平成30年度 春期 情報処理安全確保支援士

＜午後Ⅰ解答・解説＞

＜問1＞　ソフトウェアの脆弱性

■設問1

[試験センターによる解答例]

a：カ
b：ウ

a：解答群の中で，確保済みメモリ領域を超えてデータを書き込んでしまうことで任意の攻撃コードが実行され得る脆弱性は「バッファオーバフロー」である。

b：解答群の中で，解放したメモリ領域を後から使用してしまう脆弱性に該当するのは「Use-After-Free」である。

■設問2

[試験センターによる解答例]

785634120a（10字）

問題文にあるように，図3の(1)でCreateNoteメンバ関数によって確保されていたNote構造体用のメモリ領域が，図3の(2)でDeleteNoteメンバ関数によって解放され，その後図3の(3)でRegisterNameメンバ関数が呼ばれた場合，char[8]用のメモリ領域が図3の(1)で確保されていた領域と同じアドレスに割り当てられる可能性がある。その場合，RegisterNameメンバ関数で読み込まれる攻撃者の入力値により，元々Note構造体用であったメモリ領域が上書きされることになる。設問は攻撃者の指定したアドレスが0x12345678，改行コードが0x0aであった場合の入力値の具体的なバイト列であるが，その前提として，アドレスは32ビット，バイトオーダがリトルエンディアンのバイトマシンによって扱われるものとしている。

攻撃者の入力値が読み込まれるのは図1の22行目のscanf関数であり，入力値の後に改行コードが続いていることが分かる。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。したがって，アドレス 0x12345678 は 78563412 となり，これに改行コードの 0a が続くため，入力値のバイト列は 785634120a となる。なお，リトルエンディアンとは逆に，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。

■設問 3

[試験センターによる解答例]

c：(エ)

問題文に「次に CreateNote メンバ関数が呼び出された際，攻撃コードに処理が遷移することになる」とある。図 1 の 13 行目にあるように，CreateNote メンバ関数内で使われているライブラリ関数は new であり，表 1 でこれに該当するアドレスは(エ)の 0x08049e40 である。

■設問 4

[試験センターによる解答例]

d：0x0b123400

問題文に「m_note->msg が指し示すメモリ領域に攻撃コードが書き込まれていて，その先頭アドレスが 0x0b123400 と分かっていたとする」とあるので，アドレス 0x08049e40 に書き込む値は 0x0b123400 である。

■設問 5

[試験センターによる解答例]

e：ヒープ

図 1 の 26 行目にあるように，RegisterMsg メンバ関数では，new で 100 バイトのメモリ領域を確保している。このように，new で動的に確保した場合に用いられるのはヒープ領域である。

■設問 6

[試験センターによる解答例]

ライブラリ関数はデータ実行防止の対象ではないメモリ領域に配置されているから（37 字）

データ実行防止（Data Execution Prevention：DEP）とは，指定されたメモリ領域でのコードの実行を禁止する機能であり，バッファオーバフロー攻撃の対策として有効である。しかし，ライブラリ関数は DEP の対象ではないメモリ領域に配置されているため，関数テーブルに書き込むアドレスとして共有ライブラリ内のメモリアドレスを選べば，DEP が有効化されていた場合でも，攻撃者は任意のコードを実行できる可能性がある。

■設問 7

[試験センターによる解答例]

f：（ア）

/bin/sh を起動して任意のシェルコマンドを実行するには system 関数を用いる。表 2 でこれに該当するアドレスは（ア）の 0xf7cc8da0 である。

■設問 8

[試験センターによる解答例]

g：DisplayNote

ASLR が有効化されていた場合でも共有ライブラリ内のメモリアドレスを特定するには，メモリアドレスを出力する必要がある。図 1 でこれに利用できそうなメンバ関数を探すと，

printf 関数でメモリの内容を出力している DisplayNote が該当する。

■設問 9

[試験センターによる解答例]

h：m_note = NULL;

図 1 の 37～39 行目で delete を用いて Note 構造体のメモリ領域を解放しているが，m_note を初期化していないため，元の値が残ったままになっている。これを修正するには，図 1 の 39 行目の直後に "m_note = NULL;" という 1 文を加え，m_note を初期化すればよい。

＜問 2＞ 情報セキュリティ対策の強化

■設問 1

[試験センターによる解答例]

