平成 25 年度 秋期 情報セキュリティスペシャリスト

＜午後Ⅱ 解答･解説＞

＜問1＞ マルウェア感染への対策

■設問 1

〔試験センターによる解答例〕
(1)
行動①：不審と判断したファイルを削除した。(17 字)
行動②：OS 上で稼働するアプリケーションの自動起動設定を変更した。(29 字)
※上記①,②は順不同
理由：調査に必要な証跡が消えてしまう可能性があるから (23 字)
(2) 未検出のマルウェアが動作している可能性があるから (24 字)

(1) 〔マルウェアの検出〕にあるように,M さんはマルウェア P の駆除を確認した後,次のような行動をとっている。

①PC に新たなソフトウェアがインストールされていないか,PC 内のデータが消えてしまっていないかなどを確認
②不審と判断したファイルを削除
③OS 上で稼働するアプリケーションの自動起動設定を変更

これらの中で,その後の X 氏によるマルウェア感染の調査を困難にしてしまう行動が②と③であることは明白である。

マルウェア感染の調査を行うには,速やかに当該 PC をネットワークから切断し,ファイルや設定等を一切変更することなく,電源も切らずにそのままの状態を保全しておくのが望ましい。そうすることで,マルウェアの振る舞い,感染経路,影響等を調査することが可能となる。②,③のような行動をとってしまうと,マルウェアの調査に必要な各種の記録,証跡が失われてしまう可能性がある。

(2) 図 2 にあるように,マルウェア P は C&C サーバからファイルをダウンロードして実行できるため,M さんの PC に他のマルウェアを感染させたり,ウイルス対策ソフトが検出できないようにマルウェアを改変したりできる可能性がある。したがって,マルウェア P に感染していた M さんの PC では,他にも未検出のマルウェアが動作しており,ネットワークを通じて被害が拡大するおそれがある。K 主任はそのような事態を懸念し,M さんに PC から LAN ケーブルを抜くように指示したのである。

■設問２

〔試験センターによる解答例〕
(1) マルウェア感染前後における OS の状態の差分を確認するため（28 字）
(2) 8
(3)
a：80
レスポンス：エ
(4) b：HTTP レスポンス（9 字）

(1) X 氏がマルウェア P について調査する上で,M さんの PC の設定がバックアップされていることの有無を確認した目的が問われている。マルウェア感染前の PC の設定がバックアップされていれば,感染後の設定と比較することで,マルウェア感染によって設定が変更された箇所など,**OS の状態の差分を確認する**ことができる。一般的に,マルウェア感染によって PC の設定が変更される可能性が高いことから,X 氏の目的が推測できるだろう。

(2) X 氏が,M さんが受信したメールの送信者は Web メールを利用してメールを送信した可能性が高いと判断したのは,図6の何行目を基に確認したからかが問われている。図6を見ると,8行目の"Received"の末尾に**"via HTTP"**とあり,各ヘッダの意味がわからなくともこれが該当することが推測できるだろう。

メールヘッダの"Received"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ヘッダの一番下となり,ヘッダの一番上の"Received"が最後に経由したサーバが記録した情報となる。

"Received"ヘッダに含まれる主な項目の意味は次の通り。

・from：SMTP の「HELO」コマンドで通知された,メール発信者のホストドメイン名であり,送信者が任意の名称を指定可能。右側の()内には,当該ホストの IP アドレスから逆引きされたホストドメイン名や IP アドレスが入るが,こちらは詐称することは難しい。
・by：メールを受信したサーバのドメイン名,ホスト名など
・via：経由したサーバの環境や接続プロトコル
・with：転送プロトコル
・for：最終的なメール送信先アドレス

(3) 図7より,IP アドレス C.C.C.C に対して,M さんの PC は HTTP プロトコルで通信していたことがわかる。したがって,［ a ］に該当するポート番号は"80"である。

