平成 25 年度　秋期　情報セキュリティスペシャリスト試験　解答例

午後Ⅱ試験

問 1

出題趣旨
企業において PC 端末のマルウェア感染に起因する被害を最小限に抑えるためには，マルウェア感染自体を防ぐ対策だけでは不十分である。仮に PC 端末がマルウェアに感染してしまったとしても，影響範囲を限定する，感染を早期に発見し，適切な対応を行う仕組みや体制を整えることが重要となる。 本問では，企業において PC 端末がマルウェアに感染した事例を題材に，マルウェア感染時の調査能力，及び調査結果に基づいてマルウェアに対抗するセキュリティ対策を立案する能力について問う。

設問		解答例・解答の要点		備考
設問１	(1)	行動①	不審と判断したファイルを削除した。	順不同
		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。	
		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	
	(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		
設問２	(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		
	(2)	8		
	(3)	a	80	
		レスポンス	エ	
	(4)	b	HTTP レスポンス	
設問３	(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		
設問４	(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		
	(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。		
	(3)	プロキシで利用者の認証を有効にする。		
	(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	

©2013　独立行政法人情報処理推進機構

問２

出題趣旨
スマートフォンを利用したリモートアクセスにおいては，想定する利用形態，利用対象のスマートフォンの技術仕様及び利用可能なセキュリティ技術を踏まえた上で，総合的なセキュリティ対策を検討する必要がある。スマートフォンは今後も高機能化が進み，それに伴って新しい脆弱性が発見されたり，新しいセキュリティ対策技術が開発されると考えられる。そこで，常に技術動向を注視し，セキュリティ対策を見直していく必要がある。 本問では，スマートフォンの技術仕様及びアプリケーションの提供形態を踏まえた上で，総合的なセキュリティ対策を立案する能力を問う。

<table>
<tr><th colspan="2">設問</th><th colspan="5">解答例・解答の要点</th><th>備考</th></tr>
<tr><td rowspan="8">設問１</td><td rowspan="2">(1)</td><td>アクセス</td><td>①
②</td><td colspan="3">・スマートフォンから社内 Web サーバへのアクセス
・スマートフォンからメールサーバへのアクセス</td><td></td></tr>
<tr><td>対策</td><td>①
②</td><td colspan="3">・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。
・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。</td><td></td></tr>
<tr><td rowspan="4">(2)</td><td></td><td colspan="2">送信元</td><td>宛先</td><td>プロトコル</td><td></td></tr>
<tr><td>FW3</td><td colspan="2">Any</td><td>VPN サーバ 2</td><td>L2TP over IPsec</td><td></td></tr>
<tr><td rowspan="2">FW4</td><td colspan="2">Web メールサーバ</td><td>メールサーバ</td><td>POP3</td><td></td></tr>
<tr><td colspan="2">Web メールサーバ</td><td>メールサーバ</td><td>SMTP</td><td></td></tr>
<tr><td rowspan="2">(3)</td><td>問題</td><td colspan="4">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。</td><td></td></tr>
<tr><td>対策</td><td colspan="4">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。</td><td></td></tr>
<tr><td>(4)</td><td colspan="5">C15</td><td></td></tr>
<tr><td rowspan="4">設問２</td><td>(1)</td><td colspan="5">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</td><td></td></tr>
<tr><td rowspan="2">(2)</td><td>仕様</td><td colspan="4">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。</td><td></td></tr>
<tr><td>内容</td><td colspan="4">自動同期機能を無効にする。</td><td></td></tr>
<tr><td>(3)</td><td colspan="5">C5，C12，C13，C14，C16，C17</td><td></td></tr>
<tr><td colspan="2">設問３</td><td colspan="5">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</td><td></td></tr>
</table>

©2013　独立行政法人情報処理推進機構