(1) a：x1.y1.z1.4
(2) b：迷惑メール対策サーバ
c：Web メールサーバ
d：外部メールサーバ

(1) 図 2 の TXT レコードは SPF の設定であり，T 社からインターネットにメールを送信するサーバの IP アドレスを登録する。表 2 にあるように，T 社でその機能をもつサーバは外部メールサーバである。したがって [a] には"x1.y1.z1.4"が入る。

(2)

b：インターネットからのメールを最初に受信するサーバは，不審なメールや迷惑メールを破棄する機能をもつ「迷惑メール対策サーバ」である。

c：表 2 の「迷惑メール対策サーバ」の機能の概要に「受信したメールを Web メールサーバに SMTP で転送する」とあるように，[c] には「Web メールサーバ」が入る。

d：「Web メールサーバ」からのメールを受信し，インターネットに送信するサーバであるから，[d] には「外部メールサーバ」が入る。

■設問 2

［試験センターによる解答例］

(1) e：インターネット上のドメイン名についての名前解決（23 字）
(2)・インターネットへのメールの送信を許可されていない従業員が，送信できるという問題（39 字）
・送信者メールアドレスを詐称したメールを送信できるという問題（29 字）
・マルウェアのスキャンを行わずにメールを送信できるという問題（29 字）
※上記の中から二つ。

(1) 表 2 の DNS サーバの機能に「インターネット上のドメイン名の名前解決を行う」とあるが，オープンリゾルバは，問合せ元のアドレス等の制限なく，インターネットからの名前解決要求にも応じる DNS サーバである。オープンリゾルバは，DNS キャッシュポイズニング攻撃や DNS リフレクション攻撃（DNS amp 攻撃）に対して脆弱である。これを防ぐには，インターネット上のドメイン名についての名前解決を，DMZ 上の他のサーバからのみに制限するのが有効である。

(2) T 社の PC が，図 3 の CONNECT メソッドを悪用したリクエストをプロキシサーバに送ると，Web メールサーバを回避して，外部メールサーバと SMTP 通信し，インターネットにメールを送信することが可能となる。表 1 の Web メールサーバの機能の中で，T 社の PC がインターネットにメールを送る際のセキュリティ対策として有効であり，回避されると問題となるものとして次の 3 つが挙げられる。

・SMTP 通信のマルウェアスキャン機能
・送信メールについて，送信者メールアドレスをメールアカウントに対応付ける送信者メールアドレス詐称防止機能
・インターネットへの送信メールについて，送信者メールアドレスごとにインターネットへの送信の可否を設定できるインターネットメール送信制限機能

これらの中で，2 つを回避によって生じる問題として解答すればよい。

■設問3

[試験センターによる解答例]

(1) 運用PCからの接続も拒否するように変更する。(22字)
(2) 運用PCから接続できるURLは，T社標準ソフトのベンダのサイトのものだけに制限するように変更する。(49字)

(1) 表1にあるように，Webメールサーバの HTTP 接続拒否機能は，IP アドレス単位で HTTP による接続を拒否することができる機能で，内部システム LAN 上の他のサーバからの接続を拒否している。Web メールサーバは，HTTP を用いて PC の Web ブラウザでメールを送受信できる機能を提供しているが，運用 PC についてはメールの送受信を制限する必要がある。そのため，Web メールサーバの HTTP 接続拒否機能により，運用 PC からの HTTP 接続を拒否するよう設定を変更する。

(2) 表2にあるように，プロキシサーバでは送信元 IP アドレスごとに接続可能な URL を制限するアクセス制限機能があるが，現在は全ての URL への接続を許可している。運用 PC はインターネットの Web 閲覧を制限する必要があるが，問題文の冒頭にあるように，T 社の PC 及びサーバは，プロキシサーバ経由で T 社標準ソフトの各ベンダのサイトに毎月1回自動で接続し，それぞれの脆弱性修正プログラムを適用している。運用 PC についてもこの対応は必要であるため，プロキシサーバのアクセス制限機能を用いて，運用 PC が接続できる URL を，T 社標準ソフトのベンダのサイトのものだけに制限するように変更する。

＜問3＞ LANの分離

■設問1

[試験センターによる解答例]

(1) a：ウ
　　b：エ
(2) c：ア
　　d：ウ
※c，dは順不同。

(1) JIS Q 31000:2010（リスクマネジメント－原則及び指針），JIS Q 31010:2012（リスクマネジメント－リスクアセスメント技法）では，リスクアセスメントを「リスク特定，リスク分析及びリスク評価のプロセス」としている。したがって，［ a ］にはウの「リスク特定」，［ b ］にはエの「リスク評価」が入る。