また,ブラウザでアクセスを試行した結果,「当該サーバは稼働していないようであった」とあり,その際の最も適切なレスポンスが問われているが,ア～ウはいずれもサーバが稼働している場合に返されるレスポンスであるため,該当するのは**エ**である。

なお,ア～ウのレスポンスコードの意味は次の通り。

204 Not Content：コンテンツがない（サーバはリクエストを正常に処理）

404 Not Found：要求されたページが存在しない
503 Service Unavailable ：サービスが一時的に使用不可

(4) PC から C&C サーバへの HTTP リクエストが発生すると,その応答結果として,C&C サーバから PC に対し,**HTTP レスポンス**が返る。その中にマルウェア P に対する指令が含まれており,攻撃者は PC を操作することができる。HTTP の基本的な仕組みがわかっていれば解答を導き出せるだろう。

■設問３

〔試験センターによる解答例〕
(1) c：9 月 25 日 14:10
(2)
d：ア
f：ウ
(3) e：xx:xx:xx:aa:bb:22
(4) 192.168.1.1, 192.168.1.3～192.168.1.253

(1) [c]の日時以降のファイルを調査したところ,M さんからのメールが圧縮された状態で保存されており,それは N さんの PC がマルウェア P に感染し,L さんの PC のメール受信時の通信を盗聴した可能性がある,という X 氏と K 主任の会話から,[c]にはマルウェアに感染した日時が入ることがわかる。図 10 より,9 月 25 日 14:10 に N さんの PC が IP アドレス D.D.D.D の二つの URL にアクセスしていたこと,X 氏が同 URL へのアクセスを試行したところ,JRE の脆弱性を突く Exploit コードを受信したとあることから,[c]には**「9 月 25 日 14:10」**が入る。

(2)
d：X 氏が,盗聴時の L さんの PC の ARP テーブルを用いて K 主任に盗聴の手口を説明したことから推測されるように,該当するのは**「ア：ARP スプーフィング」**である。
ARP（Address Resolution Protocol）は,IP アドレスをもとに,ネットワークインタフェースカード（NIC）に割り当てられた物理アドレス（MAC アドレス：Media Access Control address）を得るためのプロトコルである。ARP スプーフィング（ARP キャッシュポイズニングとも呼ばれる）とは,偽の MAC アドレスと正規のホストの IP アドレスとを組み合わせた不正な ARP 応答パケットを送信することで,ARP テーブルの内容を書き換える攻撃手法である。ARP スプーフィングによって,L3SW の IP アドレスに対応する MAC アドレスを書き換えることで,L3SW になりすまし,当該 L3SW を経由するパケットを盗聴することが可能となる。
f：ネットワークを構築する際に利用するものであり,通常は盗聴されにくいものであるから,該当するのは**「ウ：L2SW」**である。かつて広く使われていたリピータハブは,宛先に関わらず接続された機器の全てのパケットが流れるため,盗聴が容易であったが,それに

代わる L2SW は,宛先のポートにしかパケットが流れないため,盗聴されにくくなっている。しかし,前述のように,ARP スプーフィングによってデフォルトゲートウェイとなっている L3SW になりすませば,L2SW を利用していてもパケットを盗聴することが可能となる。

(3) 図 12,図 13 より,192.168.1.254 は,N さんの PC と L さんの PC が接続されたセグメント側の L3SW の IP アドレスであることがわかる。N さんの PC がマルウェア P に感染し,L3SW になりすますことによって L さんの PC のメール受信時の通信を盗聴したと推測されることから,[e] には N さんの PC の MAC アドレスである **xx:xx:xx:aa:bb:22** が入る。

(4) N さんの PC が L3SW になりすますことによって,同じセグメントに接続された他の機器が L3SW を経由して送るパケットを盗聴することが可能となる。該当する送信元 IP アドレスは,図 12 より,N さんの PC が接続されたセグメントで,L3SW と N さんの PC 以外の全ての IP アドレスであるから,**192.168.1.1, 192.168.1.3～192.168.1.253** となる。

