平成 28 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＞ 組込み機器を利用したシステムのセキュリティ対策

■設問 1

〔試験センターによる解答例〕

a：エ

b：ア

a：IPsec では，パケットを暗号化する対象部分によって，トランスポートモードとトンネルモードという二つの通信モードがある。

トランスポートモードは IPsec に対応したホスト同士が End-to-End で通信を行う場合に使用することを前提として，IP パケットのペイロード（データ部分）及び TCP ヘッダ（トランスポート層ヘッダ）のみを暗号化し，IP アドレスなどの IP ヘッダは暗号化せずに送信する。

トンネルモードは IP ヘッダとデータ部分をまとめてカプセル化して暗号化するとともに，新たな IP ヘッダを付加（カプセル化）して送信する方式であり，VPN 装置間で通信を全て暗号化する場合など，広く用いられている。したがって，［ a ］には「**トンネル**」が入る。

b：IKEv1 では，ISAKMP SA，IPsec SA の順番で SA（Security Association）を作成する。ISAKMP SA の作成にはメインモード，アグレッシブモードがあり，一方の IP アドレスが動的に変わる環境においてはアグレッシブモードを使用する必要がある。なお，IPsec SA の作成にはクイックモードが使用される。

IKEv2 では，メインモード，アグレッシブモードが統合化され，IP アドレスが動的に変わる環境にも標準で対応している。したがって，［ b ］には「**アグレッシブ**」が入る。

■設問 2

〔試験センターによる解答例〕

(1) c：x1.x2.x3.x4

d：y1.y2.y3.y4

(2) パスワード認証を無効化し，公開鍵認証を使用する。(24 字)

(1)
c : SSH サービスのポート番号は 22 番である。表 1 を見ると，6 行目でグルーバル IP アドレス「**x1.x2.x3.x4**」を送信元とした SSH 通信が確立していることがわかる。

d : SMTP のポート番号は 25 番である。表 1 の 6 行目で SSH 通信を確立後，7 行目でグローバル IP アドレス「**y1.y2.y3.y4**」を宛先とした SMTP 通信が確立していることがわかる。

(2) SSH では，ログイン認証方式として，パスワードのほか，公開鍵暗号技術を用いた公開鍵認証などが使用可能である。パスワード強度に依存しない方式であるから，**パスワード認証を無効化して，公開鍵認証に設定変更した**と考えられる。

■設問３

〔試験センターによる解答例〕

(1) e : 送信元 IP アドレスを監視端末の IP アドレスに限定 (24 字)

(2) 中間者攻撃による通信内容の盗聴 (15 字)

(3)

作成時：秘密鍵を使用してイメージファイルにディジタル署名を付与する。(30 字)

更新時：公開鍵を使用してイメージファイルのディジタル署名を検証する。(30 字)

(4) LTE ルータにログインしてファイルシステムの中から見つける。(30 字)

(1) e：TCPWrapper とは，Unix 環境で動作するホストベースの TCP アクセス制御機構であり，TCP の各ポートに対し，送信元 IP アドレスや宛て先 IP アドレス等でアクセス制限を行うことができる。監視端末を利用した場合にだけ SSH サービスにアクセスできる仕様にするには，TCP Wrapper を使用し，SSH サービスへの接続を許可する**送信元 IP アドレスを監視端末の IP アドレスに限定**すればよい。

(2) SSH のホスト鍵が同一モデルの組込み機器で同じになっているならば，攻撃者がその鍵を入手して正当な通信相手になりすまし，**中間者攻撃によって通信内容を盗聴**したり，改ざんしたりすることが考えられる。

(3) 電子データが改ざんされていないか検証するための技術としてディジタル署名がある。ディジタル署名では，まず対象となる電子データに対し，秘密鍵を用いてディジタル署名を付与する。その後，当該電子データが改ざんされていないか検証する際には対となっている公開鍵を用いてディジタル署名を検証する。したがって，イメージファイルの作成時には**秘密鍵を用いてディジタル署名を付与**し，更新時には対となる**公開鍵を用いてイメージファイルのディジタル署名を検証する**ことによって下線③を実現する。

(4) LTE ルータに保存されているイメージファイルを暗号化した場合，システム構成上，それを復号するための鍵は LTE ルータのファイルシステムのいずれかの場所に保存されることになる。したがって，攻撃者がそれを入手する方法としては，**LTE ルータに不正にログインし，ファイルシステムの中から見つけ出す**ことが考えられる。