(2) JIS Q 31000:2010 ではリスクレベルを「結果とその起こりやすさとの組合せ」と定義している。この「結果」とは「リスクが顕在化したときの結果」であり，「起こりやすさ」とは「リスクの起こりやすさ」である。したがって［ c ］，［ d ］には，ア，ウが入る。（順不同）

■設問 2

［試験センターによる解答例］

(1) ファイル転送サーバから研究開発 PC への通信は FW2 で禁止されているから（35 字）
(2) e：利用者 ID（5 字）
f：パスワード（5 字）
g：アップロード用 URL（10 字）
※e，f，g は順不同。
方法：事務 PC の HTTP リクエストを監視する。（20 字）
(3) 研究開発 PC からファイル転送サーバにアクセスして，ファイルをダウンロードする必要があるから（45 字）

(1) ファイル転送サーバに感染したマルウェア α が研究開発 PC が感染を広げるには，FW2 を介して通信を確立させる必要があるが，表 3 にあるように，FW2 では研究開発 PC からファイル転送サーバへの必要な通信のみが許可されており，ファイル転送サーバから研究開発 PC への通信は禁止されている。そのため，A 氏は下線①のように判断したのである。

(2) 図 4 の 1 に「研究開発 PC の Web ブラウザからファイル転送サーバのアップロード用 URL にアクセスし，表示される画面で利用者ごとに異なる利用者 ID 及びパスワードを入力してログインする」とある。また，図 4 の注記に「事務 PC から研究開発 PC へのファイル転送時の操作手順は，図中の研究開発 PC を事務 PC に，事務 PC を研究開発 PC に，それぞれ置き換えて読むものとする」とある。したがって，事務 PC に感染したマルウェア β が不正なファイルをファイル転送サーバにアップロードするには，利用者 ID，

パスワード，アップロード用 URL，の 3 つの情報が必要であり，[e]，[f]，[g]にはこの 3 つの情報が入る。（順不同）

上記の事務 PC からファイル転送サーバへのアクセスは，事務 PC の Web ブラウザからの HTTP 通信で行われているため，事務 PC の HTTP リクエストを監視すれば，ファイル転送サーバにアクセスするために必要な情報を窃取することが可能である。

(3) ファイル転送サーバにアップロードされた不正なファイルが原因となって研究開発 PC が感染するには，N 社の研究開発員が研究開発 PC からファイル転送サーバにアクセスして，当該不正ファイルをダウンロードする必要がある。図 4 の 4 にあるように，ファイル転送サーバからファイルをダウンロードする際には，アップロードされたファイルの一覧を表示し，そこからファイルを選択する。このとき，マルウェアβがアップロードした不正なファイルが一覧に表示されたとしても，N 社の研究開発員が当該ファイルを選択してダウンロードする可能性は低いと考えられる。

■設問 3

［試験センターによる解答例］

h：高い
i：通信経路上に感染活動を遮断する機器が存在しないから（25 字）
j：低い
k：FW2 によって感染活動を遮断できるから（19 字）

表 5 より，研究開発 PC，配信サーバは OS-P を利用しているため，マルウェアγに感染する可能性がある。図 3 中の（あ）に配信サーバを設置した場合には，研究開発 PC と配信サーバの間は L2SW のみとなり，通信経路上にマルウェアγの感染活動を遮断する機器は存在しない。そのため，研究開発 PC から配信サーバに感染が拡大する可能性が高い。

一方，図 3 中の（い）に配信サーバを設置した場合には，研究開発 PC と配信サーバの間は L2SW だけでなく，FW2 がある。FW2 では，必要最小限の通信だけを許可しているため，マルウェアγの感染活動を遮断できると考えられる。したがって，研究開発 PC から配信サーバにマルウェアγの感染が拡大する可能性は低い。

■設問 4

［試験センターによる解答例］

ｉ：上長による承認（7 字）

図 4 の手順 2 にあるように，ファイルをアップロードする際にその正当性を確認する手順はなく，アップロードが完了すると即座にダウンロードが可能となる。そのため，研究開発 PC，事務 PC の双方にマルウェアが感染していた場合には，不正なアップロード，ダウンロードが行われ，インターネットへのファイルの流出に至る可能性がある。これを防ぐには，図 4 の手順 2 の後に上長による承認の手順を追加し，その手順の完了をもってダウンロードが可能となるようにするのが効果的である。