■設問 4

〔試験センターによる解答例〕
(1) JRE の最新バージョンにおけるシステム B の正常動作を確認すること（32 字）
(2) User-Agent ヘッダの内容に文字列"Java"が含まれるリクエストをフィルタリングする。（47 字）
(3) プロキシで利用者の認証を有効にする。(18 字)
(4)
設定を行う PC：N さんの PC
禁止する通信：インバウンド通信

(1) JRE に限らず,一般的に,OS やミドルウェアなどをアップデートする際には,関連するアプリケーション等がアップデート後のバージョンで正常に動作するかを事前に確認する必要がある。表 2 より,A 社では,システム B を利用するときにブラウザで Java アプレットを実行するために JRE を使用していることがわかる。したがって,JRE をアップデートする前に,**JRE の最新バージョンにおけるシステム B の正常動作を確認する**必要がある。

(2) HTTP 通信を対象とした対策であり,プロキシ及び UTM で共通して行うことが可能なものを表 3 から探すと,次の三つが候補として挙がる。

①ブラックリスト方式による URL フィルタリング
②ホワイトリスト方式による URL フィルタリング
③HTTP リクエストの任意のヘッダのフィルタリング

JRE の脆弱性の悪用によるマルウェア感染を防ぐ上で,URL に基づくフィルタリングは十分な

対策とはならないため,③を候補として具体的なフィルタリング方法を考察する。マルウェア感染時のHTTPリクエストが図11に示されているので,そこからJREの脆弱性を悪用した攻撃をフィルタリングする上で使えそうな文字列を探すと,リクエスト2,リクエスト3のUser-Agentヘッダに"Java/1.6.0_21"が含まれていることがわかる。"/"以降はバージョン情報であるため対象外とし,③の機能を用いて **User-Agentヘッダの内容に文字列"Java"が含まれるリクエストをフィルタリングする**ことが有効な対策となる。

(3) マルウェアからC&Cサーバへの HTTP通信をプロキシで止める上で有効と思われる対策を表3から探すと,該当するのはプロキシの利用者認証機能である。当該機能の詳細は示されていないが,図2より,マルウェアPは「プロキシ設定を参照する」以上のことは行わないため,**利用者の認証を有効にする**ことが対策となると推測される。

(4) Nさんの PCがLさんの PCの通信を盗聴できたのは,L3SWになりすましたNさんの PCに対し,Lさんの PCからのパケットが送信されたことによる。したがって,Nさん,Lさんのいずれかの PCのパーソナルファイアウォールの設定によってこれを防ぐとすれば,Nさんの PCで**インバウンド通信**を禁止することである。

＜問2＞　スマートフォンを利用したリモートアクセス環境

■設問1

〔試験センターによる解答例〕

(1)

アクセス：

・スマートフォンから社内Webサーバへのアクセス（23字）

・スマートフォンからメールサーバへのアクセス（21字）

対策：

・スマートフォン用のDMZ2を追加し,スマートフォンとモバイルPCの通信経路を分離する。（43字）

・FW4でスマートフォンから社内Webサーバ及びメールサーバへの通信を禁止する。(39字)

(2)

	送信元	宛先	プロトコル
FW3	Any	VPNサーバ2	L2TP over IPsec
FW4	Webメールサーバ	メールサーバ	POP3
	Webメールサーバ	メールサーバ	SMTP

(3)

問題：VPNアカウントを停止すると,モバイルPCから社内ネットワークに接続できなくな

る。(41 字)
対策：スマートフォンで利用する VPN アカウントを,モバイル PC で利用するものと別に作成する。(43 字)

