のファイルも暗号化の対象となる。（27 字）

(4) D サーバと G サーバのファイルの暗号化（18 字）

(1)

a：ファイル名の文字表示を逆転させることができる Unicode の制御文字は RLO（Right-to-Left Override）である。RLO はファイル名の文字の並びを右から左に向かって読むように変更する制御文字であり，通常はアラビア語などを表記する際に使われる。

b：経由したメールサーバを調べる際に使われるメールヘッダは Received フィールドである。Received フィールドはメールの受信・中継履歴であり，メールがサーバなどを経由するたびに追加される。最初にメールを受信・中継したサーバの情報がメールヘッダの一番下となり，メールヘッダの一番上の Received フィールドが最後に経由したサーバが記録した情報となる。

(2) 問題文の冒頭に「ジョブのログには，バックアップの開始と終了の時刻，総ファイル数，ジョブ実行結果などが記録される」とある。IPA が公開している採点講評にもあるように，バックアップの取得には時間が掛かるため，その間にランサムウェアが暗号化を行うと，バックアップファイルの中に暗号化されてしまったファイルが含まれてしまう可能性がある。したがって，復元に利用するバックアップデータを選択する際には，感染開始時刻とバックアップ終了時刻を比較するべきである。

(3) 問題文の冒頭に「B 社の全ての PC は，ログオン時に，D サーバへも一般利用者権限で自動的にログオンされ，D サーバ上の共有フォルダが Windows のファイル共有機能を使って各 PC の D ドライブとして自動的に割り当てる」とあるように，営業用の PC には D サーバ上の共有フォルダがネットワークドライブとして割り当てられていたことがわかる。

また，ランサムウェア X については，L 君と J 氏の会話で J 氏が「アクセス可能なドライブをドライブレターのアルファベット順に探し，見つけたドライブ内のファイルを暗号化して上書き保存します。内蔵ドライブ，外付けドライブ，ネットワークドライブが対象です」と説明していることから，ネットワークドライブ上のファイルも暗号化の対象であることがわかる。

(4) 問題文の冒頭に「本社用 PC 及び営業用 PC では，一般利用者権限でログオンすると，自動的に G サーバへもその権限でログオンされ，G サーバ上の共有フォルダが各 PC の G ドライブとして自動的に割り当てられる」とあるように，D サーバと同様に営業用 PC05 に感染したランサムウェア X による被害を受けたことがわかる。ランサムウェア X は，アクセス可能なドライブをドライブレターのアルファベット順に探してファイルを暗号化することから，ランサムウェア X の起動直後に感染を検知して営業用 PC05 をネット

ワークから切り離していれば，D サーバと G サーバのファイルの暗号化は防ぐことができたと考えられる。

■設問 3

［試験センターによる解答例］

(1) c：可
d：可
e：可
f：不可
g：可
h：不可

(2) 復号に必要な共通鍵や秘密鍵が検体に含まれていないため（26 字）

(3) PC 内で一時的に作成されたメモリ上の共通鍵が消えてしまうため（30 字）

(1) 図 2 の項番 3 に「全ての出荷指示ファイルは，出荷担当者が内容の確認と更新をすることができる」とある。また，項番 7 に「営業担当者及び本社スタッフが，A アプリを使って D ドライブ上の出荷指示ファイルを閲覧し，最新の出荷状況を確認する。ただし，内容を確認するだけで更新はしない」とある。したがって，出荷担当者グループについては，出荷指示ファイルの読み，書きを「可」と設定する必要があるが，営業担当者グループと本社スタッフグループについては，同ファイルの読みのみを「可」とし，書きは「不可」と設定すれば良い。

(2) 下線④の前の文に「共通鍵暗号と公開鍵暗号を組み合わせて使うタイプでは，PC のメモリ上に一時的に作成する共通鍵で暗号化した上で，メモリ上からは共通鍵を消去する」とある。これを復号するためには，プログラム内にハードコードされた公開鍵とペアになっている秘密鍵を使って暗号化された共通鍵を復号した後，復号された共通鍵を使って対象ファイルを復号する必要がある。しかし，検体には公開鍵とペアになっている秘密鍵も共通鍵も含まれていないため，ファイルを復号するのは難しい。

