平成 26 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 I 試験

問 1

出題趣旨
近年，様々な場面でのスマートフォンの利用が増えており，個人所有のスマートフォンを，所属する組織での情報システムの中で活用することも期待されている。しかし，そのような利用において，新たな脅威が生まれることも想定できる。 本問は，スマートフォン用 OS を題材としているが，多くの OS に共通する知識を扱っており，ルート特権化に関する技術及びシステムの運用に関する問題である。特に，スマートフォン用 OS のルート特権化の一手法であるスタックバッファオーバフロー攻撃及びその対策がどのような仕組みであるかを問う。また，それらがシステムインテグレーションや運用にどのように影響するのかのリスク分析能力・対案立案能力を問う。

設問		解答例・解答の要点		備考
設問 1		a	セキュリティパッチ	
		b	ヒープ	
		d	return-to-libc	
設問 2	(1)	スタック領域		
	(2)	c	エ	
	(3)	攻撃を成功させるためのジャンプ先アドレスの特定		
設問 3	(1)	インジェクションベクタを検知・破棄する。		
	(2)	ルート特権があること		
設問 4	(1)	あるアプリから，ほかのアプリのデータへのアクセスを禁止するという仕様		
	(2)	ルート特権化するマルウェアに感染したとき		
	(3)	M システムを使って確認する。		

問 2

出題趣旨
近年，インターネットに接続した Web サーバを用いて実に様々なサービスが提供されている。このようなサービスでは随所に暗号技術が利用されており，中でも，公開鍵認証基盤について適切な設計と運用方法を理解しておくことは，セキュリティ技術者にとって重要である。 本問では，暗号技術の基礎知識と安全性についての考え方，公開鍵認証基盤の下で用いられるディジタル証明書の基礎知識と運用上の特徴及び制約についての知識を問う。また，目標とするセキュリティレベルに合わせて，必要な技術や手法を柔軟に組み合わせ，システムを設計する能力についても問う。

設問		解答例・解答の要点		備考
設問 1	(1)	a	15,360	
		b	512	
	(2)	カ，キ		
	(3)	c	112	
		要件	利用期間は 2025 年 8 月までである。	
設問 2	(1)	端末に発行された証明書の利用停止を申請する。		
	(2)	d	公開鍵	
		e	シリアル番号	
		f	受付拒否リスト	
		g	入力された利用者 ID	
		h	利用者 ID	
設問 3	(1)	代理店の管轄下の端末に証明書がインストールされていることを代表者が確認する。		
	(2)	i	担当者の証明書を停止する権限を代表者に付与する	
	(3)	受付拒否リストに識別番号が登録されている証明書は更新を拒否する。		

問３

出題趣旨
近年，特定の企業や個人を狙った標的型攻撃によって，重要な情報が盗まれる事件が増えている。 本問は，標的型攻撃メールによるマルウェアの感染に対する調査及び情報セキュリティ対策の立案に関する問題である。メールサーバ，ネットワーク機器，標的型攻撃に対する入口対策と出口対策，マルウェア及びハッシュについての基礎知識を問うとともに，業務環境を踏まえた対策についての検討能力を出題している。

<table>
<tr><th colspan="2">設問</th><th colspan="2">解答例・解答の要点</th><th>備考</th></tr>
<tr><td rowspan="2">設問１</td><td>(1)</td><td colspan="2">メールサーバ Z から営業部員宛てに送られるメール</td><td></td></tr>
<tr><td>(2)</td><td colspan="2">送信元メールサーバの IP アドレスのホワイトリストにメールサーバ Z の IP アドレスを追加する。</td><td></td></tr>
<tr><td rowspan="3">設問２</td><td>(1)</td><td colspan="2">FW のフィルタリングルールで遮断しているから</td><td></td></tr>
<tr><td>(2)</td><td colspan="2">顧客管理</td><td></td></tr>
<tr><td>(3)</td><td colspan="2"><table><tr><td>メソッド</td><td>ポート番号</td><td>動作</td></tr><tr><td>CONNECT</td><td>2560</td><td>許可</td></tr></table></td><td></td></tr>
<tr><td rowspan="2">設問３</td><td>(1)</td><td colspan="2">利用者セグメント 2 から開発サーバセグメントへの通信を拒否にする。</td><td></td></tr>
<tr><td>(2)</td><td>a</td><td>運用サーバセグメントの管理に必要のないソフトウェアの利用</td><td></td></tr>
<tr><td rowspan="6">設問４</td><td rowspan="5">(1)</td><td>b</td><td>7</td><td></td></tr>
<tr><td>c</td><td>69[i]</td><td></td></tr>
<tr><td>d</td><td>14</td><td></td></tr>
<tr><td>e</td><td>95[i]</td><td></td></tr>
<tr><td colspan="2">同じパスワードでもソルトが異なるとハッシュ値が変わるから</td><td></td></tr>
</table>