(4) C15

(1)「D 社が認めていないアクセス」に該当するものとして,〔スマートフォンを利用したリモートアクセス環境の構築〕に,**「スマートフォンから社内 Web サーバへのアクセスは認めない」**という記述がある。また,案 1 における実現方式の(2)に,**「スマートフォンのメールクライアントからメールサーバにアクセスすることは禁止する」**という記述がある。
一方,案 1 における実現方式の(1)に「スマートフォンもモバイル PC も VPN サーバ 1 に接続された状態では,(中略) DMZ1 に接続されているのと同じように通信できる」とあり,表 4 を見ると,DMZ1 から社内 Web サーバへの通信 (HTTP, HTTP over TLS) ,DMZ1 からメールサーバへの通信 (POP3, SMTP) がともに許可されている。つまり,上記の「D 社が認めていないアクセス」が技術的に可能となっている状態である。
これに対し,案 2 では DMZ2 が新設されている。DMZ2 にはスマートフォンのブラウザから利用するために構築した Web メールサーバが接続されていることから,スマートフォン用のセグメントであることがわかる。一方,Web メールサーバが移設されたこと以外は FW1, FW2 の設定を含め,案 1 と同様の構成である DMZ1 はモバイル PC 用のセグメントであることがわかる。つまり,**DMZ2 を新設することにより,アクセス権の異なるモバイル PC とスマートフォンの通信経路を分離した**のである。
また,案 2 では DMZ2 とサーバ LAN との間には FW4 があることから,**スマートフォンから社内 Web サーバ及びメールサーバへの通信を FW4 で禁止している**と推測できる。

(2) 案 1 における実現方式の(1)に「スマートフォンの VPN クライアント機能を用いて,L2TP over IPsec で既存の VPN サーバ 1 に接続する」とあるが,案 2 では,VPN サーバ 1 に代わって VPN サーバ 2 に同様に接続する必要がある。したがって,FW3 は,スマートフォンから VPN サーバ 2 への L2TP over IPsec を許可する必要がある。記述形式は表 3 の 1 行目を参考にするとよい。
続いて,FW4 で許可する通信について考察する。スマートフォンから社内 Web サーバへのアクセス及びメールサーバへのアクセスは禁止する必要がある。一方,案 1 における実現方式の(2)に「Web メールサーバは,メールサーバに対してはメールクライアントとして動作」とあることから,FW4 ではこれを許可する必要があることがわかる。Web メールサーバがメールクライアントとして動作するには,送信元が Web メールサーバで宛先がメールサーバの POP3 通信及び SMTP 通信を FW4 で許可する必要がある。記述形式は表 4 の 1 行目,2 行目を参考にするとよい。

(3) スマートフォンの盗難及び紛失の届出があったときにとられる対策とは,図2の6にある通

り,「VPN サーバ 1 の設定において当該利用者の VPN アカウントを停止する」ことであり,これによって引き起こされる問題が問われている。案 1 では,モバイル PC とスマートフォンがともに VPN サーバ 1 に接続する形態となっていることから推測されるように,スマートフォンの盗難及び紛失によって **VPN アカウントが停止されると,モバイル PC から社内ネットワークに接続することができなくなる**という問題が生じる。

これに対し,案 2 では,DMZ2 を追加することにより,スマートフォンとモバイル PC の通信経路を分離している。これにより,**スマートフォンで利用する VPN アカウントを,モバイル PC で利用するものとは別に作成する**ことが可能となるため,スマートフォンの盗難及び紛失によって当該 VPN アカウントが停止されたとしても,モバイル PC を利用する上で特に問題はない。

(4) 表 5 において,R1～R3 のリスクに対する対策 C1～C8 については D 社のネットワークやサーバ側の設定によって対応するものであるため,確実に管理できる。残る C9～C17 についての対応を確認すると,C15 以外については次のように管理していることがわかる。

C9 ：Web メールサーバのみを使用可能とすることにより管理
C10：図 4 の 7 によって管理
C11：Web メールサーバによって管理
C12：図 4 の 6 によって管理
C13：図 4 の 6 によって管理
C14：図 4 の 4 によって管理
C16：図 4 の 5 によって管理
C17：図 3 の 2(1)によって管理