(3) 下線⑤の文にあるように，ランサムウェア X の場合，暗号化に使用した共通鍵をメモリから消去しないため，PC を休止状態で保管しておけば，メモリ上の共通鍵を取り出し，

暗号化されたファイルを復号できる可能性がある。しかし，PC をシャットダウンするとメモリ上の共通鍵が消えてしまうため，暗号化されたファイルを復号できる可能性は低くなる。

■設問 4

［試験センターによる解答例］

共有フォルダのバックアップデータも暗号化されてしまい復元できなくなる。(35 字)

下線⑥に「ランサムウェア Y は，ファイルを暗号化するとともに，他のサーバや PC の OS の脆弱性を悪用し，管理者権限で次々と感染を広める」とある。問題文の冒頭にあるように，G サーバ上の共有フォルダの利用者データは，各コンピュータのローカルディスク上に設定された一般利用者権限ではアクセスできない領域にバックアップされている。そのため，G サーバにセキュリティパッチ P を適用せずに放置した場合，管理者権限でランサムウェア Y の感染が広がり，共有フォルダのバックアップデータも暗号化されてしまい，復元できなくなる可能性がある。

＜問 2＞ Web アプリケーション開発におけるセキュリティ対策

■設問 1

［試験センターによる解答例］

(1) ア：9
イ：11
必要な全てのコード：カ，ア，イ，ウ

(2) 21, 22, 23

(3) ウ

(1) SQL インジェクションは外部からの入力データを元に SQL 文を編集してデータベース（DB）に発行し，その結果を返すしくみになっている Web ページにおいて，不正な

SQL 文を発行することで DB を操作したり，DB に登録された情報を不正に取得したりする攻撃手法である。図 1 では，9 行目から 11 行目にかけて SQL 文を編集して DB に発行しているが，9 行目で WHERE 条件としている変数 cname は，5 行目で外部から受け取っているため，不正な文字列が混入している可能性がある。例えば，変数 cname に「' OR 'A' = 'A」という文字列が入っていた場合，9 行目で生成される SQL 文は次のようになる。

SELECT * FROM companylist WHERE cname = '' OR 'A' = 'A'

これは,「cname = ''」と, 常に真となる「'A' = 'A'」との OR 条件であるため, companylist の全てのデータが選択されることになる。したがって，この 9 行目から 11 行目までを適切なコードに置き換える必要がある。

解答群のコードは，SQL インジェクション対策としてバインド機構を用いたものである。**バインド機構**とは，変数部分にプレースホルダと呼ばれる特殊文字（"?"）を使用して SQL 文の雛形をあらかじめ用意しておき，後からそこに実際の値を割り当てて SQL 文を完成させる方式である。割り当てられる変数は完全な数値定数もしくは文字列定数として扱われるため，変数の中に SQL 文として特別な意味をもつ文字が含まれていたとしても，それらは自動的にエスケープ処理され，単なる文字として認識される。

まず，プレースホルダを使用して SQL 文の雛形を用意するため，9 行目を"カ"のコードに置き換える。続いて, 用意した SQL 文の雛形に変数 cname の値を割り当てるため，10 行目を"ア", "イ"のコードに置き換える。最後に 11 行目で SQL 文を実行するが，変数"sql"に格納した SQL 文は"ア"のコードで既に引数として渡しているため，引数のない"ウ"のコードに置き換える。

(2) XSS は，外部からの入力データ等を画面に出力する際に，不正なスクリプトが混入して実行されてしまう脆弱性である。図 1 でこのような処理を行っているのは DB から抽出した値を出力している 21～23 行目である。SQL インジェクションによって DB の値が不正なスクリプト文字列に書き換えられているかもしれないため，21～23 行目で XSS 脆弱性を招く可能性を否定できない。

(3) XSS の基本的な対策を次に挙げる。

① HTTP レスポンスヘッダの Content-Type フィールドに文字コードを指定する
② タグの属性値を必ずダブルクォート（二重引用符）で囲む
③ タグの属性値等に含まれるメタキャラクタのエスケープ処理を行う

