平成 26 年度 春期 情報セキュリティスペシャリスト

＜午後 I　解答･解説＞

＜問1＞ Web アプリケーション

■設問 1

〔試験センターによる解答例〕

(1) Referer（7 字）

(2) ブラウザの設定でスクリプトを無効化する。(20 字)

(3) Web アプリケーションで拡張子判定を行う。(21 字)

(1) GET メソッドを使用した場合にバナー広告に設定されたリンク先の Web サーバへセッション ID が漏えいする原因となる HTTP ヘッダ内のフィールドであるから，該当するのは Referer である。

Referer ヘッダには，ある Web ページにアクセスした際にどのリンクをたどってきたのか確認できるように，リンク元の URL が格納される。GET メソッドを使用している場合には，Referer ヘッダにはクエリパラメタも含めた URL が格納されている。そのため，セッション ID をクエリパラメタの中に格納する方式を採用すれば，バナー広告に設定されたリンク先の Web サーバへセッション ID が漏えいする可能性がある。

(2) スクリプトは**ブラウザの設定によって容易に無効化**することができる。そのため，契約者の操作によって拡張子の判定処理が回避され，拡張子が画像ファイルのものではないファイルがアップロードされてしまう可能性がある。

(3) スクリプトを使用せずにアップロードするファイルの拡張子の判定を行うには，サーバで実行される Web アプリケーションを使用する。Web アプリケーションであれば，深刻な脆弱性などがない限り，契約者の操作によって拡張子の判定処理が回避されることはない。

■設問 2

〔試験センターによる解答例〕

(1)

a：整数オーバフロー（8 字）

b：バッファオーバフロー（10 字）

(2) ヘッダ部の列数と各ピクセルのバイト数の積にパディングを加えたものと，行数の積が kMaxInteger を超える。(55 字)

(1) a：図 6 の 38 行目では，int 型（4 バイト）の"bytesOfRow"と，short int 型（2 バイト）の"fhBuf.rows"の積を，int 型（4 バイト）の"bytesOfBuff"に格納している。そのため，"bytesOfRow"と"fhBuf.rows"の値により桁あふれが発生する可能性がある。このように，整数の演算結果が格納先の上限を超えることを「**整数オーバフロー**」，整数オーバフローの脆弱性を悪用した攻撃を「整数オーバフロー攻撃」という。C/C++言語では，整数オーバフローが発生したとしてもエラーとして検出されないため，プログラム開発者が自前で検出したり回避したりする処理を組み込む必要がある。

b：図 6 の 41 行目では，malloc 関数によって"bytesOfBuff"に格納された値のサイズでメモリを確保し，そのポインタを"pixBuf"に格納している。このとき，"bytesOfBuff"が整数オーバフローを起こしていれば，確保されるメモリのサイズは実際に必要なサイズよりも小さくなるため，50 行目でファイル fp から読み込んだデータを"pixBuf"に書き込む際に**バッファオーバフロー**が発生する可能性がある。

(2) 図 6 の 11 行目に定義されている"kMaxInteger"は，符号付きの int 型（4 バイト）に格納可能な最大値を表している。図 6 の 36 行目で，ヘッダ部の列数"fhBuf.cols"と，各ピクセルのバイト数"fhBuf.colors"の積を求めた後，37 行目で各行の先頭を 256 バイト境界に調整するため，パディングしている。続く 38 行目では，パディング後の値が格納された変数"bytesOfRow"と，ヘッダ部の行数"fhBuf.rows"の積を求めているが，この積が"kMaxInteger"の超える場合に整数オーバフローが発生する。
なお，ここで注意が必要なのは，実際の画像ファイルのサイズではなく，あくまでもヘッダ部に格納された列数，行数などによる計算結果が条件になるということである。したがって，ヘッダ部が意図的に改ざんされた場合にも整数オーバフローが発生する可能性がある。