＜問2＞ ソフトウェア開発における脆弱性対策

■設問 1

〔試験センターによる解答例〕

a：ア

b：イ

c：ウ

d：エ

a：脆弱性を識別するための識別子として，**CVE**（Common Vulnerabilities and Exposures：共通脆弱性識別子）が採用されている。CVE は個別の製品に含まれる脆弱性を対象としており，米国政府の支援を受けた非営利団体の MITRE 社が採番している。

b：脆弱性が発見された際に，その対処方法が公表されるよりも前に行われる攻撃を「ゼロデイ攻撃」，当該脆弱性を「**ゼロデイ脆弱性**」と呼ぶ。
c：特定の組織を狙う攻撃は「**標的型攻撃**」である。

d：極端に長い文字列や通常使わない制御コード等，通常の利用では想定しないデータ（これを「ファズ（fuzz)」という）を入力し，その応答から脆弱性を探す手法を**ファジング検査**という。

■設問２

〔試験センターによる解答例〕

(1) 呼出し元関数への戻りアドレス（14 字）

(2) ア：sample2

(1) スタックベース BOF 脆弱性を悪用する攻撃では，関数呼出し時にスタックに積まれる**呼出し元関数への戻りアドレス**の値を書き換えることで，開発者が意図しない命令を実行する。

(2) 通常実行可能ファイルには，そのファイルを実行したユーザの権限が設定されるが，実行権限の属性が“s”（“setuid（set userID)”もしくは“setgid（set groupID)”）の場合には，当該ファイルの所有者の権限，もしくは所有者が所属するグループの権限を一時的に設定する。そうすることで，一般ユーザなどが使用する実行可能ファイルの中で管理者の権限などを必要とする処理の実行を可能にする。図 1 の 4 つのファイルの中で，実行権限の属性が“s”となっているものとして“sample2”と“sample4”があるが，そのうち“**sample2**”は所有者が“root”であるため，一般権限者“suzuki”によって起動された場合でも“root”権限で動作する。

■設問３

〔試験センターによる解答例〕

(1) ウ

(2) 23

(3) イ，オ

(1) 図 2 のプログラム Y は，第 1 引数で指定された利用者 ID を基に登録済みパスワードを取得して pass に格納し，それと第 2 引数で指定されたパスワードを照合することで，“認証成功”，もしくは“認証失敗”の判定を行う。利用者 ID，パスワードを格納する変数は char 型 8 文字となっているが，23 行目でサイズを指定せずに利用者 ID を変数に格納しているため，取得した利用者 ID が 8 文字を超える長い文字列であった場合には，pass に格納された登録済みパスワードの値が書き換えられ，その結果利用者認証を回避される可能性がある。

　これが発生するのは，第 1 引数の末尾の文字列が第 2 引数と一致する場合であるため，

解答群で該当するのは**ウ**である。

(2) 上記の通り，ヒープベース BOF 脆弱性が存在するのは **23** 行目である。

(3) memcpy()関数， strncpy()関数は，第 3 引数で指定されたサイズの文字列を第 1 引数で指定された領域に格納する。図 2 の 20 行目で，第 1 引数 uid のサイズは“UID_SIZE+1”となっており，これと同じサイズの文字列を uid に格納する**イ**，**オ**の改修案であれば BOF の発生を防ぐことができる。

ただし，実際にはイ，オの場合，argv[1]の先頭から UID_SIZE+1 バイト以内に文字列の終端を示すナル（NULL）文字がない場合，uid に格納された文字列がナル文字で終端しないという別な問題が残る。本設問では BOF の発生個所を修正することが主題であるため，これは参考情報となるが，本来は下記のように記述する等して，格納される文字列をナル文字で終端させるべきである。

イの場合
```
memset(uid, 0, UID_SIZE+1);
memcpy(uid, argv[1], UID_SIZE);
```

オの場合
```
memset(uid, 0, UID_SIZE+1);
strncpy(uid, argv[1], UID_SIZE);
```

1 行目で uid をナル文字で埋めた後，2 行目で uid のサイズ-1 バイト分を格納している。そうすることで，BOF の発生を防ぐとともに uid に格納される文字列をナル文字で終端させる。