③は，入力データに「<」「>」「&」などのメタキャラクタが存在した場合，HTML 出力時にそれらに対するエスケープ処理を行うものであり，解答群の"ウ"が該当する。

■設問 2

［試験センターによる解答例］

(1) a：エ
b：イ

(2) 認証後のリダイレクト先の URL を，W システムの FQDN のものに限定する。(36 字)

(1)

a：Cookie 発行の際，TLS 通信時だけ Cookie をブラウザから送信するようにするのは Secure 属性である。この属性を指定することにより，パケット盗聴によって Cookie が盗まれるのを防ぐことが可能となる。

b：JavaScript から Cookie を操作できないようにするのは HttpOnly 属性である。この属性を指定することにより，Cookie の適用範囲を HTTP/HTTPS 通信だけに限定し，ブラウザで実行されたスクリプトが"document.cookie"を用いて Cookie を操作することを禁止することが可能となる。

(2)「W システムの URL である https://w-system.a-sha.jp/ で動作する Web アプリケーションにおいて，W システムにログインしていない状態で，https://w-system.a-sha.jp/dashboard.jsp という URL にアクセスすると，図 3 のように生成された URL へリダイレクトされる」とある。そのため，攻撃者が任意の URL を W システムで動作する Web アプリケーションに引き渡す不正なリンクを用意し，そこに W システムの利用者を誘導してクリックさせれば，任意のサイトにリダイレクトさせることが可能となる。これがオープンリダイレクタの問題である。W システムの画面はわずか 8 ページであるため，その FQDN をリダイレクト先のホワイトリストとして登録することで，この問題を防ぐことができる。

■設問 3

［試験センターによる解答例］

(1) セキュリティ検査を本番システムに対し行うこと（22 字）

(2) ブラウザによっては XSS 攻撃を遮断する機能をもつから（26 字）

(3) W システムで当該脆弱性に対処する前に始まる攻撃によって，セキュリティ侵害されてしまうリスク（45 字）

(1) 問題文の〔W システムの実装に関する脆弱性〕にあるように，今回指摘された脆弱性は検査すべき項目の中に含まれており，開発用 PC 上のコードでは修正済みであったが，F 氏が本番システムに修正版をデプロイし忘れていたため，本番システムに脆弱性が残存したままとなっていた。このような問題を防ぐためには，本番システムに対してもセキュリティ検査を実施するよう手順を見直すのが有効である。

(2) Internet Explorer, Edge, Google Chrome, Safari など，一部のブラウザには XSS フィルタと呼ばれる XSS 攻撃の遮断機能が実装されている。そのため，K 氏によるブラウザを用いた検査では XSS 攻撃の試みを完遂できないことがある。

(3) 問題文の〔脆弱性対策の強化〕にあるように，S サービスでは，Web システムに脆弱性が発見された際，短時間で適切なシグネチャが WAF に追加される。このサービスを利用していれば，W システムで脆弱性が発見され，当該脆弱性に対処する前に始まる攻撃によってセキュリティ侵害されてしまうリスクを低減することができる。

＜問 3＞ SSL/TLS を用いたサーバの設定と運用

■設問 1

［試験センターによる解答例］

(1) a：コ
b：カ
c：オ
d：イ

(2) 正規の EC サイトの URL でアクセスしたときに，偽の EC サイトに誘導する。(36 字)

(3) エ

(1)

a：サーバ証明書の作成とその検証に利用しており，公開鍵暗号方式を使用した技術であるから，解答群で該当するのは「ディジタル署名」である。

b：SSL/TLS で，データの送受信時に暗号化と復号のために利用するのは「共通鍵暗号」である。

c：データの送信者と受信者が共通鍵暗号で使用する鍵を共有するために，公開鍵暗号方式を用いて行うのは「鍵交換」である。

d：サーバ証明書としてドメイン証明書とともに広く使用されているのは「EV 証明書」である。**EV（Extended Validation）証明書**とは，従来のディジタル証明書よりも，発行にあたっての審査基準を厳しく設定しており，組織が法的かつ物理的に実在することや，その組織が証明書に記載されるドメインの所有者であることが求められる。