表 1 にあるように,スマートフォン B では,T 社ストアや携帯電話事業者の Web サイトで提供されているものであっても,アプリケーションの安全性審査及び導入時のディジタル署名の検証は行われず,導入するアプリケーションの選択は利用者に任されている。したがって,C16 を実施したとしても,**C15** については D 社の管理が及ばない。

■設問２

〔試験センターによる解答例〕
(1) 携帯電話網を介さずにインターネットに接続されている状態（27 字）
(2)
仕様：一部の機種では,デフォルト設定の状態で自動同期機能が有効になっている。
内容：自動同期機能を無効にする。
(3) C5, C12, C13, C14, C16, C17

(1) 図 5 にあるように,スマートフォンのインターネット接続形態には,携帯電話網を介する場

合と介さない場合とがあるが，〔リモートアクセス環境の改善〕の(2)にある通り，D 社ではスマートフォンの携帯電話網を介したデータ通信を無効化して，無線 LAN 経由でリモートアクセスを行っている従業員が多いのが実情である。下線③のサービスは，携帯電話網を介したデータ通信を用いて提供されるため，上記のように，スマートフォンが**携帯電話網を介さずにインターネットに接続されている状態**ではデータを消去することができない。一方，製品 E では，スマートフォンが携帯電話網を介さずにインターネットに接続されている状態であってもデータを消去することが可能である。

(2) Z 主任は案 3 のレビューにおいて″スマートフォンの仕様の一部が D 社の業務データ取扱事項違反の原因となる″と指摘した。図 6 で業務データの取扱いに関するものを確認すると，データの暗号化や盗難・紛失時の消去のほか，「バックアップデータの保管先として（中略）D 社の管理及び規程が及ばないサービス又はシステムを利用することを禁止する」とある。問題文の冒頭に例示されている通り，「D 社の管理及び規程が及ばないサービス又はシステム」とは，クラウドサービスによって提供されるサービス，オンラインストレージサービス，ファイル共有システムなどである。

続いて表 2 で「クラウドサービスの利用」に関する機能を確認すると，スマートフォン A，B ともに，一部の機種では，スマートフォンに保存されているデータをクラウドサービスのサーバに定期的にコピーする**自動同期機能がデフォルトの状態で有効**になっており，これが D 社の業務データ取扱事項違反の原因となることがわかる。

自動同期機能を無効に設定すれば対策が可能であるため，この問題への対策としてスマートフォン利用手続に追加すべき内容は，**「自動同期機能を無効する」**である。

(3)〔リモートアクセス環境の改善〕にある，製品 E の機能に関する記述部分を表 5 に照らしながら確認することで解答を導き出すことができる。

まず，本文中の「デバイス保護機能の設定及びスマートフォンの設定の監視と強制」が C5，「改造されたスマートフォンの検知」が C14，「OS 及びスマートフォンに導入されているアプリケーションの名称及びバージョンなどの取得」が C12，C13 が該当する。

続いて，図 6 の項番 1 にある「製品 F が導入・設定されていることを，製品 E によって監視する」が C17，項番 2 にある「安全性が疑わしいアプリケーションを導入しているスマートフォンを，製品 E によって検知する」が C16 に該当する。

■設問３

〔試験センターによる解答例〕
スマートフォンの盗難又は紛失の届出があったときに、従業員個人のデータも消去されること（42 字）

〔リモートアクセス環境の改善〕にあるように、製品 E のデータ消去機能は、スマートフォン及び外部記憶媒体に保存された全てのデータを対象としている。したがって、**スマートフォ**

ンの盗難又は紛失の届出によって製品Eのデータ消去機能を実行すれば、業務データに限らず、スマートフォンや外部記憶媒体に保存された従業員個人のデータも全て消去されることになる。この点について事前に従業員に説明し、同意を得ておかないと、当該対策の実施において支障をきたすおそれがある。