■設問３

〔試験センターによる解答例〕

ア群

c：kMaxInteger / fhBuf.rows

d：bytesOfRow

イ群

c：kMaxInteger / bytesOfRow

d：fhBuf.rows

※同じ群中の組合せとする

整数オーバフローを回避するためには，図 6 の 38 行目の処理の前に，"bytesOfRow"と"fhBuf.rows"の積が"kMaxInteger"を超えていないかチェックする必要がある。これを図 7 の空欄部分になぞらえて単純に不等式で表すと下記となる。

kMaxInteger < bytesOfRow * fhBuf.rows

しかし，このままでは不等式の右辺を計算する際に整数オーバフローが発生してしまう可能性がある。解決策としては，"bytesOfRow * fhBuf.rows"とならないように，不等式を下記のいずれかの形に変換することである。

kMaxInteger / fhBuf.rows < bytesOfRow
kMaxInteger / bytesOfRow < fhBuf.rows

こうすることで，整数オーバフローの発生を防ぐことが可能となる。

＜問2＞ インターネット接続システムにおける迷惑メール対策

■設問 1

〔試験センターによる解答例〕

(1) a：syslog（6 字）

(2) b：-all（4 字）

(1) UNIX でログ収集，転送するために一般的に使われているプロトコルは"**syslog**"である。

(2) SPF レコードでは，設定した IP アドレス以外の IP アドレスからのメールを認めない場合には，末尾を"-all"とする。A 社のメールアドレスを使ったメールを送信するのは外部メールサーバだけであるから，［ b ］には"**-all**"が入る。

■設問２

〔試験センターによる解答例〕

インターネットから迷惑メール対策装置を経由せずに送られていた。(31 字)

全ての機器が設定どおりに動作している状態でありながら迷惑メールの数が増加したことから，迷惑メール対策装置を経由せずにメールが送られたことが推測される。まず表１の「外部メールサーバ」の機能概要を見ると，「迷惑メール対策装置の故障に備えて，インターネットから内部メールサーバへのメール転送も行うことができる」とある。そのため，表２では項番２でインターネットから外部メールサーバへの SMTP が許可されており，項番５で外部メールサーバから内部メールサーバへの SMTP が許可されている。また，図３を見ると，迷惑メール対策装置より優先順位は低いものの，外部メールサーバが MX レコードに登録されていることがわかる。この DNS への登録内容は，攻撃者など悪意のある第三者が参照することが可能である。

■設問３

〔試験センターによる解答例〕

(1) メールサーバの IP アドレスが変更された場合（21 字）

(2) 迷惑メールの送信者がドメインを正当に取得した場合（24 字）

(3)

c：プロキシサーバ

効果：迷惑メールの拒否率向上（11 字）

(1) IP アドレス WL には，メールの転送を許可する取引先のメールサーバの IP アドレスが登録されている。取引先のシステム構成変更や ISP の変更などにより，**メールサーバの IP アドレスが変更される**場合がある。その際には IP アドレス WL を見直す必要がある。

(2)下線②の直前にある「SPF を使えばドメイン名を詐称する迷惑メールの拒否が可能である」という E 主任の説明が解答のヒントになる。これは，裏を返せば「ドメイン名が詐称されていない場合は SPF を使っても迷惑メールを拒否することができない」ということである。つまり，迷**惑メールの送信者がドメイン名を正当に取得**し，ドメイン名を詐称せずに迷惑メールを送ってきた場合は SPF では防ぐことができない。その

ような場合にはドメイン名 WL やドメイン名 BL への登録によって対処する必要がある。

(3) URL BL に登録するのであるから，登録するのは URL である。表 1 の各機器の機能概要を見ると，**プロキシサーバ**には，サーバ管理者が URL を登録することにより，URL フィルタリングを行う機能があることがわかる。プロキシサーバの BL には Web アクセスにおいて拒否すべき URL が登録されるが，そこに登録されるサイトが迷惑メールの発信源となっている可能性があるため，URL BL にも登録することで，**迷惑メールの拒否率が向上**することが期待される。

■設問 4

〔試験センターによる解答例〕

SMTP 通信を迷惑メール対策装置に振り分ける。(23 字)

下線④に「ネットワーク構成と LB の設定を変更することで，インターネット上のメールサーバからの SMTP 通信を制御することにした」とあり，表 1 の LB の機能概要を見ると，「HTTP，SMTP などのサービスの振分け機能」があることがわかる。従前の DNS による優先順位の設定のみでは，迷惑メール対策装置にメールを強制的に振り分けることはできないが，LB の振分け機能を用いれば，迷惑メール対策装置が正常に稼働していることを前提として，**SMTP 通信を迷惑メール対策装置に強制的に振り分ける**ことができる。その場合，表 2 の FW のルールについては，項番 1 の宛先を LB に変更し，項番 2 を削除する。また，図 3 の DNS の設定については，MX レコードに LB の情報のみを登録するよう変更する必要がある。

＜問3＞ インターネットを利用した銀行取引サービスを狙うマルウェアへの対策

■設問 1

〔試験センターによる解答例〕

(1) フィッシングサイト (9 字)