(2) DNS キャッシュポイズニング攻撃は，DNS のキャッシュに偽の名前解決情報を登録することで，利用者を不正なサイトに誘導する手法である。攻撃者は，C 社の EC サイトを複製した偽の EC サイトを立ち上げた後，DNS キャッシュポイズニング攻撃で偽の名前解決情報を DNS キャッシュサーバに登録することにより，利用者が正規の EC サイトの URL でアクセスしたときに偽の EC サイトに誘導する。

(3) 擬似乱数生成器が生成する擬似乱数に規則性があったり，特定の文字が出現しやすかったり，同じ文字列が生成されるまでの周期が短かったりすれば，攻撃者によって推測される可能性が高まる。擬似乱数には予測不可能であることが求められる。

■設問 2

［試験センターによる解答例］

(1) ア：利用（2 字）
　　イ：失効（2 字）

(2)・鍵が危たい化した Web サイトの FQDN（19 字）
　　・鍵が危たい化したと思われる日時（15 字）

(3) g：鍵ペア（3 字）

(1) サーバ証明書に対する秘密鍵が危たい化した場合には，当該サーバ証明書の利用を停止するとともに，発行元に対して失効申請を行う必要がある。サーバ証明書等の失効情報は CRL（Certificate Revocation List）に登録される。CRL は有効期限内に失効させる必要が生じたサーバ証明書等が登録されたリストであり，認証局（CA）から随時発行される。

(2) 問題文の〔社外からの通報〕で H 氏が説明しているように，サーバ証明書にはサーバの FQDN と公開鍵が記載されている。サーバの利用者が自身の被害の可能性を判断できるようにするためには，まず鍵が危たい化した Web サイトの FQDN を公表する必要がある。また，鍵の危たい化が発生したと思われる日時を公表することも重要である。

(3) 秘密鍵が危たい化した場合に，システムを復旧させるには，鍵ペアを生成した上で，生成した新たな公開鍵が記載されたサーバ証明書の発行を受ける必要がある。

■設問 3

［試験センターによる解答例］

(1) SSL3.0 を利用しない設定にする。(18 字)

(2) ウ，オ

(3) エ

(4) ドメイン認証証明書ではサーバの運営者が C 社であることを確認できないから (35 字)

(1) 図 4 の POODLE 攻撃の概要に「SSL3.0 プロトコルのパディングチェックの脆弱性を利用した攻撃であり，ソフトウェアの開発時に起こり得る実装上のミスによる脆弱性を利用するものではない」とあることから，SSL3.0 のプロトコルに問題があることがわかる。また，TLS1.0 以降のプロトコルについては「攻撃の可能性はあるが，実装上の問題がなければ成功は困難と考えられている」とある。これらのことから，各サーバに SSL3.0 を利用しない設定を施すことで，POODLE 攻撃を受ける脆弱性に対処することが可能と判断できる。

(2) PFS とは，暗号化されたデータと秘密鍵が漏えいした場合であっても，過去の暗号データを復号することが不可能であるという性質であり，前方秘匿性と訳される。解答群の中でこれに該当するのは，DHE（Ephemeral Diffie-Hellman）と ECDHE（Elliptic Curve Diffie-Hellman Exchange）である。

(3) RSA の鍵が危たい化したことにより，攻撃者はセッション鍵を共有するための秘密情報を復号し，そこからセッション鍵を取得することが可能となる。これにより，攻撃者によって取得された危たい化前後における通信データを全て復号されてしまうおそれがある。

(4) 前述のように，EV 証明書の場合，発行に際に組織が法的かつ物理的に実在することや，その組織が証明書に記載されるドメインの所有者であることが求められる。一方ドメイン認証証明書では，発行の際にドメインの所有名義について確認するのみで，組織の実在性については確認しない。そのため，サイトの利用者はサーバの運営者が C 社であることを確認することができないことになり，新たに立ち上げた EC サイトが使用するサーバ証明書として適切とはいえない。