■設問 4

〔試験センターによる解答例〕

(1) ヒープメモリの確保方法が，メモリ確保のライブラリによって違うから（32 字）

(2) ヒープ領域を書き換える行為を防止できないから（22 字）

(1) 図 2 のプログラムでヒープベース BOF が発生するのは，uid を格納するヒープメモリ領域の後ろに pass を格納する同領域が確保されている場合である。実際には，**メモリ確保のライブラリの仕様によりヒープメモリの確保方法が異なる**ため，引数が同じであっても

利用者認証を回避されない場合もある。

(2) DEP 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，スタックベース BOF 脆弱性を悪用する攻撃を防ぐ対策となるが，**ヒープ領域を書き換える行為を防止することはできない**。

＜問3＞ プロキシサーバによるマルウェア対策

■設問１

〔試験センターによる解答例〕

a：エ

インターネットから Web サーバへの通信を中継する機能であるから，該当するのは「**リバースプロキシ**」である。

■設問２

〔試験センターによる解答例〕

(1) b：イ

c：オ

(2) プログラムの内容を変え，かつ，プログラム名を変える場合（27 字）

(1)

b：問題文にあるように，マルウェア Z が社員 PC 上にダウンロードした攻撃用プログラムが OS の管理用コマンドを複数ダウンロードして起動させ，サーバ情報を窃取した。したがって，社員 PC で起動禁止設定すべきプログラムは攻撃用プログラムと OS の管理用コマンドであり，解答群の**イ**が該当する。なお，マルウェア Z は単体のプログラムではなく，文書ファイルのマクロとして実装されているため，起動禁止設定することはできない。

c：管理 PC では，OS の管理用コマンドを起動禁止設定することはできないため，攻撃用プログラムのみ起動禁止設定を行う。したがって解答群の**エ**が該当する。

(2) プログラム名を指定して起動を禁止する方式では，プログラム名が変わると起動を防ぐ

ことができない。また，プログラムの実行ファイルのハッシュ値を指定して起動を禁止する方式では，プログラムの内容が変わるとハッシュ値も変わるため，起動を防ぐことができない。したがって，上記の二つの方式でプログラム起動禁止設定を行ったとしても，自身の名称と内容を変える攻撃プログラムについては起動を防ぐことができない。

■設問３

〔試験センターによる解答例〕

(1) 送信元 IP アドレスがプロキシ 1 の IP アドレスとなるので（27 字）

(2) d：オ

(1) フェーズ 1 では，社員 PC はインターネット接続時にはプロキシ 1 と通信しており，プロキシ 2 は，プロキシ 1 とインターネットへ間の通信を全て中継する構成となっている。そのため，プロキシ 2 が中継する通信の**送信元 IP アドレスは全てプロキシ 1 となり**，プロキシ 2 のログから送信元 PC を特定することはできない。

(2) フェーズ 1 のような構成において，送信元 PC の IP アドレスをプロキシ 2 で特定できるようにするために使用する HTTP ヘッダは“**X-Forwarded-For**”（XFF）ヘッダフィールドである。XFF は，プロキシサーバや負荷分散装置等を経由して通信するホストの送信元 IP アドレスを特定する用途で標準的に使用されるヘッダフィールドである。

■設問４

〔試験センターによる解答例〕

(1) Web ブラウザからプロキシサーバへの通信を盗聴して認証情報を取得し，プロキシサーバに送信する。(47 字)

(2)

URL フィルタリング機能：ホワイトリストに業務に必要かつ安全であることを確認した URL を設定する。(36 字)

カテゴリ単位フィルタリング機能：業務に不要であるカテゴリを遮断する。(18 字)

(1) プロキシ認証に対応したマルウェアは，まず感染した PC とプロキシサーバとの通信を**盗聴し，そこに含まれる認証情報を取得する**。続いて，取得した認証情報をそのまま**プロキ**

シサーバに送信し，認証を成功させる。このような機能を持つマルウェアは数多く存在し，プロキシの認証機能を危殆化させている。

(2) 問題文にあるように，プロキシ 2 のフィルタリング機能では，URL フィルタリングとカテゴリ単位フィルタリングで同じ URL が設定された場合は URL フィルタリングが優先される。また，URL フィルタリングのホワイトリストとブラックリストで同じ URL が設定された場合はホワイトリストの設定が優先させる。

このように，ホワイトリストの設定が最優先されるため，**業務に不要であるカテゴリをカテゴリ単位フィルタリング機能で遮断する**ように設定し，**業務に必要かつ安全であることを確認した URL を URL フィルタリング機能のホワイトリストに設定**し，許可すればよい。