(2) 攻撃者はクライアント証明書がなく，ログインできないから (27 字)

(1) 本物のサイトと酷似した偽 Web サイトに利用者を誘導し，パスワードやクレジットカード番号などを入力させて盗む行為を「フィッシング」，その目的のために開設された Web サイトを「**フィッシングサイト**」と呼ぶ。

(2) 図 1 にあるように，法人利用者の利用手順では，個人利用者の利用手順とは異なり，クライアント証明書による TLS 接続を確立するための認証プロセスがあり，同プロセスにおいてクライアント証明書とそれに対応した秘密鍵が必要となる。そのため，マルウェア J によって法人利用者の利用者 ID とパスワードが盗まれたとしても，クライアント証明書とそれに対応した秘密鍵をもたない攻撃者は X ネットサービスとの間で TLS 接続と確立することができず，ログインすることはできない。こうしたことから金銭的な被害が発生する可能性は低いといえる。
なお，マルウェア J によってクライアント証明書と秘密鍵まで盗まれたとすれば金銭的な被害が発生する可能性があるが，図 1 の注記にあるように，秘密鍵はエクスポートできない状態で PC にインストールされている。そのため，マルウェア J によって秘密鍵が盗まれる可能性は極めて低いと考えられる。

■設問 2

〔試験センターによる解答例〕

(1) 利用者のブラウザに表示される警告画面を見て気付くことができる。(31 字)

(2)

a：123456

b：10000

目的：マルウェア K が書き換えた口座番号と送金額を利用者に隠すこと（29 字）

(1) サーバ証明書による認証では，次のような事項によって当該証明書の正当性を検証し，問題があった場合には使用者のブラウザに警告画面を表示する仕組みになっている。ただし，古いバージョンのブラウザでは脆弱性やバグによって警告画面が表示されない場合がある。

・サーバ証明書の有効期限が切れていないこと
・サーバ証明書が失効状態でないこと
・サーバ証明書のコモンネームとアクセス先の FQDN が一致すること
・サーバ証明書が信頼される認証機関から発行されていること（証明のパスをルート CA までたどって信頼性が確認できること）

そのため，中間者攻撃によって偽の Web サイトに誘導されたとしても，最新のブラウザを使っている利用者であれば**表示される警告画面を見て攻撃に気付くことができる**はずである。

(2) 攻撃者が書き換えた送金内容をそのまま送金確認画面に表示すれば利用者に気付かれてしまう。そのため，**マルウェア K は，自身が書き換えた送金内容を利用者に隠すこと**を目的として，送金確認画面には利用者が入力した口座番号「**123456**」と送金額「**10000**」を表示する。

■設問３

〔試験センターによる解答例〕

(1)

c：対策になる

d：対策になる

(2)

e：二要素（3 字）

(3) 利用者の PC がマルウェアに感染した場合，HMAC 計算ツールの入力内容も改ざんされる可能性がある。（48 字）

(1)

c：マルウェア J は，利用者 ID，パスワード，乱数表の情報を盗み，攻撃者はそれらを用いて不正な送金を行う。ワンタイムパスワード認証を採用した場合には認証のたびに要求するパスワードが変わり，入力すべきパスワードは専用デバイスに表示される仕組みとなる。そのため，攻撃者が利用者 ID，パスワード，乱数表の情報を入手していたとしても認証を成立させることはできない。したがって c には「**対策になる**」が入る。

d：送金内容認証を採用すると，送金する際に共通鍵を設定した HMAC 計算ツールが必要となる。そのため，マルウェア J が利用者 ID，パスワード，乱数表の情報を盗んだとしても正当な HMAC 値を計算することはできず，送金を行うことはできない。したがって d には「対策になる」が入る。

(2)

e：項番１と項番４の方式に限らず，二つの方式を組み合わせた認証方式を**二要素認証**という（「多要素認証」と呼ぶ場合もある）。また，インターネットと携帯電話網など，二つの経路で認証を行う方式を二経路認証という。

(3) HMAC 計算ツールを PC 用のプログラムで利用者に提供した場合には，マルウェア K が進化して HMAC 計算ツールにも対応し，**利用者の PC に感染したマルウェア K**

によって HMAC 計算ツールの入力内容が改ざんされる可能性がある。一方，HMAC 計算ツールを専用デバイスの形態で利用者に提供した場合には，利用者の PC にマルウェア K が感染したとしても HMAC 計算ツールにまでアクセスされることはないため，不正送金を防げる可能性が格段に高まる。